The Axioms of Set Theory
Part II: How to Understand The Axiom of Choice

Thomas Forster

September 15, 2019

Contents

1 Understanding the Axiom **9**

1.1 Thinking you need it when you don't . . . 11

2 Getting the right datatype **15**

2.1 Four Examples . . . 15

2.1.1 A Countable Union of Countable Sets is Countable . . . 15

2.1.2 Socks . . . 16

2.1.3 Every perfect binary tree has an infinite path . . . 17

2.1.4 Lagrange's theorem . . . 17

2.2 The Fallacy of Equivocation . . . 17

2.2.1 Datatypes . . . 18

2.2.2 The Perfect Binary Tree . . . 20

2.2.3 The Countable Union of Countable Sets . . . 21

2.2.4 Lagrange . . . 23

2.2.5 Socks . . . 25

2.3 How the fallacy gets committed . . . 28

2.4 Talk about Datatype expansions here . . . 30

3 What is a Choice? **31**

3.1 The Rule of ∃-elimination . . . 31

3.2 The Rule of ∀-introduction . . . 32

3.3 Some remarks about ∃-elim and ∀-int . . . 33

3.3.1 (i) In what sense are they dual? . . . 33

3.3.2 (ii) They have the same side-conditions . . . 33

3.3.3 (iii) . . . 34

3.4 Back to the Syllogism . . . 34

3.5 Another look at the proof of theorem 1 . . . 34

3.6 Infinitely many choices . . . 35

3.7 Maximal Formulæ . . . 37

3.8 "But I'm making only one choice!" . . . 38

3.9 Executive Summary . . . 39

3.10 Coda . . . 39

4 Supertasks and Zorn's Lemma **41**
4.0.1 Monotonicity and Determinism 43
4.0.2 Supertasks: Expansions and Forcible Wellordering 46
4.1 Counting 48
4.2 Some Subtleties 51
4.2.1 Banach-Tarski 51
4.2.2 Infinite exponent partition relations 51
4.2.3 Grue Emeralds 52
4.2.4 AC^{ω}_{ω} 53
4.2.5 Agency 55

5 Odds and Ends **59**
5.1 A section on Skolemisation? 59
5.2 AC keeps thing simple 60
5.2.1 AC keeps things simple 60
5.3 Is AC true? 61
5.3.1 IBE and some counterexamples 64
5.4 Some thoughts about certificates 68
5.4.1 AC and Certification 72
5.5 Leftovers 74
5.6 Chapter on AC lifted from vol 1 77

6 Appendices etc etc **81**
6.1 Glossary 81

There is plenty of literature on the axiom of choice. However the bulk of it is designed primarily for sophisticates—people who already understand the axiom of choice and are interested in *minutiæ*: mainly questions of which versions imply which other versions, or perhaps some history. Most people who seek information about the axiom of choice are not really interested in which mathematical assertions it is equivalent to, or is needed in the proof of; their concerns are of a much more basic sort: what does AC do? And when am I using it?

This means that the entirely excellent—in its own terms—[8] is precisely the kind of thing I am trying *not* to write. Books like that (and the invaluable [14]) explain various equivalents of the axiom, and weak versions, but they do not set out to banish the bafflement that beginners experience when first trying simply to understand what on earth is going on. The endeavour to understand when you are using the axiom of choice and when you aren't is not at all the endeavour of learning which things are equivalent to AC and which are weak versions of it. [Explaining the technical details of these equivalences and independences is an important exercise, but it is not what the troubled mathematician-in-the-street is looking for. The mathematicians in the street do not want to know what the equivalents of AC are; they want to know when they are using it [and when they should be using it] and that is what the stuff in books like Rubin-and-Rubin doesn't help with.] Cut

My intended audience is the working mathematician who has heard stories about the obscure but important rôle played by this annoying thing called the *Axiom of Choice*, and who thinks it might be an idea to find out what on earth is going on. It assumes that its readers know enough mathematics to have kinds of concerns that the author blah. Probably not for *every* mathematics undergraduate, but perhaps at least every mathematics undergraduate who is moved to pick up a book with a title like this one has. In this it is intended to be the companion volume to [**?**] However there is one bolus of material here which is emphatically not of the kind routinely mastered by the mathematician on the clapham omnibus, and that is the proof theory touched on in chapter 3.

It's not technical, and yet it's not foundational/philosophical either

When i say that most mathematicians have essentially no understanding of AC i am not having a go at them. Most mathematicians don't need to understand it, and not mastering is not a dereliction of duty

Put the working mathematician in the picture

In a nutshell: I am offering not an essay on the mathematics of AC, but a commentary about how it enters into our mathematical practice. I am addressing myself to people who have reached a stage where they can state the axiom—and perhaps know a few equivalents of it—but don't really know what it means and are unsure about when they are making use of it, and who want to know what all the fuss is about. I think my target audience—in the first instance at least—was third-year students at Cambridge who are attending the lecture course on *Set Theory and Logic*. At all events I am addressing working mathematicians who are trying to understand the meaning of their praxis. I am not going to get involved in discussions of whether or not the axiom of choice might be true (whatever that might mean).

In some ways this document is going to be a bit like the sex lessons you had at school. People dishing them out are at pains to reassure you that they are not advocating any particular course of conduct, but are merely trying to put you in possession of certain facts. I don't want my readers to have to learn about this stuff behind the bike sheds the way I had to. The parallel may be better than i know: as with the sex lessons there will be reactions who will complain that young people will be encouraged to experiment and ....

Not going to say anything about the rôle of countable choice in Analysis.

So who am I to lift my head above the parapet and write the book that no-one else does? What is my excuse? The peculiar history of my mathematical education resulted in my being a dedicated student of a distinctly odd set theory of Quine's, namely *New Foundations*. One of its oddities is that it refutes the axiom of choice, so that anybody who wishes to explore the world it describes has to be prepared to eschew the axiom of choice altogether, and to be able to do that you have to be able to detect when you are using it. Subsequently hanging out with theoretical computer scientists (initially as a postdoc) inevitably made me more sympathetic to constructivists than an unreconstructed Quinean would be, and innoculated me with their scepticism of AC. It also made me think in terms of datatypes, and (as I hope to show in what follows, starting in [4]) a proper understanding of AC is helped by unpicking fallacies of equivocation about datatypes. Finally a logician in a mathematics department is forced to think about AC and explain it to their students, even if only because no-one else will.

Imre's practice when proving that a union of countably many countable sets $\{A_i : i \in \mathbb{N}\}$ is countable is to say: "for each i, pick an enumeration of A_i ..." and not mention that this is a use of AC. That's OK in a context where you are not doing this stuff axiomatically.

Douglas Bridges says: Bishop warned us about pseudogenerality

You read on the side of a bus that if you believed in the axiom of choice the cargo would come.

A further fallacy of equivocation is not distinguishing between
(i) the assumption that AC_ω is true (debatable)
and the assumption that
(ii) you don't need it to prove that ctbl U of ctbl sets is Ctbl (plain wrong)

$$\mathrm{AC} \longleftrightarrow X \times X \sim X$$

$$\mathrm{AC} \longleftrightarrow X \hookrightarrow Y \ \vee \ Y \hookrightarrow X$$

Knowing things like that doesn't help you understand why you needed AC to show that a ctbl union of ctbl sets is ctbl.

AC inplies that union of ctbly many ctbl sets is ctbl, but not by using a choice function on the set of all subsets of things in the family. Go round and round picking an element at each stage until you run out. All that tells you is that a union of ctbly many ctbl sets is of size $\aleph_1$ at most.

The Axiom of Choice has—arguably—been the cause of more anxiety and of more ill-informed and unproductive disputation than any other proposition of pure mathematics. Its only rivals for that title are to be found in the disputes about infinitesimals and about the status of complex numbers. What is distinctive about the debate around the axiom of choice is that nobody really seems to know what is at stake. There is an old joke that the axiom of choice is obviously true, the wellordering principle obviously false and that the jury is still out on Zorn's lemma. This joke—like so many really good jokes—circles around an uncomfortable truth: in this case the uncomfortable fact that *we don't know what the axiom itself means*. If you think that the wellordering principle is obviously false but ZL is obviously true then you cannot have understood either of them. It actually isn't a joke at all.

This uncomfortable truth is a daily nightmare of pure mathematics: there is probably a majority of pure mathematicians who profess to believe it, but it's only a minority—even of the believers—who can state it correctly. And—remarkably—even among those who can state it correctly there are plenty who do not know when they are using it (or not using it) . . . which reminds us (again) that they—and we—can't have understood it.

The most straightforward manifestation of this uncertainty and confusion is the dual pair of common errors made by people in its grip. One error is thinking that you blah

The first warning one has to give to the reader, the reader I am addressing myself to, who "just wants to know what in God's name is going on" is that altho' the Axiom of Choice is not in any obvious sense a logical principle, the techniques one needs to employ if one is to flush it out tend to be familiar to logicians rather than to Mathematicians at large. That is absolutely not to say that only a logician can understand what is going on, but if you are to break into the problem you do need some *aperçu* s that do have a rather logical flavour. It is no accident that this little book is being written by a logician. But do not be discouraged!

Chapter 1

Understanding the Axiom

We shall start with a form of it that is particularly simple, to make it easier for the reader to see what is being claimed, and perhaps see whether or not they want to believe it. This first form that we consider is the axiom that Russell [16] called the *multiplicative axiom*. We will see later (p. 24) why it bears this name.

One pleasing feature of this version of the axiom is that it is purely set-theoretical and doesn't need any notation beyond '$=$' and '$\in$' and no concepts beyond *set*. (No pairing, no functions ...)

> Let X be a nonempty family of pairwise disjoint nonempty sets, so that $(\forall y, z \in X)(y \cap z = \emptyset)$ and $(\forall x \in X)(\exists y)(y \in x)$.
>
> Then there is a set Y such that, for all $y \in X$, $Y \cap y$ is a singleton.(M)

Y is said to be a *transversal* set[1].

I can remember thinking—when I first encountered this axiom—that this must be a consequence of the axiom scheme of separation that says that any subcollection of a set is a set. The Y that we are after (once we are given X) is obviously a subcollection of $\bigcup X$, and *that's* a set all right. This is true, but it doesn't help, since there is no obvious way of finding a property ϕ so that Y is $\{w \in \bigcup X : \phi(w)\}$. Contrast with the existence of a bijection between $A \times B$ and $B \times A$: we can specify such a bijection *without knowing anything about A and B*—just flip the ordered pairs round. To find such a Y, given X, it seems that we need to be given a lot of information about X. For an arbitrary X we do not have that kind of information; accordingly we cannot prove (M) above for arbitrary[2] X; this leads us to the conclusion that if we want to incorporate

[1] However one should bear in mind that 'transversal set' has additionally other meanings/uses.

[2] The sudden appearance of the word 'arbitrary' at this juncture is an indication that the stage at which we need to make the axiom of choice explicit at precisely the stage where we acquire the concept of an arbitrary set... in-extension! NOT THE PLACE FOR THIS REMARK

M and its logical consequences in our theory then we will have to adopt it as an axiom.

The problem seems to be that in order to obtain Y we have to select an element from every member of X and we need information about X (and its members) to guide us in making our choices.

At this point I shall revert to a more usual version of the axiom:

> **Every family of nonempty sets has a choice function, a function that picks one member from each element of the family.**

I come to this version of the axiom with some reluctance, since it involves a new mathematical notion, that of *function*; the reader might quite reasonably suspect that we need to sort out the correct way to conceptualise functions before we can understand how they play their rôle in the axiom of choice. Actually we don't, and I hope the reader will consent to read on leaving 'function' undefined.

Equally simple might be: every surjection has a right inverse

One fact we must hang onto, for it is important (even tho' we won't prove it here!) is that the axiom of choice does not follow from the other axioms of set theory. It genuinely is a principle about sets distinct from the other principles of set existence. In insisting on this fact I am not taking a position on whether or not the axiom of choice is *true*. As far as I am concerned you are welcome to believe that the axiom of choice is true, and even that it is obvious (tho' I shall argue that if you do that then you are probably in the grip of a radical misunderstanding)[3]; what you are not at liberty to believe is that the axiom follows from the other axioms of set theory.

Is this the right place to be making this point?

B A D B R E A K

The inability to grasp AC takes two forms. One form is thinking that you aren't using it when you are, and the other is thinking that you need it when you don't. Either way you end up believing it.

If you are making the first mistake, you don't know what all the fuss is about. So, these sad weirdos called *logicians* keep buttonholing you and telling you that you are using the axiom of choice (to do things that are obviously OK) so suppose for the sake of argument that they are right (they're weirdos not idiots, after all) then—of course—that tells you that the axiom of choice is OK. If, on the other hand, you are making the second mistake, of always thinking that you need it, then you naturally think you have to assume it from Day One, since otherwise you would never get anything done.

In broad terms, the thrust of this little essay is to help sufferers recover from these two errors. I start by attempting to explain how the two forms of this inability arise. I shall address the other issues later. I freely admit that the explanation I offer is conjectural and pretty vague, but my aim is pædogogical not philosophical, so I will be happy even if all it achieves is helping some readers

[3] Misquote Maynard Keynes here: Every mathmo who believes AC is in the grip of some hopelessly naive philosophical theory.

get their thoughts in order. Acquiring a correct understanding of what is going on with the Axiom of Choice does more for us than tidying up a skeleton in a remote cupboard in the west wing, since in the process one will come to a clearer understanding of how one does one's mathematics.

1.1 Thinking you need it when you don't

There is a mistake of thinking you need the axiom of choice when you don't, a mistake of *overidentification*. If nobody brought you up to recognise the axiom of choice when you see it, but you learnt behind the bikesheds that this kind of thing goes on, you might startle at shadows. For example you might think that you need AC in the proof of the familiar fact that

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \tag{A}$$

Plenty of people do!

Cast your thoughts back to the old proof of this fact that you have stored somewhere in the back of your mind. If we want to select $k+1$ things from $n+1$ things then we arbitrarily pick one of $n+1$ things, as a sort of pivot, and we then either

(i) select a further k things from the remaining n or
(ii) select $k+1$ things from the n things remaining after we have chosen our pivot.

Process (i) gives us the first summand and process (ii) gives us the second summand. Process (i) gives us all the unordered $(k+1)$-tuples that contain the pivot, and process (ii) gives us all the unordered $k+1$-tuples that do *not* contain the pivot, so we add the two terms to sweep up all the $(k+1)$-tuples we need. But how do we decide which thing to choose for a pivot? It is true that the aggregate number comes out the same whichever pivot we *in fact* choose, but we still have to choose some element, don't we? (i) . . . and aren't we going to need the axiom of choice to tell us that we can in fact choose some element? (ii). We shall see that the answer to (i) is *yes* as expected but that the answer to (ii) is *no*. The 'yes' answer to (i) is probably what the reader expected, but the 'no' answer to (ii) requires some explanation.

Or again:

This example is too sophisticated for this stage

Challenge 1 *If $f : X \to \bigcup X$ is a choice function, and $A \notin X$ is a nonempty set then f can be extended to a choice function for $X \cup \{A\}$*

(You have to pick a member of A, don't you!. . . don't you??)

We need some more illustrations here

The key to understanding why you are not using the axiom of choice on those occasions when you mistakenly think you do—like equation (A) above—lies in some very basic logic. (Indeed the mild disdain with which many mathematicians regard formal logic probably has a significant rôle in perpetuating this misunderstanding)

In elementary Logic classes students are invited to take sentences of ordinary language and regiment them into the language of first-order logic. The aim of the exercise is of course to introduce the student to the idea of formalisation: bringing-out and dealing-rigorously-with the features of interest, while concealing everything else.

(1) If there is a Messiah then we are saved.

(2) If there is even one person in this room with the human-to-human transmissible form of bird-flu then we are in trouble.

(3) If there is even one righteous man in the Cities Of The Plain then God will not fry the city.

Consider (1). Using an obvious lexicon such as '$M(x)$' for 'x is a Messiah' and 's' a propositional constant for 'We are saved' we get

$$(\exists x)(M(x)) \to s \quad \text{or perhaps} \quad (\forall x)(M(x) \to s)$$

Or, looking at (2), writing '$B(x)$' for 'x is a person in this room with the human-to-human transmissible form of bird-flu' and p for 'we are in trouble' we get

$$(\exists x)(B(x)) \to p \quad \text{or perhaps} \quad (\forall x)(B(x) \to p)$$

The fact that in each of these examples there are two apparently quite different formulations is a reflection of the fact that the two following formulæ are logically equivalent:

$$((\exists x)\phi(x)) \to A \qquad (\forall x)(\phi(x) \to A) \tag{1}$$

By 'logically equivalent' we mean that once we have determined what ϕ and A are then the two results have the same truth value.

Attend closely to where the brackets open and close: the first formula is of the form $A \to B$ (top level connective is an if-then); the second formula is of the form $(\forall x)$ stuff ... (the top level connective is a universal quantifier.)

The fact that the two formulæ in (1) are equivalent means that the following inference is good, whatever ϕ and A are.

$$\frac{(\exists x)\phi(x) \qquad (\forall x)(\phi(x) \to A)}{A} \tag{S}$$

The letter 'S' here is intended to suggest 'syllogism'. (It's not a proper syllogism in the classical Greek sense, but never mind[4]). This inference is the crucial

[4]You could obtain something like a syllogism:
There are men
All men are mortal
There are mortals

one to bear in mind when considering situations that look like applications of the axiom of choice that aren't, and the reader is advised to stare at it for a good long while. It's telling you that if, for any x, the ϕ-ness of x is sufficient for A to be the case, then any x will do to ensure A … *you don't need to know which one is* ϕ!

We can use this syllogism to shed some light on situations where some people think we need the axiom of choice. Let us return to one of our earlier examples.

Let's deal with equation (A) first. We are given a set X of $n+1$ things, and we want to prove that the number of $k+1$-sized subsets of X is $\binom{n}{k}+\binom{n}{k+1}$. We notice that, for any $x \in X$, there is a partition of the set of $k+1$-sized subsets of X into two pieces (when wondering which piece to put a subset into, ask whether or not x is a member of the subset in question) of sizes $\binom{n}{k}$ and $\binom{n}{k+1}$. Notice that 'x' does not appear in these formulæ for the sizes of the two pieces, so we get the same answer whichever x we use. This fact gives us the equality we desire—always assuming that there is such an x. But of course there is such an x—in fact there are $n+1$ of them.

Let us recall challenge 1

> If $f : X \to \bigcup X$ is a choice function, and $A \not\in X$ is a nonempty set then f can be extended to a choice function for $X \cup \{A\}$

Consider now the assertion:

> If $f : X \to \bigcup X$ is a choice function, and $a \in A \not\in X$, then $f \cup \{\langle A, a\rangle\}$ is a choice function for $X \cup \{A\}$.

This is pretty straightforwardly true.
Using quantifier-speak it becomes

> $(\forall X)(\forall$ choice functions $f : X \to \bigcup X)(\forall A \not\in X)(\forall a \in A)(\exists x)(x$ is a choice function for $X \cup \{A\})$

which (assuming we are allowed to mix our languages for the sake of telling a story) is unexceptionable. The x in question is of course $f \cup \{\langle A, a\rangle\}$. However when we do the above manipulation to the $\forall a$ quantifier we get

> $(\forall X)(\forall$ choice functions $f : X \to \bigcup X)(\forall A \not\in X)((\exists a)(a \in A) \to (\exists x)(x$ is a choice function for $X \cup \{A\})$

which rewrites to

> $(\forall X)(\forall$ choice functions $f : X \to \bigcup X)(\forall A \not\in X)(A \neq \emptyset \to (\exists x)(x$ is a choice function for $X \cup \{A\})$

which might suggest that we have smuggled in a choice of a member of A. In a sense we have, but what this shows is that *one* choice is all right!

(It might help to consolidate this in your mind by reminding yourself that, in example (2) above, if there is even one person in this room with the human-to-human transmissible form of bird flu then we are in trouble … *even if we don't know who that person is*.)

So the moral to be drawn is that in order to prove things like (A) at the start of this chapter then, yes, you do have to make a choice, but that the act of making that choice is authorised—by first-order logic if you want to think of it that way. We can certainly formalise a proof of (A) in first-order arithmetic.

This means we can upgrade Challenge 1 to an actual lemma!

LEMMA 1 $(\forall X)(\forall$ *choice functions* $f : X \to \bigcup X)(\forall A \notin X)(A \neq \emptyset \to (\exists g)(g$ *is a choice function for* $X \cup \{A\})$.

We are now in a position to prove

THEOREM 1 *(The Finite Axiom of Choice)*
Every finite set has a choice function. For every $n \in \mathbb{N}$*, if* X *is a set of nonempty sets with* $|X| = n$ *then* X *has a choice function.*

Proof:
The proof is by induction[5] on $\mathbb{N}$.

The base case is $n = 0$. The empty function is a choice function for the empty set of nonempty sets.

If you are not happy about the empty function (and you might not be) then start instead with the case $n = 1$. In this case X is $\{x\}$ for some nonempty x. But then, for any $y \in x$, the singleton $\{\langle x, y\rangle\}$ is [the graph of] a selection function for X.

For the induction step we use lemma 1.

■

[5]There is a proof in Russell and Whitehead [17] volume 2, as theorem *120.63.

Chapter 2

Getting the right datatype, and the fallacy of equivocation

This section is designed in the first instance for people who make the second mistake: that of thinking that they don't need the axiom of choice when in fact they do. At the risk of medicalising their errors one can here make good use of the medical slang *presents*[1]: usually the first sign that someone is in the grip of this error comes when they assert blithely that a union of countably many countable sets is countable, *and that no special assumptions are required to show this.* That is when they *present*.

There are many mistakes of this kind being made out there all the time. In this chapter I discuss four examples.

2.1 Four Examples

(i) A union of countably many countable sets is countable;
(ii) Russell's example of the countable family of pairs of shoes;
(iii) Every perfect binary tree has an infinite path;
(iv) Lagrange's theorem that the order of a subgroup divides the order of the (finite) group.

2.1.1 A Countable Union of Countable Sets is Countable

This is the most familiar of the four examples, and is the best one to start on.

People who get into a tangle about this matter typically present with a history of having been taught that a union of a countable family of countable

[1] The stress is on the second syllable; this isn't something you find under a Christmas tree.

sets can be proved to be countable by a simple zigzag construction without any need for further assumptions.

Let $\{X_i : i \in \mathbb{N}\}$ be a family of countable sets. We want $\bigcup\{X_i : i \in \mathbb{N}\}$ to be countable. And we all remember the proof(!)

Draw the X_i out in a doubly infinite array, and then count them by zigzagging, as in the picture below. Let $x_{i,j}$ be the jth member of X_i. Put the members of X_i in order in row i, so that $x_{i,j}$ is the jth thing in the ith row. The *zigzag construction* uses a bijection $f : \mathbb{N} \longleftrightarrow \mathbb{N} \times \mathbb{N}$. Indeed we can even exhibit a definable bijection. On being given $n \in \mathbb{N}$, we recover the largest triangular number $\binom{k}{2} \leq n$. Think about the increment y that we have to add to $\binom{k}{2}$ to obtain n. Evidently $\binom{k+1}{2} = \binom{k}{2} + (k+1)$ so we infer $0 \leq y \leq k$. If we now rewrite k as $x + y$ we have

$$n = \binom{x+y}{2} + y.$$

Clearly x and y are unique by construction. So we can think of n as the pair $\langle x, y \rangle$. Thus, at stage n, we declare that the nth thing in the union is to be xth member of X_y.

Copy stuff about Indiscrete Categories from logicrave to here. . . ?

$$\begin{array}{c|ccccccccccc}
5 & 15 & \dots & \vdots & \dots & & & & & & & \\
 & & \searrow & & & & & & & & & \\
4 & 10 & & 16 & \dots & & \dots & & & & & \\
 & & \searrow & & \searrow & \vdots & & & & & & \\
3 & 6 & & 11 & & 17 & \dots & & & & & \\
 & & \searrow & & \searrow & & \searrow & \vdots & & & & \\
2 & 3 & & 7 & & 12 & & 18 & \dots & & \dots & \\
 & & \searrow & & \searrow & & \searrow & & \searrow & \vdots & & \\
1 & 1 & & 4 & & 8 & & 13 & & 19 & \dots & \\
 & & \searrow & & \searrow & & \searrow & & \searrow & & \searrow & \vdots \\
0 & 0 & & 2 & & 5 & & 9 & & 14 & & 20 \\
\hline
 & 0 & & 1 & & 2 & & 3 & & 4 & & 5
\end{array}$$

2.1.2 Socks

Should have an Erewhonian joke somewhere about having the socks

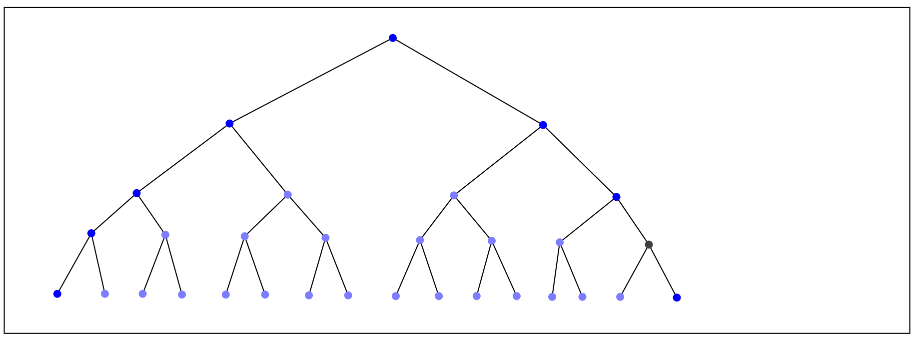
In [16] (p 126) we find the *sutra* of the millionaire whose wardrobe contains a countable infinity of pairs of shoes and a countable infinity of pairs of socks. OK, countably many *pairs* of shoes; how many *shoes*? Obviously $\aleph_0$. Again, countably many *pairs* of socks; how many *socks*? $\aleph_0$ again? If you want a hint, think about why the puzzle contrasts shoes with *socks*, rather than with (say) *gloves*. Then you will see why there really are $\aleph_0$ shoes, not just $\aleph_0$ *pairs* of shoes.

Very well: you have proved that there are countably many shoes; *how many socks?*

2.1.3 Every perfect binary tree has an infinite path

A perfect binary tree is a tree with one root, wherein every node has precisely two children. Probably best thought of as a connected digraph wherein every vertex is of outdegree 2 and every vertex but one is of indegree 1, with the solitary exception being of indegree 0. There are no decorations on the graph, neither on the edges nor the vertices.

If one has a blackboard to hand when telling this story, one is tempted to start off drawing a perfect binary tree on it:



...which makes it obvious that this perfect binary tree at least (the one you have started drawing) has an infinite path. Always choose the leftmost branch. What could be easier!?

2.1.4 Lagrange's theorem

There is a theorem of Lagrange that says that if H is a subgroup of G, then $|H|$ (the "order" of, the number of elements in, H) divides the order of G.

We all know the proof. The cosets of H partition (the carrier set of) G. And they're all the same size, and that size is $|H|$. So clearly $|H|$ divides $|G|$.

2.2 The Fallacy of Equivocation

There are plenty of other examples, but those four are sufficiently familiar and exhibit enough of the common features to serve as generic examples. If you think that the proof-sketches above are sketches of actual proofs—that need only to be written out neatly to be satisfactory—then you are mistaken; as it happens, none of these proofs used the axiom of choice, whereas it is known that these results cannot be proved without some use of AC. Whether one reaches for the word *fallacy* or the word *ellipsis* in this situation is a question to which return on p. **??**. Be that as it may ... the likeliest cause of your mistake is the commission of a *fallacy of equivocation*.

In a *fallacy of equivocation* an unauthorised conclusion is drawn by reading one of the terms in the argument in two different ways. One of my students supplied me with the following excellent illustration.

$$\frac{\text{Bronze is a metal; all metals are elements}}{\text{Bronze is an element.}}$$

This argument (as we say) "*equivocates* on" the word 'metal'.

However in the three cases above we are equivocating on something less tangible than bronze.

And the reason why you are committing the fallacy of equivocation is not (of course!) because you have a desire to be difficult, but simply because you have not noticed that there is a distinction there that needs to be drawn.

So: what fallacy of equivocation is being committed by the miscreants here? What are they equivocating between. . . ? They are equivocating between datatypes. Datatypes?

2.2.1 Datatypes

Greg W sez: metrizable and metric spaces not the same!

The rationals as an ordered set are an ordered set; the rationals as an abelian group are a group. They have the same underlying set but are distinct structures. Many mathematicians grumble about being leant on to observe the distinction between a set and a set-with-knobs-on, but the distinction does make a lot of things clear. A group is not the same as the set of its elements. An ordered set is not the same as a naked set. Model theory has the wonderful word **reduct** which is very useful here. For example, the rationals as an ordered set are a reduct of the rationals as an ordered group. The converse operation is **expansion**, and the rationals as an ordered group are an expansion of the rationals as an ordered set. The rationals as an ordered set are a *reduct* of the rationals as an ordered group because one obtains the first object from the second by "*throwing away*" some structure, and the rationals as an ordered group are an *expansion* of the rationals as an ordered set because one obtains the former from the latter by *adding* some structure. A key observation is that a structure and an expansion of it remain distinct even if one can be turned into the other in only one way. The abelian group of natural numbers less than p (p prime) with addition mod p can be turned into a field in only one way, but—even so—that field is not the same thing as the abelian group, let alone the set $[0, p]$ of natural numbers less than p.

To properly deploy the understanding of the concept of datatype in the struggle to understand AC you have to free yourself from the idea that—for example—there is this object which is $\mathbb{R}$ and can be thought of indifferently as a total order, a field, an ordered ring, a real-closed field, a complete ordered field etc. There is no one object in that sense (or at least, it isn't helpful to think as if there is); instead there are all these objects: $\mathbb{R}$–as–an–ordered-set, $\mathbb{R}$–as–a–real-closed-field ... etc, all obtained by clothing the `naked-set` of reals with the various appropriate gadgets.

Distinguishing between these various manifestations of the reals is a very unnatural move for most working pure mathematicians, who are not interested in thinking of the reals (or for that matter anything else) as a set, but rather as a rich and complex structure with more aspects than you can shake a stick at, and certainly more than you can be bothered to count[2] Indeed, the very idea that mathematical structures are sets-with-knobs-on couldn't even get started until mathematicians acquired/invented the concept of set less than two centuries ago. If you think of the entire history of human mathematics as compressed into a single day, Set Theory appears a few minutes before midnight.

For them the natural point of departure is the reals themselves. The reals can do, and act, many things—"one man in his time plays many parts" after all, so one an think of the reals as ... a field, as an ordered set, as a topological space, as a vector space ... but the tendency is to think that the reals remains the same though all these retellings, and to think that there is no significance—no *cost*—attached to the decision to change one's viewpoint.

To use another bit of logical (well, *philosophical*) jargon, our picture of the reals is rather *intensional* ... we think of the reals as an entity that has a soul, and a soul of which all the other manifestations of $\mathbb{R}$—complete ordered field, vector space over $\mathbb{Q}$, etc etc—all partake. How else are we to explain the common mathematical parlance of [for example] "Consider the reals as an additive abelian group"? I am not saying that there is anything *wrong* with this way of thinking; what i am saying is that there are times when one has to stand back from it.

Of course $\mathbb{R}$ is only one example of a structure that has lots of reducts and natural expansions, all of which one naturally wants to think of as being the same thing; there are other examples. And it is in (some of) these other settings that the intensional way of thinking can obscure uses of the axiom of choice and lead us into error. These distinctions that standard mathematical practice tends to blur are actually in themselves legitimate objects of mathematical study, and we often use the word "(Abstract) Data Type" (or *ADT*) to describe the kinds of structure that conventional practice equivocates between: *Group, ring, vector space, list, tree, ...* and there has been—since the 1960's—an interesting and growing literature on the subject, mainly generated by (theoretical) Computer Scientists.

Make space here for some snide remark about Williamson on Converse Relations [22].

Let us now consider what this identification-of-different-manifestations looks like from the point of view that considers all these manifestations to be distinct

[2] This reluctance to think of the reals as a `naked-set`—or even to contemplate the `naked-set` that you obtain from their conception of reals by throwing away all the extra (fun!) structure—is exemplified by the striking lack of interest that most mathematicians show in the properties that the reals has *qua set*. It is remarkable how many people with degrees in mathematics from reputable institutions do not know that the cardinality of the reals so much as has a *name* let alone that that name is '$2^{\aleph_0}$' rather than—say—'$\aleph_1$". Ask around, you'll see what I mean. And we should not be surprised by this: most of the interesting questions about the set-with-knobs-on that is $\mathbb{R}$ concern the knobs not the naked set.

mathematical objects, mathematical objects distinguished by their datatypes. Any attempt to reason in a way that identifies these (now officially distinct) entities commits . . . a *fallacy of equivocation*.

> *At some point (possibly here) we need a discussion of what operations the ADT of sets does in fact support. It's unlikely to be satisfactory, in that it will be contrastive rather than substantial. Here goes . . .*

One point to bear in mind here is that the ADT of SET is the most stripped-down [back?] of all the extensional datatypes. Any other datatype is distinguished from the ADT of sets by supporting *more* operations not *fewer*. If OP is to be an operation supported by SET then that must be beco's it is supported by all other extensional ADTs. This minimal-structure feature of SET is revealed by the practice in Model Theory of thinking of mathematical structures as sets decorated with gadgets. Not *lists* or *multisets* decorated with gadgets. SETs are the only things so stripped back that every mathematical structure has even a chance of being conceptualised as one of those things with knobs on.

isomorphism of sets is just equinumerosity

So sets have no structure? How does one square that with the idea that when we are given a set we are given all its members and all their members and so on, everything in the transitive closure? That extra structure is not structure of the set; it's the structure (or structures) of its members.

So: what operations does the ADT of sets support? There are plenty of operations that one can easily show that it *doesn't* support; not so easy to find more than one operation that it clearly *does* support. One might expect it to support adjunction and/or subscission, but whether or not it does is really a question about which axioms are true. Are $x \cup \{y\}$ and $x \setminus \{y\}$ reliably sets for all sets x and all objects y? Perhaps it supports all boolean operations except complementation . . . and CO sets support that too? How do these questions differ from questions about which axioms are true?

where do we define these operations?

Perhaps, but it certainly doesn't support "give me your first member". Does it support "Is x one of your members?"? Or "Are you equal to y?"? Or "Give me either a random member or a failure message if you are empty"? If it supports *that* then an application of replacement gives us AC! It's probably safest to say that SET supports only the operation "Is x one of your members?" Actually perhaps it also supports the operation that takes two sets and says whether or not they are identical.

Say something about this?

Thus armed, we can return to the four examples we considered above.

2.2.2 The Perfect Binary Tree

The fact that is obvious is not the fact that

A perfect binary tree has an infinite path; (i) but the fact that

> A perfect binary tree *with an injection into the plane* has an infinite path; (ii)

since we cannot follow the rule "take the leftmost child in each case" unless we can tell what the leftmost child is, and this information is provided for us not by the tree itself but by its injection into the plane. Let us coordinatise the plane: equip it with an origin and two axes. Then the two children of any one node have two distinct addresses that are ordered pairs of reals. When constructing an infinite path we extend it from a given bud node by proceding to the child node whose address is the lexicographically first of the two addresses of the two children.

[*possibly connect this with Ken Manders' tho'rt that any formalisation introduces spurious detail. In this case its a representation rather han a formalisation but the idea is the same*]

Are not (i) and (ii) the same? They certainly will be if any two perfect binary trees are isomorphic. And aren't any two perfect binary trees isomorphic? Isn't that obvious?

No, it isn't: what is obvious is *not*

> Any two perfect binary trees are isomorphic; (iii)

but

> Any two perfect binary trees *equipped with injections into the plane* are isomorphic; (iv)

and (iii) and (iv) are not the same. A perfect binary tree is not the same thing as a perfect binary tree equipped with an injection into the plane.

2.2.3 The Countable Union of Countable Sets

We need to be alert to the difference between *countable set* and *counted set*. A countable set is a naked set that just happens to be countable—there is in the universe somewhere a bijection between it and $\mathbb{N}$, but the whereabouts and nature of this bijection have not been revealed to us; we are like the hero in the mediæval romance who knows there is somewhere in the universe a magic sword to cut the head off the dragon that guards the ring, but he has not been told where it is nor what it looks like. A counted set is, strictly speaking, not a mere naked set at all, but is a structure consisting of a set actually equipped with such a bijection with $\mathbb{N}$. **Knowing that a naked set can be counted is not the same as being in possession of a designated counting of it.** The set and the set-equipped-with-a-counting are two different kinds of objects. The fact that each can be easily obtained from the other doesn't mean they are the same thing. Recall the warning on page 18 that the fact that the additive group of integers mod p can be expanded to a field in only one way does not mean that it is already that field.

(Brief remark: we are overloading "union" to mean all four operations: countable/counted sets of countable/counted sets.)

We need to consider three related propositions[3]:

[3]This formulation is due to Conway (oral tradition)—hence the 'C'.

(Ci): A counted union of counted sets is counted;
(Cii): A countable union of counted sets is countable;
(Ciii): A counted union of countable sets is countable.

These three assertions sound so similar that it is easy for the incautious to confuse them. Fortunately we are now in a position to disentangle them. The zigzag construction from page 16 will be essential.

Let start with (Ci). It's snappy but that's partly because it's an abbreviation. It's a snappy abbreviation for the observation that there is a canonical way of obtaining a counting of the sumset of a counted family of counted sets: the zigzag algorithm.

Now let's think about (Cii). The zigzag algorithm gives us a way of taking a counted bundle of countings and returning a counting of the union of the sets counted. Reflect that the zigzag construction wants its input to be a counted set of counted sets. Let $\{A_i : i \in \mathbb{N}\}$ be a counted set of counted sets. At stage $n = \binom{x+y+1}{2} + x$ the algorithm says to A_x: "Give me your yth element". The zigzag algorithm is the function f in the syllogism. '$A(x)$' says that x is a counted set of countings, and '$B(y)$' says that y is a counting of the union of the sets counted. So (Cii) is straightforwardly provable from first principles, and we have made no use of the axiom of choice.

Not seen supertasks yet

Observe, too, that the execution of the zigzag algorithm is not what we will, later, in section 4.0.2, come to call a *supertask*: all the actions in a run of it can be done simultaneously—at least if counted sets are random-access devices—so that, for any n, we can ask a counted set for its nth member. Send the number $\binom{x+y+1}{2} + x$ to the xth member of the yth counted set.

(Those familiar with realizability semantics for constructive logic might like to think of the zigzag algorithm as a *realizer* of the universally quantified conditional (Cii). A realizer[4] of a conditional $A \to B$ is a function from the set of realizers of A to the set of realizers of B.)

Now consider (Ciii). We have a countable family of countable sets. OK, let's count the family, so we can think of it as $\{A_i : i \in \mathbb{N}\}$. We can do that with a single choice, so we are not using AC.

This is why we have to have the datatype section after the one-choice-is-allowed section

Reflect that the zigzag construction wants its input to be a counted set of counted sets, as it was in case (Cii), where everything was tickety-boo. In contrast, here, faced with a counted set $\{A_i : i \in \mathbb{N}\}$ of merely count*able* sets it won't run. Let's think a bit about this. The zigzag algorithm says to A_1 "Give me your first element". A_1 replies. "I'm a *set* not a *wellordering*—I don't *do* "first" elements; I don't need this; I want my mummy!!" and bursts into tears. In computer science terms what happens is that we here encounter a `typecheck_error`, and we would get a message from the operating system saying something along the lines:

[4] The 'z' in this word is not a violation of the spelling rules of the British English in which I am writing this essay: 'realizer' (as in constructive logic) is an American loan word and we retain the original spelling in order to flag its distinctive use.

`I expected a counted-set, but I found a naked-set.`

[The reader may by now be thinking: "OK, so what are these ADTs? I've had quite a lot dangled in front of me: set, counted-set, binary-tree, binary-tree–with–an–injection .... Can we have a list please? 'Fraid not. We make up these ADTs as we go along, invoking them locally to provide contrastive explanations.]

OK, so how *do* we use AC?

Let us take AC in the form we first encountered it here: every set of pairwise disjoint nonempty sets has a transversal. If we have to invoke AC here, the question is, which family of pairwise disjoint nonempty sets is it that we desire a transversal for?

A moment's reflection will persuade the reader that we can assign a counting to each A_i by applying AC to the (countable) family of sets-of-countings; for each A_i there are plenty of countings—$2^{\aleph_0}$ of them to be precise—and we need to decorate each A_i with one of them in order to expand them into counted sets suitable for the zigzag construction.

where do we define *expand*?

In effect we have used AC to get us back into situation (Cii); we use AC to expand every member of a (counted) family of objects of type `naked-set` into a counted family of objects of type `counted-set`.

In fact this use of AC is neccessary: it cannot be proved in pure set theory that a union of countably many countable sets is countable, but demonstrating this unprovability is a nontrivial task. We discuss below (section 4.2.4) what can be said in the absence of AC.

Do we Say something about independence of AC in vol 1?

(Ci) shouldn't really be taken literally; it's more of a soundbite. If we have a counted family of counted sets then certainly we can use the zigzag algorithm to count it. However, there are uncountably many variants of the zigzag algorithm and they will give us uncountably many countings of the sunset. We can think of (Ci) as true only if we regard the *particular* zigzag algorithm of the picture on page 16 as somehow *canonical*.

The fallacy of equivocation here is between (Cii) and (Ciii).

Somewhere here emphasise the elementary point that for all $n \in \mathbb{N}$ a union of n countable sets is countable.

2.2.4 Lagrange

We want to say that $|H|$ divides $|G|$, of course. That is to say that there is a set C s.t. $|C| \cdot |H| = |G|$. That—in turn—is to say there is a bijection between $C \times H$ and G, since that is how multiplication of cardinals is defined ... so every element of G can be represented by an ordered pair $\langle h, c \rangle$ with $h \in H$ and $c \in C$.

But what is this set C?

If we cannot find such a C then all we can say is that G is the union of a certain number—c, say—of things all the same size h. But in the absence of

AC the expression "the cardinality of a union of c-many things each of size h" cannot be relied upon to denote the cardinal $c \cdot h$. The union of countably many pairs (e.g. of socks, yes) cannot be assumed to be of size $2 \cdot \aleph_0$ (which of course is $\aleph_0$) in the absence of AC.

How do we find such a set C? This is an instance of a general problem, but in this case it's clear what we have to do. Every left coset of H is a bijective copy of H, so for each such coset H' we pick $g \in G$ s.t. $gH = H'$ and call it $g_{H'}$. Then the set C we want is $\{g_{H'} : H' \text{ is a left-coset of } H\}$. Then every $g \in G$ really does correspond to a unique pair $\langle h, g \rangle$ with $h \in H$ and $g \in C$.

What a lot of faff! The average pure mathematician revolts at the thought. Why do they revolt? Because they have been happily equivocating between two data types, and are now being told not to. Indeed even being forced to listen to talk like 'data type' is an unwelcome distraction. In this case the two data types are (i) the data type of (naked) set, which is a set of group elements, and the other (ii) is that of *decorated set* which is a coset $C \subseteq G$ decorated with a g such that $C = \{gh : h \in H\}$. It's rather like the difference between countable-set and counted-set. In fact in one sense it is *exactly the same distinction*: it's the distinction between two datatypes.

That is why I was right to use the letter 'H'' for the coset, rather than write 'gH'. 'gH' is not really a natural notation for denoting a coset, but it is a natural notation for denoting a *decorated coset*.

Of course if there is such a C you can take it to be the set of H-cosets.

Change the Definition of Multiplication . . . ?

The thoughtful and suspicious reader might look at this explanation and say that the difficulty to which the axiom of choice purports to be the answer arises only beco's of the way we have defined multiplication. We have been saying of three cardinals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ that $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$ if and only if there are sets A B and C such that $\mathfrak{b} = |B|$, $\mathfrak{c} = |C|$ and $\mathfrak{a} = |B \times C|$. Perhaps we should instead say that $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$ if and only if a set of size $\mathfrak{a}$ can be expressed as a union of $\mathfrak{b}$ things each of size $\mathfrak{c}$. For this definition to succeed we would have to show whenever A_1 and A_2 are two sets both of which can be expressed as a union of $\mathfrak{b}$ things each of size $\mathfrak{c}$ then $|A_1| = |A_2|$.

The reader has probably guessed by now that proving that equation needs the axiom of choice.

The reader might also think (as I did, for a while) that the fact that the axiom of choice enables us to prove that these two definitions of cardinal multiplication are equivalent is what lies behind the name "The Multiplicative Axiom". That is not so. The significance of AC in this context is that it enables us to prove that *infinite* products (or cardinals) are defined: a product of nomepty sets is nonempty. If we want to show that a product $\Pi_{i \in I} \mathfrak{a}_i$ of a family $\langle \mathfrak{a}_i : i \in I \rangle$ of cardinals is well defined, we use AC to pick a representative set A_i from each $\mathfrak{a}_i$ and then use AC *again* to form the direct product $\Pi_{i \in I} A_i$. Of course the product of the family $\langle \mathfrak{a}_i : i \in I \rangle$ of cardinals is $|\Pi_{i \in I} A_i|$.

2.2.5 Socks

How many shoes does the squillionaire have if he has countably many pairs of shoes? You want to say “countably many” and you are right, but why are you right? Let’s go back to basics. What is a countable set? One that is in bijection with $\mathbb{N}$—one that has a *counting*. So, given that we want to infer that the set of shoes is countable from the information that the set of pairs of shoes is countable, what we should be doing is arguing from the existence of a counting for the set of pairs to a counting for the set of shoes. Classroom experience teaches me, however, that that is not what most mathematicians actually do when confronted with this challenge. They tend to say things like “it’s obvious” or “I can count them” “just pick one, and then another . . . ”. It’s not clear to me (and i suspect not to them either) whether or not they think that their *mere* claim to be able to count the set is evidence that it is countable. It’s almost as if an insistence on my part that they actually exhibit a counting is a veiled attack on their status as adult mathematicians. A certain amount of tact is required on the part of those who insist (as I do in these circumstances) that if you claim that a set is countable you have issued a promissory note that commits you paying the bearer on demand with a counting of it. Merely outlining an answer is not the same as actually giving one. At some point you have to either exhibit an enumeration or admit that you don’t know how to. No stonewalling!

Sometimes it is necessary to lean quite hard on rubes. Those who think they can wave their arms over it. One has to lead such cullions through a catechism along the following lines.

ME	What does it mean to say that a set is countable?
VICTIM	It means you can count it
ME	The set of shoes is countable?
VICTIM	Yes
ME	So it can be counted?
VICTIM	Yes!
ME	I challenge you to count it
VICTIM	[flannel and bluster]
ME	OK! If you know how to count it (but don’t want to show me) at least tell me which shoe is the first shoe according to your scheme. While we’re about it, which is the 15th?
VICTIM	[silence]
ME	I don’t believe you can count it.
VICTIM	[more flannel and bluster, plus indignation]
ME	Prove me wrong in front of witnesses! [*to the sudience*] He can’t count the shoes! He has a mathematics Ph.D. and he can’t count shoes? (He probably can’t even tie the laces on them!) Can anyone here show him how to do it?

The point is easily missed. It is of course true that it doesn’t matter in the least (for the rube’s purposes or mine) which counting you use. But it does matter a very great deal that there is a counting, so it matters that you should be able to produce one on demand—even tho' it doesn't matter which one you produce. People who are affronted by the demand that they produce a counting are confusing two things, one of which matters and the other of which doesn't. It's another fallacy of equivocation.

> "It doesn't matter which bijection I use"

is not the same as

> "It doesn't matter that I can produce a bijection"

The first is true and the second is not.

Sophisticates might discern here a connection of ideas with the constructive critique of classical mathematics. Constructivists never admit that $(\exists x)F(x)$ has been proved until something that is F has been produced. My insistence here, that people who say the set of shoes is countable should be willing to exhibit a counting, isn't really based on these (what a student of mine used to call) *exhibitionist* scruples. I'd be perfectly happy with a nonconstructive proof that there is a counting of the shoes; it's just that prompting the rube to produce a constructive proof is more effective polemically and pædogogically; in any case all the obvious proofs that the set of shoes is countable are themselves straightforwardly constructive so there is no additional cost to the victim in insisting that the proof they come up with should be constructive.

A combination of cajolerie and threats of public humiliation will—eventually—persuade most mathematicians to get off their high horse and condescend to say, out loud: "Yes, the left shoe from the nth pair can be sent to $2n$ and the right shoe from the nth pair can be sent to $2n + 1$." (Tho' this is often done with bad grace, as much as to say that any insistence on an actual bijection is the height of unreason). This does, indeed, show that there are $\aleph_0$ shoes. Good! (Blood from a stone but better late than never.) The point of insisting—at gunpoint—that the rube actually come up with a way of counting the shoes is essential for what is to come, for it is only once they have done that that they will appreciate the significance of their inability to do the same for the socks when the time comes...

...which is does now. How many socks? One wants to say "countably many" of course. This invites the same challenge: "Count them" and, with any luck, the victim will provide (or at least initially reach for) the same answer as they eventually reached with the shoes: send the left sock from the nth pair to $2n$ etc. Of course, for that to work you have to have always a readily identifiable *left* sock and a readily identifiable *right* sock, and of course only mathematicians have odd socks. Old jokes are the best.

Perhaps move this elsewhere

With the shoes you have an algorithm that you can hand on to unskilled unsupervised labour so that you can bunk off for a quick pint at the restaurant at the end of the universe and come back at the end of time when they've finished.

Part of the attraction of this parable (for the preacher) is that, at first blush, the two cases—socks and shoes—look essentially equivalent, and this renders all the more striking the revelation that they are not equivalent. How can they look so similar when they aren't? The answer is that the very physical nature of the setting of the parable has smuggled in a lot of useful information. It cues us to set up mental pictures of infinitely many shoes (and socks) scattered through space. The shoes and socks—all of them–are (or can with only a minimal amount of abstraction)–or can be thought of—as extended regions of space and–as such–they all have nonempty interior. Every nonempty open set in E^3 contains a rational point (a triple all of whose entries are rational), and the set of rational points has a standard wellordering. This degree of asymmetry is enough to enable us to choose one sock from each pair, as follows. In any pair of socks, the two socks have disjoint interiors[5] and both those interiors contain rational points. Consider, for each sock, that rational point in its interior which is the first in some standard wellorder of the rational points, fixed in advance. This will distinguish between the socks, since one will have been given a rational point earlier in the canonical ordering than the rational point given to the other. The physical intuitions underlying this last argument make it very clear to us that we can pick one sock from each pair—as indeed we can. Space is *just sufficiently* asymmetrical for us to be able to explicitly enumerate the socks in countably many pairs scattered through it.

So we have another example of a fallacy of equivocation, this time between:

Every countable set of pairs has a choice function (P)

and

Every countable set of pairs of open subsets of E^3
has a choice function (P')

(P') does not need the axiom of choice, and it ought to be obvious. However I suspect it's worth banging the drum for a proof, as we have just done. In contrast (P) *does* need the axiom of choice, but it looks obvious if you confuse it with (P').

. . . should Say something about how P' is obvious to us beco's of our physical intuitions rather than for any mathematical reasons. This might matter.

In summary:

> *Typically, when someone believes of a consequence of the axiom of choice that it is obvious, it's because they have committed a fallacy of equivocation.*

This is true *typically* rather than *invariably* but the reader is encouraged to take it personally anyway. If you find yourself thinking of some familiar

[5] All right! The two socks in your pair of socks might be folded into each other the way your mother used to do it, so their interiors are not disjoint. However even in these circumstances their interiors S_1 and S_2 are at least *distinct*, The first rational point in the symmetric difference S_1 `XOR` S_2 will belong to one of the two socks, and we can pick that sock!

assertion that it looks obviously true without recourse to the axiom of choice, while nevertheless having at the same time access to expert testimony to the effect that AC is needed for it, then go looking for a fallacy of equivocation.

It may be helpful to think of many of these fallacies of equivocation as failures to attend to the question of which datatype one is using.

- In the case of the socks we are failing to distinguish between `naked-set` [of socks] and `set–equipped-with–injections-into-space` [of socks embedded in space];
- In the case of the perfect binary trees we are failing to distinguish between things of datatype `tree` and things of datatype `trees–equipped-with–an-injection-into-the-plane`.
- In the case of the countable union of counted sets we are failing to distinguish between `naked sets` and `counted sets`.
- In the case of Lagrange's theorem it's a failure to distinguish between cosets as `naked-sets` and cosets as `decorated-sets`.

2.3 How the fallacy gets committed

Blend this paragraaph in somehow

Not mentioned certificates yet

Say something about quite what they are unconsciously assuming in this Lagrange case

Whatever else it is, mathematics is at least a social activity, and a part of becoming a mathematician is learning how to talk like a mathematician. People learning mathematics who have learnt to say things like "let gH be a (left-)coset of H in G" think they are merely learning how mathematicians talk, but they are actually taking on board a great deal more than that[6]. They are learning a language all right, but it is a language that has induced its users to assume the axiom of choice by artfully bundling it into the machinery they use. gH is not a mere left-coset of H in G—a `naked-set`; it is a left-coset decorated with a certificate. That is no more the same thing as a mere left-coset any more than the rationals as an ordered field are the same thing as the rationals as an abelian group. They are not merely learning a language, they are unwittingly adopting unacknowledged assumptions.

OK, so how *does* it get committed?

Mathematics is not revealed, anew and afresh, to each generation. It is transmitted by toiling professionals—whose expositions may be trapped in local optima—to bright young minds that cannot be expected to absorb in a handful of lectures all the facts and all the ill-articulated pitfall-avoidance skills that

[6] Several philosophical communities have the expression 'analytic truth' which means [roughly!] something whose truth is ascertainable merely by analysing it (rather than by checking the way the world is). Ever since Quine made the point a lifetime ago it has been a commonplace among philosophers in his tradition that your decisions about which propositions are to be analytic are made as soon as you choose a language. `https://plato.stanford.edu/entries/analytic-synthetic/` is as good a place to start as any.

their elders have somehow accumulated. It is never possible, when handing on the torch to the next generation, to tell them everything at once. You paint a broad picture, leave some details out, tell a few jokes to make them comfortable and—above all—you *don't frighten them*. Respecting the need for omissions sometimes results in the telling of outright lies, and the way in which first-year students are told that a union of countably many countable sets is countable is a case in point. N.B. the lie is not "a union of countably many countable sets is countable"; the lie is the claim that the usual story is a *proof*. Reasonable people can disagree about whether the axiom of choice ought to be embraced; reasonable people can disagree about whether a policy of lying to children is defensible in this case; what reasonable people are *not* free to disagree about is whether or not the story is a lie. I can imagine that some readers will baulk at this claim, but they shouldn't. We know that some invocation of a choice principle is needed to prove that a countable union of countable sets is countable, so any purported proof that doesn't invoke any such principle is defective. Nowadays we have objective criteria for whether or not a proof is correct, in the form of computer-verification of proofs. And we all know what the verdict would be.

But i said earlier there had been no lies…

Say something about how one feels sympathy with people who confront the expository problem.

[If you want to defend current practice (and it may well be entirely defensible) you have to do it on the basis that it is one of those cases where it is all right to lie to children. Part of that will be an argument that there is no other way of doing it. I will argue that there is a way of doing it with lying, and that is to explain datatypes and casting.]

Even if the mathematics lecturer is not him/herself in the grip of the fallacy of equivocation, the elisions and glossings-over caused by the pædogogical need to press on to the mainstream subject matter of the course have the effect that the students are led to commit the fallacy on their own account. This is because committing the fallacy is the simplest way of exhibiting the behaviour that has been exhibited to them by their lecturer, namely not worrying about AC.

This is the primrose path. You start off by eliding uses of AC from the proof, on the grounds that the details it would involve are not germane to your purposes: the lecturer can be forgiven for forming the view that the distinction between `counted-set` and a countable `naked-set` is one that serves no *immediate* purpose for the first year student, and that accordingly it is entirely proper to gloss over it for the moment, and to leave to lecturers of subsequent years the task of explaining what is going on.

Thus it happens that the first-year students are told that a countable union of countable sets is countable, and they are shown the zigzag picture … and then the caravan moves on without further explanation. They subsequently learn on the grapevine that there are these sad weirdos called *logicians* who insist that this—by now familiar—fact (that a countable union of countable sets is countable) apparently needs this axiom called *"the axiom of choice"*(!?). Mostly they aren't told why, so—rather than make the countable/counted distinction (which in any case they haven't been told about)—they simply uncomprehendingly and innocently embrace the axiom by means of an inference-to-the-best-explanation.

So what happens in their second year, when someone should be dotting the i's and crossing the t's on the dodgy first-year proof that a countable union of countable sets is counted? They are then lectured by someone *who has been through the same process, and made the same mistake*. (A policy of *putting off the explanation until some suitable later date* is always likely to run into trouble if there is no-one whose responsibility it is to ensure that the explanation is ultimately provided.) Never telling the student these things is a sort of tail-event; at any stage there is the possibility of providing an explanation, so it can always be put off. It is only at the end of time that one knows one has failed, and by then it is too late.

Not a tail-event...

'Lying' ... Isn't that a bit harsh? Perhaps nobody has been actually *lied to*, not literally, not *strictly*, but they have been victims of a policy of telling judiciously selected half-truths—albeit with the best intentions. Such policies do not reliably achieve their ends. I remember being told the story of the child that was told that if it sucked its thumb it would swell up and burst. The child takes this on board, as children always do. Next day the child sees on the bus a woman who is 7-months-pregnant and says to her reproachfully "Anybody can see what you've been doing".

There are people who brazenly defend this policy. One of my colleagues (Imre Leader) says that one doesn't routinely flag uses of the axiom of pairing when giving a proof, so why should one have to flag AC? The answer is as follows. The only reason for wanting to flag all uses of the axiom of pairing is if one is trying to reconstruct mathematics inside set theory and is concerned to keep track of which bits of set theory one is doing, in order to prove a point. That is a very special situation to find oneself in, and most of us don't find ourselves in it, so we don't flag uses of the axiom of pairing nor—usually—any other axioms of set theory. The reason why we flag uses of AC is not that AC is a set-theoretic axiom and we want to flag all uses of the axioms of set theory, rather it's because AC is an important distinct mathematical principle: if you're carrying it, you'd better declare it.

2.4 Talk about Datatype expansions here

Chapter 3

Finitely many Choices ... but what is a Choice?

If you were one of the people who are spooked by the equation

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

on page 11 then this chapter is for you.

The fact revealed by theorem 1 is often expressed by some formulation like the *aperçu* :

> "We can always make finitely many choices:
> to make infinitely many choices we need AC" (F)

(F) is extremely arm-wavy, but the thing it is waving towards is important and true. It would be nice to know what a choice is, what choices are, and how we count them. There is a famous remark of Quine's: "No entity without identity" which is very much to the point here. If we haven't got identity criteria for widgets, so that we can't tell when two widgets are the same widget, then we don't really know what a widget is, and we can't use our concept of widget to explain anything. If we are to make sense of (F) then we'd better have a way of individuating choices. What is a choice? One pointer towards answers to these challenges comes from reflecting on the fact that theorem 1 can be proved without using AC, and therefore—if the *aperçu* is correct—while making only finitely many choices. So what is a choice? On the face of it we make a choice every time we go through the induction loop.

Places where we seem to be making choices are typically places where we invoke the syllogism, so I am going to risk doing enough logic to analyse the syllogism. It would be very good for the reader's soul to learn some basic Natural Deduction, but of all the multitude of rules it harbours (two for each connective or quantifier, for starters) the one that will concern us most here is the rule of

$\exists$-elimination, which is the rule that tells us how to exploit—when building a proof—the information wrapped up in an assertion like $\exists x F(x)$.

3.1 The Rule of $\exists$-elimination

The picture below is a hugely simplified picture of a proof of an expression p using $\exists$-elimination. The rule of $\exists$-elimination is famously intimidating to beginners so I am hoping that my readers will not feel that their intelligence is being insulted if I offer a few words of patter. The rule is telling us that if we can deduce p from the news that x has property F—and that the security of the deduction doesn't depend on x, that any x will do—*and* that we know (somehow) that there is something that is F, then we can deduce p. The calligraphic $\mathcal{D}$ names a $\mathcal{D}$erivation of p from the assumption $F(x)$, represented by the vertical dots. The square brackets round the '$F(x)$' mean that that assumption is "used up" by the $\exists$-elimination that is the last line of the proof. That is to say, although $F(x)$ was an assumption in the proof $\mathcal{D}$ (of p) that eventually got processed into our proof of p, it is no longer an assumption of that final proof, of which $\mathcal{D}$ is a part. $\exists x F(x)$ is an assumption in our (displayed) proof of p, but $F(x)$ isn't. The '(1)' connects the application of the rule to the premiss being discharged (there may be lots of other $\exists$-eliminations in the stuff $\mathcal{D}$ abbreviated by the vertical dots.)

$$\dfrac{\exists x F(x) \qquad \begin{array}{c}[F(t)]^{(1)} \\ \vdots\ \mathcal{D} \\ p\end{array}}{p}\ \exists\text{-elim (1)}$$

3.2 The Rule of $\forall$-introduction

There is also the rule of $\forall$-introduction (well, there are lots of rules, but this is the only other one that needs a song-and-dance *here*). Here is the rule of $\forall$-int:

$$\dfrac{\begin{array}{c}\vdots \\ A(t)\end{array}}{(\forall x)(A(x))}\forall\text{−int}$$

To prove that everything has property A, reason as follows. Let t be an object about which we know nothing, reason about it for a bit and deduce that t has A; remark that no assumptions were made about t; Conclusion: *all* xs must therefore have property A. But it is important that x should be an object about which we know nothing, otherwise we won't have proved that every x has

A, merely that A holds of all those x's that satisfy the conditions x satisfied and which we exploited in proving that x had A. The rule of ∀-introduction therefore has the important side condition: 't' **not free in the premisses**. The idea is that if we have proved that A holds of an object x *selected arbitrarily*, then we have actually proved that it holds for *all* x. explain free variable

The rule of ∀-introduction is often called **Universal Generalisation** or **UG** for short; readers may know it under that name. It is a common strategy and deserves a short snappy name. It even deserves a joke.[1]

Remark 1 *Every government is unjust.*

Proof: Let G be an arbitrary government. Since G is arbitrary, it is certainly unjust. Hence, by universal generalization, every government is unjust. ■

This is of course also a fallacy of equivocation.

3.3 Some remarks about ∃-elim and ∀-int

There are some remarks about ∃-elim and ∀-int which are commonplace in Natural deduction circles. (i) They are "dual"; (ii) they have the same *side conditions*; and (iii) ∀-int is easier to understand (or perhaps I mean *accept*) than ∃-elim.

3.3.1 (i) In what sense are they dual?

∃-elim says that if you can deduce p from $F(a)$, then you can deduce p from $\exists x F(x)$. (Modulo side conditions) Consider the following proof:

$$\cfrac{\cfrac{\cfrac{\begin{array}{c}[\neg p]^1\\ \vdots\\ \neg F(a)\end{array}}{(\forall x)\neg F(a)}\;\forall\text{-int} \qquad \neg(\forall x)(\neg F(x))}{\bot}\;\to\text{-elim}}{p}\;\text{classical negation (1)} \tag{3.1}$$

and compare it with the proof by ∃-elimination on p **??** That proof contained a deduction of p from $F(a)$. But if there is such a deduction we can easily obtain from it a deduction of $\neg F(a)$ from $\neg p$.

The proof displayed above shows how, if you can deduce p from $F(a)$, then you can deduce p from $\exists x F(x)$ (Modulo the same side conditions) using ∀-int (instead of ∃-elim) as long as you have a rule of classical negation (the rule that says that if you can deduce a contradiction from $\neg p$ then you can infer p) and accept that $\exists x F(x)$ is the same as $\neg(\forall x)(\neg F(x))$. (You might, Dear Reader, but not everybody does.)

Moral: if you are happy with ∀-introduction, you should be happy with ∃-elimination.

[1] Thanks to the late Aldo Antonelli.

3.3.2 (ii) They have the same side-conditions

t not free in premisses!!!
(∀-elim and ∃-int have no side-conditions.)

3.3.3 (iii)

The significance of the duality lies partly in point (ii). If you are happier with ∀-int than ∃-elim then you might find the demonstration in proof **??** above helpful in making ∃-elim acceptable.

3.4 Back to the Syllogism

What has all this got to do with the syllogism? Answer: if we try to corall an argument that uses the syllogism into anything like Natural Deduction form then we find occurrences of the rule of ∃-elimination appearing wherever we needed the syllogism. Here is a proof of the syllogism in Natural Deduction style.

$$\dfrac{\dfrac{\dfrac{(\forall x)(F(x) \to p)}{F(a) \to p}\ \forall \text{ elim} \qquad [F(a)]^{1)}}{p}\ \to\text{-elim} \qquad (\exists x)(F(x))}{p}\ \exists\text{-elim}(1) \tag{3.2}$$

Suppose we have a proof of a proposition p and at some point in the proof we need there to be a thing which is F. Specifically, if a is such a thing then the deduction $\mathcal{D}_1$ will lead us from $F(a)$ to the conclusion p as desired. We don't care which thing is F (and we may not even know) but we do at least know there is one. This is the assumption '$\exists x F(x)$'.

There will be an instance of the rule of ∃-elimination at any stage in the proof where our construction needs a thing that is F and we know there are some but we haven't identified any. We will be applying ∃-elim to the formula '$\exists x F(x)$'. On our analysis, this is where we make a (single) choice.

3.5 Another look at the proof of theorem 1

With this in mind let us look closely at the proof of theorem 1.

It is a proof by induction on 'i' that every unordered i-tuple of nonempty sets has a choice function. The base case is clear enough, so let us consider the induction step.

Our induction hypothesis is that every set $\mathcal{X}$ of nonempty sets with $|\mathcal{X}| = i$ has a choice function. We wish to deduce that every set $\mathcal{X}$ of nonempty sets with $|\mathcal{X}| = i + 1$ has a choice function.

Let $\mathcal{X}$ be a set of nonempty sets with $|\mathcal{X}| = i + 1$. Since $|\mathcal{X}| = i + 1$, there is an $X \in \mathcal{X}$ with $|\mathcal{X} \setminus \{X\}| = i$. Choose one such X. (Clearly we are going to be doing an $\exists$-elimination using this X). Since $|\mathcal{X} \setminus \{X\}| = i$ we apply the induction hypothesis to $\mathcal{X} \setminus \{X\}$ to infer that it has a choice function. (This conclusion is going to be the premiss of another $\exists$-elimination)

Now suppose f is a choice function for $\mathcal{X} \setminus \{X\}$. By assumption, X is a nonempty set. Then, whenever $x \in X$, we have that $f \cup \{\langle x, X\rangle\}$ is a choice function for $\mathcal{X} \cup \{X\}$. X is nonempty by assumption, so there is, in fact, such an x so (by $\exists$-elimination—again!) there is a choice function for $\mathcal{X}$. But $\mathcal{X}$ was an arbitrary $i+1$-sized set so, by UG, every $i+1$-sized set has a choice function.

Thus the inference from "Every set with n nonempty members has a choice function" to "Every set with $n + 1$ nonempty members has a choice function" makes three uses of $\exists$-elimination. Thus, if n is a concrete natural number we can prove that every set with n nonempty members has a choice function using $3n$ uses of $\exists$-elimination. And we can prove it in some very very minimal set theory without even any arithmetic. The proof of theorem 1 uses only three instances of $\exists$-elim but they sit inside an induction loop and the proof wherein that loop resides is in a stronger system with at least some arithmetic.

Thus the fact that you can make *one* choice is a gift of first-order logic (*constructive* first-order logic indeed—we don't need excluded middle or anything even remotely suspect like that); the fact that you can make *any concrete finite number of* choices, too, is a gift of first-order logic (*constructive* first-order logic, again); the fact that you can make any arbitrary finite number of choices is a theorem of (a suitably spiced up) arithmetic. You prove by induction on n that, for every n, you can make n choices. But this is not a theorem of pure logic (it can't be: pure logic does not know the concept of arbitrary natural number). What about infinitely many choices?

3.6 Infinitely many choices

Taking up the idea that there is a correspondence between constructions ("recipes" à la Euclid) and proofs, and that making a choice corresponds to performing a $\exists$-elimination, what sort of proof might correspond to a construction that makes infinitely many choices? Well, presumably an infinite proof, since one has to somehow fit in infinitely many uses of $\exists$-elimination. In this frame of mind let us look at the proof that a union of countably many countable sets is countable.

It will use the rule of infinite conjunction and have a $\exists$-e in each branch. It would look a bit like this:

$$
\cfrac{
  \cfrac{
    \begin{array}{cc}
      \left[\begin{array}{l} c_1 \text{ is an enum–} \\ \text{eration of } x_1 \end{array}\right]^1 \ldots &
      \left[\begin{array}{l} c_i \text{ is an enum–} \\ \text{eration of } x_i \end{array}\right]^i \ldots \\
      \vdots & \vdots \\
      \vdots & \vdots \\
      \multicolumn{2}{c}{\text{zigzag}\{c_i : i \in \mathbb{N}\} \text{ is an enumeration of } \bigcup_{i \in \mathbb{N}} x_i}
    \end{array}
  }{
    (\exists e)(e \text{ is an enumeration of } \bigcup_{i \in \mathbb{N}} x_i)
  } \ \exists\text{-i}
  \qquad E_1,\ E_2,\ \ldots E_i\ \ldots
}{
  (\exists e)(e \text{ is an enumeration of } \bigcup_{i \in \mathbb{N}} x_i)
} \ \exists\text{-elim}
$$

where 'E_i' is short for '$(\exists e)(e$ is an enumeration of $x_i)$'.

Figure 1

The single occurrence of $\exists$-elimination discharges simultaneously all the infinitely many assumptions "c_i is an enumeration of x_c".

If we are in a situation where we can identify a particular thing which is F then we do not need to make a choice, and our proof will look like the proof in Figure 2 above.

Return to the topic of countable unions of countable sets, and the proof in Figure 1 on on p. 36. If you have an f s.t. $\forall i \in \mathbb{N}$, $f(i)$ is a counting of x_i then the corresponding construction simply zigzags through the c_i in the way you always thought you were supposed to, and allowed to.

If, for each $i \in \mathbb{N}$, we can actually supply a counting c_i, then we can simplify that proof to:

$$
\begin{array}{cccccc}
\begin{array}{l} c_1 \text{ is a} \\ \text{counting} \\ \text{of } x_1 \end{array} &
\begin{array}{l} c_2 \text{ is a} \\ \text{counting} \\ \text{of } x_2 \end{array} &
\begin{array}{l} c_3 \text{ is a} \\ \text{counting} \\ \text{of } x_3 \end{array} &
\ldots &
\begin{array}{l} c_i \text{ is a} \\ \text{counting} \\ \text{of } x_i \end{array} &
\ldots \\
\vdots & \vdots & \vdots & & \vdots & \\
\multicolumn{6}{c}{\text{zigzag}\{c_i : i \in \mathbb{N}\} \text{ is a counting of } \bigcup_{i \in \mathbb{N}} x_i}
\end{array}
$$

and the infinitary occurrence of $\exists$-elim has disappeared. The proof is still infinitary, but it makes no choices. All the x_i are now *counted sets* not mere *countable sets*. And a counted union of counted sets is, as they say, counted.

But there might be lots of a thus designated! Don't we have to choose one? And doesn't this put us back in the situation we started in?

The short answer to this (recommended for people who don't want to think too hard about it) is that, yes, indeed, we do have to make a choice, but the choice is a choice from a smorgasbord of *proofs*, not a ...

Say something about this

3.7 Maximal Formulæ

A *maximal* formula in a proof is a formula that is both the conclusion of an introduction rule and the major premiss of the corresponding elimination rule. There are some technical terms in there for possible future reference; for the moment what matters is that these technicalities *identify formulæ that can be got rid of.* In this proof

$$\dfrac{\dfrac{\begin{array}{c}[p]^1\\ \vdots\\ q\end{array}}{p \to q}\,\to\text{-int }(1) \qquad p}{q}\,\to\text{-elim} \tag{3.3}$$

the formula '$p \to q$' is maximal within the meaning of the act, and there is an obvious manipulation that will turn the proof into

$$\begin{array}{c}p\\ \vdots\\ q\end{array} \tag{3.4}$$

That maximal formula was the conclusion of an $\to$-introduction and the premiss of an $\to$-elimination. Of more concern to us is the following example of a maximal formula that is the conclusion of an $\exists$-introduction and the premiss of an $\exists$-elimination.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ \mathcal{D}_2\\ F(a)\end{array}}{\exists x F(x)}\,\exists\text{-int} \qquad \begin{array}{c}[F(a)]^{(1)}\\ \vdots\ \mathcal{D}_1\\ p\end{array}}{p}\ \exists\text{-elim }(1)$$

The formula '$\exists x F(x)$' is maximal in the sense that it is the conclusion of an $\exists$-int rule and the premiss of an $\exists$-elim rule. There is nothing to stop us taking the proof $\mathcal{D}_2$ (whose last line is $F(a)$) and moving it bodily to the right to place it above the assumption $F(a)$ ... at which point we no longer need the '$\exists x F(x)$' and we have the new, simpler proof[2]:

$$\begin{array}{c} \vdots \; \mathcal{D}_2 \\ F(a) \\ \vdots \; \mathcal{D}_1 \\ \hline p \end{array}$$

Figure 2

The difference between this new proof and the old one is that we have disappeared one occurrence of $\exists$-elimination. And that matters to us because the new construction corresponding to the new proof will have one fewer choice. Thus *the elimination of a maximal formula* corresponds to an operation on constructions that removes one choice.

3.8 "But I'm making only one choice!"

We need to have a reply to the person who says. "OK, as you say, *one* choice is OK. So I make a single choice of a selection function on the family of sets-of-countings of the sets in the family of counted sets. So that's OK!" (S)he is correct: it is indeed only one choice. But that doesn't make it OK; we can make one choice from any nonempty set, agreed; but how do we know that the set of such selection functions is nonempty? It's one thing to show that the collection of such functions constitutes a set, but it has to be nonempty.

Relevant in this connection is the fairly standard exercise for beginners with AC to demonstrate that the Ordering Principle (OP) implies AC for sets of finite sets. (That is, every family of nonempty *finite* sets has a choice function). The ordering principle says that every set has a total order (not a *well*order—it's weaker than AC).

Thinking in terms of actions, OP brings the news that your Fairy Godmother promises to totally order any set for you, on demand. It says:

$$(\forall x)(\exists y)(y \text{ is a total order of } x) \tag{OP}$$

You want a choice function for $\{A_i : i \in I\}$, where all the A_i are finite and nonempty, and you are told OP. If I is infinite (and it's not interesting

[2]A note for proof-theory sophisticates: the formula '$(\exists e)(e$ is an enumeration of $\bigcup_{i \in \mathbb{N}} x_i)$' in Figure 1 is *not* a maximal formula despite being both the conclusion of an $\exists$-int *and* the premiss of an $\exists$-elim

unless it is) then *prima facie* we need the axiom of choice to make the (infinitely many) choices from the various A_i. One wants to say that one can get away with making only one choice, a single choice from the set of choice functions on $\{A_i : i \in I\}$. If we are to achieve our ends by making a single choice—from this set of choice functions—then that set had better be nonempty. We've been here before of course, but this time we have OP. How might OP help?

It's pretty clear that you want to trade on the useful fact that happens to be lying around that any total ordering of a finite set has a first element, so the ability to totally order things looks as if it might come in handy. Can you simultaneously order all the A_i by ordering only one thing? When you put it like that, it becomes obvious what you have to do: totally order $\bigcup_{i \in I} A_i$. Then, for each $i \in I$, the restriction of that order to A_i is a wellorder (since A_i is finite and every total order of a finite set is a wellorder) and you plump for the first element.

It does involve a choice—a single choice, and an instance of $\exists$-elimination. Let R be an arbitrary total order of $\bigcup_{i \in I} A_i$. Then there is a choice function on $\{A_i : i \in I\}$. But (by OP) there is a total order of $\bigcup_{i \in I} A_i$. So there really is a choice function on $\{A_i : i \in I\}$, by $\exists$-elimination.

3.9 Executive Summary

If you always find ourself thinking you are making choices and therefore needing AC, what is probably going on is this. Yes, you are making a choice (as—for example—with formula (A) on p 11 above) but no, you don't need AC, because you are making only a *single* choice. A single choice is justified by $\exists$-elimination.

The rule of $\exists$-elimination gives us a licence to make choices; the ability to make choices give us a licence to use the rule of $\exists$-elimination. If you are happier with one of these licences than the other you can start with the one you feel happier with and venture thence towards the other. Similarly the two rules of $\exists$-elimination and $\forall$-introduction are equivalent and if—like most people—you are happier with $\forall$-introduction than with $\exists$-elimination you can start from $\forall$-introduction, use it to justify $\exists$-elimination and then the licence to make finitely many choices.

3.10 Coda

To a certain extent this chapter is addressed to the concerns of people who realise that in their mathematical praxis they are making choices all the time but mistakenly think they need AC to do so[3]. Such people can find it helpful to become acquainted with the rule of $\exists$-elimination. I don't want to exaggerate the usefulness of the idea that a choice corresponds to an occurrence of $\exists$-elimination, and I am happy to leave the correspondence at a fairly informal

[3]People who don't think they are making choices at all will probably find the next chapter more helpful than this one.

level. However it does help make sense of a number of things. Finitely many choices are always all right because a finite proof can contain finitely many applications of $\exists$-elimination. Infinitely many choices are problematic, but then infinite proof objects (and if a proof is to contain infinitely many $\exists$-eliminations it will perforce be infinite) are problematic. The proof of theorem 1 which says we can make n choices for any $n \in \mathbb{N}$ (and does not use the axiom of choice) is provable because its (finitely many) application of $\exists$-elimination occur inside an induction loop. Finally, constructions-relying-on-having-a-widget do not need a choice when there is a canonical widget available, and in those circumstances the proof associated with the construction does not have an $\exists$-elimination at the crucial point.

To pursue this parallel deeper and further and more seriously than is done here one would need to study infinitary proof objects, and such things are not for the nervous beginner (nor the overconfident beginner) being, as they are, much trickier than they appear. Even *finitary* proof theory remains a fairly niche subject familiar only to theoretical computer scientists of a particular stamp. I harbour the hope that the neat correspondence between making-proofs and eliminating-existentials might encourage missionary-position mathematicians to cast a close eye over Proof Theory.

Cognoscenti may be struck by the lack here of any discussion of the ϵ-calculus. This is partly because the ϵ-calculus is a can of worms, but principally because, altho' a discussion of the axiom of choice can help to shed some light on the ϵ-calculus, there seems to be less traffic in the opposite direction. Our aim is instead to explain the functioning of the Axiom of Choice in Ordinary Mathematics, and the nexus between the ϵ-calculus and the Axiom of Choice is not illuminating for the mathematician on the Clapham omnibus.

Chapter 4

Supertasks and Zorn's Lemma

Tear this up and start again.

Some supertasks can never be completed: if the task is to iterate until you reach an object which—as it happens—isn't there, then you can iterate until you are blue in the face and you get nowhere. More formally, you iterate until you have used up all the ordinals, and you still don't get anything. For example, if you are trying to obtain an $X = \mathcal{P}(X)$ (the power set of X) then you can take power sets at successor stages and take unions at limits and you never reach a fixed point—co's there aren't any! (If X is a fixed point think about $\{x \in X : x \notin x\}$ and as whether it is a member of itself or not.)

manifests itself as blah Failure of continuity at limit stages is part of the problem

A B S T R A C T

Thompson's lamp. Monotonicity and Determinism. M+D $\rightarrow$ completable (Hartogs' lemma). O/w it appeals to a tacit assumption that the infinite resembles the finite—trickery. Separability of the set of points in time.

We saw in theorem 1 on p. 14 how the axiom of choice for finite families is straightforwardly deducible from first principles. In contrast the countable axiom of choice (AC for countable families) is a nontrivial assumption. How can this be? The finite axiom of choice tells us that, for any n, we can make n choices, so why can we not just "keep going" and make infinitely many choices? This leads us to the concept of a *supertask*.

A *supertask* is a task that involves doing infinitely many things. But not *merely* infinitely many things: obtaining $\{n^2 : n \in \mathbb{N}\}$ from $\mathbb{N}$ by squaring everything in $\mathbb{N}$ is not a supertask: since no one act of squaring interferes with any other, all the squarings can be done independently and simultaneously, You have a supertask on your plate when the infinitely many things cannot be done simultaneously but have to be done in succession.

Talk of supertasks entered the philosophical literature with *Thompson's Lamp* (see [20][1] At time $t = 0$ the lamp is off. At time $t = 1/2$ it is switched on, at time $t = 3/4$ it is switched off, then on again at time $t = 7/8$ and so on. The puzzle then is: what is its state at time $t = 1$? The problem is supposed to be that there are compelling reasons to believe that it cannot be on (because every time it is switched on before time $t = 1$ it is subsequently switched off) and similarly it cannot be off. People like us will say that, because the Thompson's Lamp process is discontinuous, what it does *near* $t = 1$ tells us nothing about what it does *at* $t = 1$, so there is no problem. They are right to say that, but to say that is to miss the larger point that there is a huge assumption in the background that the process *can be completed!*, or perhaps I should say that *sense can be made of the idea of the process being completed*. This assumption needs to be identified and examined if we are to understand what is going on with the Axiom of Choice.

If the reader feels that theorem 1 justifies the claim that every *countable* set has a selection function then (s)he is probably thinking that a selection function for a countable set can be obtained by performing the following supertask. First count the set (and by assumption this can be done—the set is countable) so that it has become $\{X_i : i \in \mathbb{N}\}$ and then construct a $\subseteq$-increasing sequence of choice functions for longer and longer initial segments of the ordering by acting out the induction in the proof of theorem 1. Completion of this—nondeterministic—supertask would, indeed, give us a choice function for $\{X_i : i \in \mathbb{N}\}$. But that is to say that the assumption that we can complete this supertask implies the axiom of choice for countable sets.[2] So we seem to be appealing to a principle that supertasks can be completed. When is this assumption safe?

All the supertasks considered in the literature have the feature that the subtasks that compose them and are executed successively have an order-of-execution relation on them that is a wellordering. The assumption that the reals can be wellordered has a multitude of bizarre consequences [my favourite example—shown me by Imre Leader—is that there is an uncountable total ordering with no nonidentity order-preserving injection into itself] obtained typically by constructing the desired bizarre object by recursion on the hypothesised wellordering in a process that can really only be described as a supertask.

In principle one might want to consider supertasks where the order-of-execution relation is not a wellordering, but in the current setting we have

[1] Littlewood [11] is earlier. See also [1]. There is a very readable discussion of supertasks in `https://plato.stanford.edu/entries/spacetime-supertasks/`. It's readable, but not very helpful to readers of this book. Do not be distracted!

[2] The idea that countable choice relies on a supertask argument goes back at least as far as Schuster, [19], though I gather that he no longer holds the views expressed there.

no need to consider such generality: all supertasks considered here will have an order-of-execution relation that is a wellordering. One could say that for us, here, "supertask" is simply a nice sound-bite (or strapline) for *discrete process of wellordered transfinite length*.

4.0.1 Monotonicity and Determinism

Executive summary of this subsection

> *Every monotone [continuous] deterministic process can be completed—Hartogs' thm;*
> *Every monotone nondeterministic process can be completed–AC;*
> *Some non-monotone nondeterministic processes cannot be completed.*

BLEND IN

This use of the word 'monotone' here might sound funny to some, so let me illustrate with a couple of examples:

• The riddle of *Thompson's lamp* [20] see above ...

• Disjunction and conjunction ($\vee$ and $\wedge$) are commutative and associative, so one can think of them as operations on finite sets of propositions. Thought of as functions from sets-of-propositions to truth values they are *monotone* in the sense that

$$P \subseteq Q \to \bigvee P \geq \bigvee Q \tag{4.1}$$

and

$$P \subseteq Q \to \bigwedge P \leq \bigwedge Q \tag{4.2}$$

(setting `false` $\leq$ `true`).

Further, given an infinite family $\langle p_i : i \in \mathbb{N}\rangle$ of propositions, both the sequences

$$\langle \bigwedge_{i<n} p_i : n \in \mathbb{N}\rangle \tag{4.3}$$

(That is to say: p_0, $p_0 \wedge p_1$, $p_0 \wedge p_1 \wedge p_2$ ...)

and

$$\langle \bigvee_{i<n} p_i : n \in \mathbb{N}\rangle \tag{4.4}$$

(That is to say: p_0, $p_0 \vee p_1$, $p_0 \vee p_1 \vee p_2$ ...)

—thought of as their truth-values—are monotone;

This has the effect that a conjunction (or disjunction) of an infinite set of propositions is well-defined[3]. The limit of 4.3 is `false` as long as even one of

[3] Or perhaps—to be cautious—one should say that if one wants to think of the infinite con(dis)junction as being well-defined, it is obvious what the answer has to be. This kind of argumentation is familiar from elementary analysis

the p_i is false (and `true` otherwise)—the point being that if 4.3 ever takes the value `false` then all subsequent values are `false`. Analogously the limit of 4.4 is `true` as long as even one of the p_i is `true` (and `false` otherwise)—the point being that if 4.4 ever takes the value `true` then all subsequent values are `true`.

Contrast this with exclusive-or (`XOR`). `XOR` similarly is associative and commutative and so can be thought of as a function from finite-sets-of-propositions to truth-values. However there is no analogue of 4.1 or 4.2: the sequence

$$\langle \underset{i<n}{\mathtt{XOR}}\, p_i : n \in \mathbb{N}\rangle$$

is not monotone and we do not have a good notion of its limit; one cannot apply `XOR` to infinite sets of propositions; the expression:

$$\underset{i \in \mathbb{N}}{\mathtt{XOR}}\; p_i$$

is not defined: no sense can be made of it.

BLEND IN

Mind you, monotonicity of the function isn't enuff—you need continuity…think power set!!!

If you have both determinism and monotonicity then you have a good notion of what-happens-in-the-limit. Processes that are monotone and deterministic can always be completed: that is the true meaning of Hartogs' lemma: *you never run out of ordinals*. [**Say something about this**]

A monotone deterministic supertask is a project that has a starting condition, and instructions to add something at successor stages, and at limit stages take the union of what you have got so far. There will be a termination condition that tells you when you have succeeded (or crashed). Such a project will always succeed (or crash). If the process never halts (because it neither succeeds nor crashes) then the collection of ordinals of stages you have been through will contain all ordinals, and the set of all ordinals is not to be borne.

Lots of examples: inductively defined sets as unions of stages—completely unproblematic.

However if the process is not deterministic then the collection of stages is not totally ordered and we cannot appeal to the Burali-Forti paradox. What might happen? Instead of getting one well-defined sequence of stages, we might find that we have a debouchement of ever-fragmenting sequences of stages none of which ever come to anything, like a mountain stream getting lost in rivulets in a desert.

Consider the process of trying to find a choice function for a countable family of sets, armed only with the finite axiom of choice, theorem 1.

More generally (if your process is not both monotone and deterministic) then it might crash. However, if it does, it's not because you have run out of ordinals.

If you lack one or other of monotonicity and determinism then bad things can happen, or you need special assumptions if you want to be sure that the supertask completes. Thompson's lamp is deterministic but not monotone, and the state of the lamp at time $t = 1$ is not well-defined; the supertask with AC_ω is monotone but not deterministic, and can't be completed without [some] AC. The supertask of embedding the set of countable ordinals into $\mathbb{R}$ in an order-preserving way is monotone but nondeterministic and cannot be completed *at all* even on the assumption of AC. And this despite the fact that all its proper initial segments can!

The challenge of embedding the countable ordinals into $\mathbb{R}$ looks a bit like a supertask. It looks like a monotone nondeterministic supertask, so AC (or more specifically Zorn) will tell us that it can be completed: the poset of order-preserving partial maps from the countable ordinals into $\mathbb{R}$ ordered by $\subseteq$ is chain-complete and therefore (by Zorn) has maximal elements no problem: the problem is that these maximal elements might not be defined on all countable ordinals—the [modified] identity map that sends the finite ordinal n to the real number n is maximal! The supertask can be completed all right (if we have AC); it's just that the result of that completion isn't what we wanted.

So perhaps we want to tease apart two things. We want to construct a Wombat; it looks as if the Wombat can be obtained as a result of a supertask. We design the supertask, and it completes jez' fine, but sadly we were mistaken: the output is not the Wombat. An order-preserving injection from the second number class into $\mathbb{R}$ is a case in point.

The Axiom of Dependent Choices (DC) is the principle that every [nondeterministic] supertask of length ω can be completed. In its usual formulation it says that, for any set X with a binary relation R satisfying $(\forall x \in X)(\exists y \in X)(R(x,y))$ there is a sequence $\langle x_1, x_2 \ldots n_n \ldots \rangle$ where, for all i, $R(x_i, x_{i+1})$.

Consider the supertask in [11] p 26, which we recapitulate here. We have a bag, and infinitely many beads. Our points in time and our beads are both indexed by countable ordinals. At time $t = 0$ the bag is empty; at time $t = n$ beads with numbers $n \cdot 10$ to $n \cdot 11$ are put into the bag, and the bead with number n is removed. At time $t = \omega$ the bag is empty again; every bead that has been put in before $t = \omega$ is removed before time $t = \omega$. ("let b be an arbitrary bead ..." then b is not in the bag at time $t = \omega$). In fact the bag is empty uncountably often. There is no real mathematical significance to this; the point to the trick is that the mathematically naïve can be spooked by the fact that, athough at every stage you put in more beads than you remove, nevertheless there are stages at which you have removed everything that you have put in. There is nothing wrong with this really, except the fact that the function $n \mapsto$ the cardinality of $\{k :$ the bead with number k is in the bag at time $n\}$ is not a monotone function from the class of countable ordinals to $\mathbb{N}$.

Hang on, what if $n > \omega$?

I bring supertasks up really only in order to wave them away—I think they are a conjuring trick: they entertain but do not enlighten. However one cannot simply ignore them, since appeal to supertask intuitions underlies many people's belief in the truth of the Axiom of Choice. They derive their plausibility from beguilingly familiar features which are actually mathematically entirely irrelevant. Using a supertask argument is like working a conjuring trick, or telling a joke well: they have to direct—or rather *mis*direct—the audience's attention. This is something we shall see again. They also trade on an assumption that the default is for the infinite to resemble the finite. Not in *all* respects it doesn't—clearly!—so this is an assumption that needs to be smuggled in subliminally rather than explicitly made. Better still—as in all good joke-telling—the audience should be induced to make the necessary background assumptions *themselves*.

The Separability of $\mathbb{R}$

It is central to the idea of a supertask that the subtasks be done *in succession*. But succession in what? Both the Thompson's lamp supertask and the countable choice supertask seem to be (notionally) executed in time—actual, physical time. It is this reassuring air of concreteness that lends them what plausibility they have. But one shouldn't be led by this concreteness to an acceptance that all supertasks are executable. It is a consequence of the separability of $\mathbb{R}$ that we cannot embed any uncountable wellordering into the reals in an order-preserving way, and this means that we cannot conceive of any transfinite process (supertask) of uncountable length as taking place *in time*.

This has implications for the possibility of arguing for AC on the basis of supertasks. I want to argue that if you sensibly believe AC—in particular that an arbitrary uncountable set can be wellordered, then it isn't beco's of supertasks. You can't wellorder $\mathcal{P}(\mathbb{R})$ by a supertask since supertasks take place in (notional) time. Once one has taken that on board it seems hardly necessary to follow up with the special case that you can't wellorder even the reals by supertasks beco's if you did, then, the reals being uncountable, the dates at which you pointed to the various reals would form an increasing ω_1 sequence in the time line, and that is impossible.

With the best will in the world it is hard to see a project to justify AC by appeal to supertasks as anything other than an uncritical extrapolation of finite behaviour to the infinite.

If you want to say that your supertasks take place in some other kind of time then you are severing the last link to intuitive motivation.

4.0.2 Supertasks: Expansions and Forcible Wellordering

In this section we discuss the possibility of datatype expansions being performed by supertasks. These are 'expansions' in the model-theory sense in which the rationals as an ordered field are an expansion of the rationals as an ordered set[4] We expand a countable `naked-set` into a structure of type `counted-set` by performing the (mental) supertask of counting it... or do we?

Actually we have to be **very** careful here. If the supertask consists in nondeterministically pulling members out of the set like rabbits out of a hat, in a discrete wellordered sequence of pulls clocked by the ordinals, then there is no reason to expect that we will exhaust it in ω steps (tho' we know we will exhaust it in countably many steps). To be sure of exhausting it in precisely ω

[4]See `https://en.wikipedia.org/wiki/Model_theory`.

steps we'd have to know the enumeration in advance, and be merely *reciting* it, and of course such a recitation effects nothing. In contrast, embedding a perfect binary tree into the plane, or the socks in E^3, are both supertasks of length ω.

It might be worth noting the following facts.

(i) Can't count a countable set just on being told that it's countable;
(ii) Can't count a countable set on being given a wellordering of it;
(iii) Can't count a countable set even if all its members are reals.

need references for these

We consider these in turn.

(i) Every proper initial segment of the set of countable ordinals (the second number class) is countable. If we could count a countable set on being told that it is countable we would have a function that, to each countable ordinal α, replied with a counting of the ordinals below α. That would be enough to prove that the set of countable ordinals has no countable unbounded subset, and it is known (since at least [6] and surely earlier) that any proof of this fact must use at least some AC. It's not even as if there is some strategy we can use on a set X, some project on which we embark, which is guaranteed—*if X is countable*—to produce a counting of it (and which produces something uninformative if X is not countable). We can try picking elements from X as we run through the ordinals. If X is countable we will run out of members of X—and therefore stop—at some countable stage, but there is no guarantee that the output of this process is a counting of X. It'll be a *wellordering* all right, but it might not be a *counting*. It is a deep fact that there is no definable way of extracting a counting of a countable set from a wellordering of it.

(ii) If we could count a countable set on being given a wellordering of it we would have a function that, to each countable ordinal, replied with a counting of the ordinals below it, and this, as we have just seen, needs some AC.

(iii) If we could use the structure of the reals to count a countable set of reals then we would be able to prove that $\mathbb{R}$ is not a union of a countable set of countable sets, and it is known that we can't.

Even once one has taken on board the idea that `naked-set` is a different type from `counted-set` one can still fall into the trap of thinking (and i have heard people say this) that some objects [$\mathbb{N}$ is the obvious example] are obviously counted sets whereas some are obviously merely countable. That's the wrong way to think. It's not that $\mathbb{N}$ is obviously a `counted set`, it starts off as a `naked-set` like everyone else; it's that the `naked-set` $\mathbb{N}$ *happens to* have a counting [the identity map will do nicely] that is rather more salient than the counting of—for example—$\mathbb{Q}$, or—to take a more extreme example—the set of recursive ordinals. need more discussion here

Interestingly to describe this situation properly we seem to need a concept of a structure—$\mathbb{N}$—which we are at liberty to think of as set, a worder, a ...

Even the act of expanding countably many countable sets to countably many counted sets requires AC_ω!! If we think of it as an application of DC it's a supertask of length ω.

4.1 Counting

What does it mean to ask for the cardinality of a (finite) set A?

The answer will be a number ... but how do i give you a number? The number i have to give you is constituted precisely by the collection of things in bijection with A. So, to give you the cardinality of A the only thing i can possibly be doing is giving you the collection of things equinumerous with A: "Give me the cardinality of A" can only mean: "show me all the things that are equinumerous with A". And that collection is an infinite object. How am i supposed to assemble all its members in finite time? Clearly i can't. Of course an infinite object can have a finite description—think: *recursively enumerable subsets of* $\mathbb{N}$—but the most salient finite description of the cardinality of A is as... err ... the cardinality of A, which is depressingly circular. What can i do? If i have, for each cardinal n, a canonical representative $\mathfrak{n}$ of that collection of equinumerous sets, then, to check that A belongs to n all i have to do is find a bijection between A and $\mathfrak{n}$. This means that in order to check whether or not A is equinumerous with some other set B all i have to do is check whether or not B is equinumerous with $\mathfrak{n}$, and this is something i may have ascertained already.

For the moment let us suppose that finding such a bijection is unproblematic—if there is one that is. However, if there isn't one—in the sense that we *fail* by one of A and $\mathfrak{n}$ running out before the other—then we haven't succeeded in ascertaining the cardinality of A. We have to try another cardinal m and canonical representative $\mathfrak{m}$ and hope for better luck. This could take a long time! It's true that if our set A is finite then this process must eventually give us an answer[5] but there must surely be a better way. Of course there is: we choose our canonical representatives in such a way that they *cohere*, so that the canonical representative of smaller cardinal is a subset of the canonical representative of any bigger cardinal[6]. It would help if the canonical representatives came equipped with an ordering, so that the way to ascertain the cardinality of A is to pluck some random member of A, pair it off with the canonical representative of 1, then pick up another and pair it off with the canonical representative of 2, and so on. Then we can use the London Western Railway i mean the last thingumiejig trick, where the last thing we pick up is a flag that tells us what the cardinality is of the set we are counting. It's a no-brainer: the canonical

[5] if our exploration is systematic but that's another story

[6] There is actually a theorem of John Truss that says that any finite collection of cardinals (infinite or whatever) has an order-preserving set of representatives: if $\alpha \leq \beta$ then the representative from α is a subset of the representative from β.

representative of n is simply the set $[1, n]$ of numbers between 1 and n inclusive. What's not to like!?

Mostly this is OK. Admittedly it makes the assumption that the set A is a kind of random access device from which one can pick members *ad libitum* which we can then put back—marked somehow as used, but that's not going to be controversial, since people who think about sets conceptualise them in a way that makes that obvious. What's not to like is this: the numbers in $[1, n]$ are infinite objects, and we don't have access to them. Whatever it was that prevented me from giving you the number as an answer to the question "what is the cardinality of A?" also prevents me giving you a canonical representative that is a set of numbers. We have to have finite objects that are proxies for them. We can use what Quine ([15] p 246*ff*) called *counter sets*[7]. [There are infinite counter sets but until further notice all counter sets are finite]. Some folk—happier with language than with mathematics—would find a tally mark a more natural offering, a string of identical characters of the appropriate length. Either way one is being given a *notation* for a number rather than an actual number ... not that there's anything obviously wrong with that. The lingering sense of dissatisfaction comes about because both answers seem to be entirely *uninformative*.

Of course the standard example of the uninformative answer is "Scott" in answer to "Who wrote Waverley?"

Somewhere above i say something like "if i give you the cardinal number of A, i can only be giving you the set of things equinumerous with A", but of course that doesn't really follow from the conception of cardinal as something that arises from the equivalence class. The cardinal number isn't *literally* the equivalence class, rather it is something that *arises* from it. Indeed, if we are to use cardinal numbers to count things then they literally cannot be the equivalence classes co's those equivalence classes are not finite objects that we can manipulate. So i give you the thing that i have magicked out of the equivalence class. God knows what that is, a dog turd from a very special dog, perhaps. But it's no good my giving you this thing that i have magicked out of the equivalence class unless you know that that's what it is, unless you can tell which equivalence class it's been magicked out of. So i have to tell you that the dog turd is *that* cardinal rather than any other. And how do i do that? Well, the collection of magicked things has to have enough structure for you to be able to

[7]A.A. Verhaegh a.a.verhaegh@uvt.nl writes

Dear Thomas (if I may),

In the footnote you mention, Quine is referring to Robert M. Ravven, a philosophy major and teaching assistant at Harvard in the late 1930s. Unfortunately, I do not know where Ravven developed the idea of counter sets but my best guess is that he did it in his A.B. thesis, written about a year before Quine finished Mathematical Logic. Another possibility is that Ravven had not yet published his work on counter sets (perhaps he never did) and that Quine could only mention Ravven's suggestion when he was writing ML. I am sorry I couldn't be more helpful.

Best wishes,

Sander

recognise its members as members of that collection, and you have to be able to recover—for example—the successor relation from it. Counter sets are pretty good for that sort of thing.

Incidentally this illustrates how we *don't* need the axiom of choice to pick a representative from each natural number.

SO: once you have a classifier for cardinality you can set up a system of pointers. So checking whether or not two things are equipollent becomes simply a matter of checking pointers.

But actually you want not so much a classifier as a choice function, and you want the representatives to *cohere*, to be *order-preserving*. Specifically you want your representative from $S(n)$ to be your representative $\mathfrak{n}$ from n plus an extra element. Is there a cute way of choosing that extra element? What is the obvious candidate for the job of being something-that-is-*not*-in-$\mathfrak{n}$? If we can ensure that none of the members of $\mathfrak{n}$ is $\mathfrak{n}$ itself, then the obvious candidate is $\mathfrak{n}$ itself. How do we ensure that that works? By having ensured, at all earlier stages $m < n$, that the thing-we-added-to-$\mathfrak{m}$-that-wasn't-in-$\mathfrak{m}$ is $\mathfrak{m}$!

Perhaps there is some profit to be derived from the exercise of applying an analysis like this to the counting of countably infinite sets. This gets very murky indeed, since it involves supertasks and the axiom of choice. It's a situation where one has to make risky assumptions simply to get off the ground.

OK, so i have a set X which happens to be countable. How do i count it? I attempt to build a bijection between it and my collection of natural-number-representatives, of counter sets. This is legitimate as long as `set` is the kind of datatype that supports random access and replacement (which is OK) but we also need to be able to perform the supertask of indicating members of X (novel members of X indeed) infinitely often. The assumption that we have this kind of ability is a nontrivial choice principle, since it implies that every infinite set has a countable subset.

And even if that is all right (which i don't think it is, but never mind) we are still not satisfied, and here's why. Let X be an infinite set, and let us pair off members of X with counter sets. That shows that X has a countable subset. It doesn't show that X is countable, because there might be stuff left over *even if X is–in fact—countable*. How are we to ensure that the process of counting, of matching up members of X with counter sets, exhausts X and the set of counter sets simultaneously? Clearly the only way of ensuring that is for X to come equipped with a wellordering of length ω. Notice that even having X being actually countable, plus being equipped with a wellordering doesn't help us. There is no effective route from a wellordering of a countable set to a counting of that set.

4.2 Some Subtleties

It's not a proof [that a union of countably many countable sets is countable] because we know that its possible for the premisses to be true but the conclusion false. Is it an add-warm-water-and-stir pseudoproof that you leave to stand for five minutes and then everything is OK (i.e., a casual description of a correct proof)? There are such proofs, but this is not one of them ... because the student has no way of knowing that anything has been left out. It's like the Blonde Expedition to the Sun "It'll be OK, we're landing at night".

A nice turn of phrase, but what does it mean?

Since it's not a [valid] proof, it's an instance of a fallacy. Which fallacy? Affirming the consequent.

Telling them that is a proof doesn't just give them false beliefs about the axiom of choice [which is bad enough] it gives them false ideas about the nature of proof, and that is much more serious.

It's amazing that anyone should think that the importance and centrality of AC is a reason for *not* telling 1st-years about it. Would Christianity be where it is today if the first christians had said to themselves "The death of Jesus on the cross is this hugely important event that gives us all eternal life *but we're not going to tell anyone about it*".

This policy of not telling students about AC is not a considered result of a set of deliberations; it's a continuation of what would have been a sensible policy before we understood the rôle of AC, compounded by a *post-hoc* rationalisation of bad practice that should have been abolished by the discovery of the axiom.

rewrite this para

4.2.1 Banach-Tarski

Also Vitali, $\mathbb{R}$ as a VS over $\mathbb{Q}$

The real problem thrown up by Banach-Tarski is not AC but the idea that regions of space are sets (of ordered triples of real numbers). How on earth did we get the idea that they were sets? (Never mind sets of triples of reals). Surely this is just as crazy as thinking that numbers are sets?

Banach-Tarski arose from consideration of the dissection puzzles. These are not questions about infinite sets; they are finitary combinatorial questions.

The problem with B-T is not AC, it's pointillism; AC is merely the stain that makes the pathology visible. If you stain pointillism with AC, you get these Banach-Tarski–shaped splodges in the microscope.

4.2.2 Infinite exponent partition relations

There is a theorem [find references] that says that infinite exponent partition relations violate choice. Conversely, if choice fails, one can sometimes find models in which some infinite exponent partition relations hold. What is going on? If one is undecided about AC what is one to believe? What is the mathematical content of these nonexistence proofs? I think the correct response is to say that the possibility of the truth of AC means that there are no algorithms [even in an extended sense] for finding infinite monochromatic sets for partitions of infinite sets… no constructive proof of their existence. Indeed there is a useful parallel here with the critique of classical logic by the constructivists (the exhibitionists). You don't have to discard the classical proof altogether, you just have to start thinking of it as a proof of something else.

4.2.3 Grue Emeralds

Does every perfect binary tree have an infinite path? We haven't examined every perfect binary tree of course, but what we can say is that every perfect binary tree *so far examined* has had an infinite path… and isn't that evidence that every perfect binary tree has an infinite path? There is a curious echo here of a famous puzzle of Nelson Goodman's: the grue emeralds. An emerald is grue (see [7]) if either (i) it is examined before 1/i/2500 and found to be green or (ii) is unexamined before 1/i/2500 and is blue. There is much to debate in this gruesome scenario, but one thing is clear: the fact that every emerald so far examined has turned out to be grue is not evidence that all emeralds are grue.

Granted, every perfect binary tree so far examined has had an infinite path … just as every emerald so far examined has been grue. The act of examining the emerald makes it grue, and the act of examining a tree expands it from an object of type `naked-tree` to an object of datatype `tree-with-an-embedding-into-E`^{3}.

I offer the thought that the mere fact that every perfect binary tree so far conceived has an infinite path is not evidence that all perfect binary trees have such paths.

Expand this section

Examining a perfectly ordinary emerald makes it grue. Conceiving of a set makes it wellordered. So 'wellordered' is a grue predicate.

The suggestion is that thinking that all perfect binary trees so far encountered have infinite branches is evidence for AC_2 is the same mistake as thinking that there is inductive support for "all emeralds are grue".

Can we conceive of perfect binary trees with no infinite branches? Certainly there are models of set theory containing such special trees, but of course they do not *really* lack infinite branches. There are infinite branches all right, just not in the special corner of the universe that is the model containing the special tree. So we haven't succeeded in conceiving of a perfect binary tree with no infinite branch; what we have managed to conceive is a perfect binary tree all of whose infinite branches can be overlooked or mislaid … are in other words *deniable*.

Does this mean that a perfect binary tree lacking an infinite branch is inconceivable? And does its inconceivability mean it's impossible? These avenues of enquiry will remind some readers of Berkeley's Master Argument for Idealism. Berkeley leads his readers by the nose through a thicket of

"it's inconceivable that anything should exist unconceived"

and its like to

"it is impossible that anything should exist unconceived".

The parallels are strong, and they are not encouraging for the advocate of AC, since the general view nowadays is that Berkeley's Master Argument is deeply flawed, and successful repairs—if any—won't capture the sense of the original exercise[8]. There are parallels between the Master Argument on the one hand, and—on the other—the thought that AC is obvious because one cannot imagine a set that can't be wellordered, and an exploration of them may be useful to both parties. I don't think anyone has considered the act of expanding (in the model theoretic sense) a mathematical object to be a mental construction in the way one would in this context, but—altho' it might be helpful—I do not have the stomach for it. But i'll have a tentative stab in section 4.0.2 which now follows.

Get the reference right

4.2.4 $\mathbf{AC}_\omega^\omega$

Nathan says this should be incorporated into the section on supertasks

If we make the countably many choices in advance then, in executing the zigzag algorithm, all we are doing is passively executing a deterministic process; (we are the machine on which it runs, and *we* are not making any choices at all) we are merely proving that a counted union of counted sets is counted. At stage $\binom{m+n}{2} + m$ we take the mth thing from the nth counted set.

However—on the face of it—there is another way of doing it, by making infinitely many choices *in succession* rather than simultaneously. [explain DC] (I suspect that of the people who are aware that one needs AC to show that a countably union of countable sets is countable, most of them think that this is how we make use of choice.)

There are people who have taken on board the fact that one needs countable choice to prove that a union of countably many countable sets is countable, but haven't fully grasped the manner in which AC is put to use in proving it. If you are trying to prove that a union of countably many countable set is countable then, you might think, when you visit the xth set to get its yth member you have to invoke the axiom of choice to obtain that yth member—because that xth set is merely countable not counted. As we've just seen, that is not in fact how the axiom of choice is used in this proof. The endeavour to give a formal description of this strategy results in a story along the following lines.

> "First you count the index set, so you have a family $\{A_i : i \in \mathbb{N}\}$. As we have observed, this costs nothing. Then at stage 1 you ask all the A_i for an element, using a choice function f_1. Where does this f_1 come from? Well, there is this choice principle called $\mathrm{AC}_\omega^\omega$ that says that if I have a countable family $\{A_i : i \in \mathbb{N}\}$ of countable sets then there is a function picking one element from each. This function can be thought of as an ω sequence $i \mapsto f_1(A_i)$ of elements from the union of the A_i. Replace each A_i by $A_i \setminus \{f_1(A_i)\}$ and do

[8] I am endebted to Maarten Steenhagen for directing my attention to [18] (specifically pp 127ff.)

> the same thing, this time using f_2, which is a choice function that $\mathrm{AC}^\omega_\omega$ tells you is to be had for the family $\{A_i \setminus \{f_1(A_i)\} : i \in \mathbb{N}\}$.
>
> Subsequently you iterate, at each stage using a function defined on the (set of the) remains of the A_is, concatenating the ω-sequence you have just obtained onto the end of the sequence you have been constructing so far, so that after n steps you have a wellordering of length $\omega \cdot n$ of a subset of $\bigcup_{i\in\mathbb{N}} A_i$. You keep doing this—possibly transfinitely—until the A_i are all used up. Of course there is no guarantee that the A_i all run out at stage ω, so the process might be of transfinite length. But at least, when it stops, you have a wellordering of $\bigcup_{i\in I} A_i$."

Interestingly this doesn't prove that $\bigcup_{i\in I} A_i$ is countable. *Wellordered* yes, but that isn't enough to show that it is countable. We will return to this later. For the moment our concern is to understand how AC *is* used in the proof that a union of countably many countable sets is countable.

It turns out that here we are using more than merely $\mathrm{AC}^\omega_\omega$. The axiom we are using in this construction is actually the (presumably much stronger) "There is a global function that assigns to each countable family of countable sets a choice function". But observe that even if you have this your desired end will not be reliably achieved. Suppose I use this function ω times, what have I achieved? I have a wellordering of length ω^2 that, for each i, contains infinitely many elements of A_i. I don't know that I have got everything in A_i. I can persist with this process, and run it transfinitely, and eventually I will have wellordered the whole of $\bigcup_{i\in\mathbb{N}} A_i$—but there is no visible countable bound on how long this process will run. It is true that each A_i will be exhausted in countably many stages—at stage α_i, say, to give it a name—but how do we know that the set $\{\alpha_i : i \in \mathbb{N}\}$ is bounded below ω_1? That allegation follows from countable choice, as we know, but the obvious proof (try it) exploits the power to pick representatives from countable families of *uncountable* sets. All we have proved is that a countable union of countable sets is wellordered and of size $\aleph_1$ at most.

Thus it seems that $\mathrm{AC}^\omega_\omega$ doesn't (at least not straightforwardly) prove that a union of countably many countable sets is countable. What can we actually do with it? The obvious thing to do is to try the doomed strategy above and see how far we can go with it. Consider the special case where our countable family of countable sets is in fact a family of *finite* sets. Socks! Clearly our axiom will tell us that we can count the set of socks in the attic. We use the axiom once to simultaneously pick one sock from each of the $\aleph_0$ pairs. Each pair then has only one sock left, and we are done.

THEOREM 2
$AC^\omega_\omega \vdash$ For every $n \in \mathbb{N}$, every countable family of sets all of which are of size n at most has a sumset of size $\aleph_0$.

Proof:

By induction on n.

The theorem is is clearly true for $n = 1$. For the induction step suppose $\mathcal{F}$ is a countable family of sets all of size $n + 1$ at most, and suppose that any countable family of sets all of which are of size n at most has a sumset of size $\aleph_0$. By AC^ω_ω we have a selection function f that picks one element from every set in $\mathcal{F}$. $\mathcal{F}' = \{x \setminus \{f(x)\} : x \in \mathcal{F}\} \setminus \{\emptyset\}$ is now a family to which the induction hypothesis can be applied (all of its members are of size n at most) so it has a sumset of size $\aleph_0$. But $\bigcup \mathcal{F}$ is $\bigcup \mathcal{F}' \cup f``\mathcal{F}$, and $f``\mathcal{F}$ is clearly countable, So $\bigcup \mathcal{F}$ is the union of two countable sets and is countable. ■

What if $\mathcal{F}$ is a countable family of sets all of them finite, but with no finite bound on their size? This theorem tells us nothing about this situation at all!

Nathan says we can prove thm 2 as follows. Suppose we have a countable family of finite sets. Associate to each set the (countable!) set of its total orderings. Use AC^ω_ω to pick an ordering for each, and then concatenate them. This actually shows that a union of countably many finite sets is countable.

This works because each set of total orders is finite. If each set in the family is infinite then it won't work.

Suppose we know that a union of countably many countable sets is wordered. Then AC^ω_ω follows. So, clearly, AC^ω_ω doesn't imply that a countable union of countable sets is countable.

4.2.5 Agency

Most of the ways of pointing up the use of AC involve making fine distinctions that seem to invoke the concept of agency, and this is something of which mathematicians are suspicious, and rightly so: Mathematics is agent-independent. It's one of the reasons why the constructivist critique of classical mathematics gets a cool reception. When we say "it may be that it can be counted, but not by you" it looks as if we are relativising mathematics to agents. Agency is clearly involved in the constructive critique. ... but we aren't really, what we are actually doing is invoking a concept of *information*.

Perhaps this belongs with supertasks

Curry-Howard reeks of agency; anything to do with computability reeks of agency. But remember that a function can be computable even if the agent doesn't know how to compute it.

AC looks plausible in some versions and implausible in others. There are plenty of people who find it entirely plausible that every surjection should have a right inverse but baulk at the tho'rt of every set being wellordered. How can you wellorder $\mathbb{R}$, after all? If you think propositions A and A' have different features then clearly you think they are different propositions. If you find one version of AC plausible and the other one implausible then these two alleged versions of AC cannot both be versions of AC, and you are misidentifying at least one of them—and, if one, then perhaps both. . . ? Why not?

If you think it is implausible that every set can be wellordered then you are probably thinking that the wellordering must be in some sense definable. If you think it plausible that every surjection has a right-inverse then you are probably thinking of the set as having useful added structure. In general you are probably equivocating over different concepts of set.

Of course it might also be that the reason why you don't think that $\mathbb{R}$ can be wellordered is that you can't imagine a wellordering of the reals, and the reals look so familiar that you expect that if there were one, you would be able to imagine it.

Paradoxically you might find yourself more inclined to believe that arbitrary sets can be wellordered than that $\mathbb{R}$ can be wellordered! Is this an example of the conjunction fallacy?

Using the axiom of choice isn't bad mathematics so much as bad *practice*.

Banach-Tarski is loaves-and-fishes.

Nathan says that DC is even more obviously a supertask than is AC_ω.
Wellordering an arbitrary set is a supertask;

Expanding a countable set to a counted set is **not** a supertask of length ω!

Why do we ignore AC? It's not because (like Ax Power set) it's straightforwardly true and there's nothing to stress about. AC is not straightforwardly true in that way.

When confronted with entirely novel stimuli we reach for the tools that we have, however inadequate they be, and try to see the new data as substrates for those old tools. This results in our applying perfectly good intuitions to material for which those intuitions were not designed. It also results in us performing fallacies of equivocation.

Dually when presented with new tools we try to apply them to old problems. When some clever bugger invented the hammer there was a mad rush to go through old outstanding problems to see if any of them were nails.

As Ben Garling says, we often find that old foundational crises leave behind them scars in the form of expository/pedagogical problems.

As Oron says: "why didn't mathematicians work this out ages ago? Why do they understand so little? I think the answer is that for most of mathematical practice a clear understanding of the axiom of choice is not really required. Most of mathematics is the study of the finite, and AC holds in finite domains. Some things that are easy to understand are also easy to *mis*understand, and unless there is an immediate and dire cost to misunderstanding that thing one can continue to misunderstand it for a long time, while nevertheless continuing to enjoy the nice warm feeling brought to one by that misunderstanding-which-one-mistakes-for-an-understanding—which of course is *phenomenally* the same as the nice warm feeling one obtains from *actual* understanding. In these circumstances there are no cues to tell one that one is going down the wrong path.

Chapter 5

Odds and Ends

But perhaps this is a good moment to remind ourselves that AC is not a proposition but a licence: it is not in *proofs* that choices are to be found: it is in *constructions*. Mathematics is not a body of truths/propositions, but a body of constructions, and that is the only way to understand AC. It's not declarative but performative : it confers a licence. Think of Euclid's *Elements*: it's not a body of theorems but a *recipe book*, a body of *instructions for doing things*. You are allowed various tools: for example you are empowered/authorised to draw a line through two points; to draw a circle whose centre is at x and has y on the circumference, and so on. In that spirit AC allows you to wellorder anything.

Explain 'performative'

5.1 A section on Skolemisation?

Well-trodden ground! Provide some pointer and get out fast

Consider what you can expect when you are told $(\forall x)(\exists y)\phi(x, y)$. If you are very lucky there will be a Fairy Godmother who, whenever you say 'x' to her nicely, will reply with a y s.t. $\phi(x, y)$. She has a method for doing this, but she doesn't tell you what it is; she's a fairy, after all. You know that $(\forall x)(\exists y)\phi(x, y)$, but she—unlike you—is actually acquainted with a function f such that $(\forall x)\phi(x, f(x))$. That is to say: the two assertions $(\forall x)(\exists y)\phi(x, y)$ and $(\exists f)(\forall x)\phi(x, f(x))$ are different assertions.

Notice that she only promises to totally order any one set. Or does she, as fairies routinely do, offer to give you *three* wishes? In fact she will even give you *finitely many* wishes. However she does not undertake, on being given $\{A_i : i \in I\}$, to totally order every A_i. (Unless I is finite, of course). That's because OP is $(\forall x)(\exists y)(y$ is a total order of $x)$ rather than the rather scary (infinitary!) expression

$$(\forall x_1)(\forall x_2)(\forall x_3)\cdots(\exists y_1)(\exists y_2)(\exists y_3)\cdots\bigwedge_{i\in\mathbb{N}}(y_i \text{ is a total order of } x_i)$$

5.2 Isn't it simplest just to believe it?

5.2.1 AC keeps things simple

So that everybody is called 'Bruce'. Finite sets obey AC, and mostly the infinite sets we encounter in mathematics do too. Isn't it a reasonably sensible simplifying assumption to make that unobserved sets will behave like observed sets? There are two replies to this. One is that it might be that if we made more strenuous efforts to observe the unobserved sets one might observe them and make interesting discoveries about them. The second is that not every observed set is observed to be wellordered anyway! Don't forget that the best information we have about wellordering the reals is that we *know* there is no definable relation that can be proved to wellorder them. (This allows there to be definable relations that might, in suitable models, wellorder the reals, and this is in fact the case.)

blend these two paragraphs

There are people who do not have a philosophical position on the nature of sets and mathematical entities but who just want to get on with their mathematics. They need a reason to jump one way or the other on the question of the axiom of choice. One suggestion that might carry some weight with such people is that the axiom of choice is a good thing because it *keeps things simple*. If AC fails there are these annoying objects around: infinite sets without countable subsets, countable sets of pairs of socks without a counting of the socks, and so on. Who needs them? Aren't they just a pain?? Why not adopt the axiom of choice and be shot of them all?

One reply that one would like to use, but can't, is that this flies in the face of a widely used (and thoughly bad) line of talk about set-theoretic axioms, namely that one should populate the mathematical universe with everything one can. This line of talk is terrible, because *Extremalaxiomen* of this kind basically never make sense. But this reply may be worth using nevertheless, since there are people who are susceptible to maximisation principles of this kind, and might be induced to adopt . . . infinite sets without countable subsets, countable sets of pairs of socks without a counting of the socks, and so on, as above.

Which view? I've got lost

Widespread though this view is, and appealing though it undoubtedly is, it really is entirely without merit. The choiceless family of pairs of socks is a pain, no doubt, and it seems we would be better off without it. But then the paradoxical decomposition of the sphere is a pain too, and you get that if you adopt AC. Not only is it a pain, but it is a pain of a very similar stamp: the pathological sock collection and the paradoxical decomposition of the sphere alike have the twin features of not only being initially counterintuitive but also—even on inspection—lacking any motivation in what one might tempt fate by calling *ordinary mathematics*. However the point is not so much the tit-for-tat point that the Axiom of choice has some pathologies that are as gross as the pathologies associated with its negation; the point is that it is a mistake to try to anticipate what mathematics will throw at us. We can't simply ignore things we don't like. Perhaps there just *are* bad families of pairs of socks, in the way that (at least according to AC) there just are paradoxical decompositions of the sphere. Granted: the paradoxical decomposition of the sphere no longer looks paradoxical, but the fact that something that looked paradoxical *then* no longer looks paradoxical *now* serves only to remind us that something that looks pathological at the moment might look a lot less pathological in fifty or a hundred years' time.

It may well be that the wisest course in relation to the axiom of choice is the same course as the $\sqrt{2}^{\sqrt{2}}$ story leads us to in relation to the law of excluded middle. Use it sometimes, but bear in mind that there may be other times when the news it brings you is useless to you. And to always, *always*, prefer proofs that do not use it to proofs that do.

The current situation with AC is that the contestants have agreed to differ. People who are fully signed up to the modern consensus realist view of sets as arbitrary objects-in-extension believe—almost without exception—that the axiom of choice is true. There is a smaller party—consisting largely of constructivists of various flavours—who have a subtly different—and more intensional—concept of set and who in consequence do not accept the axiom of choice.

As well as the agreement (between the camps) to disagree there appears to be agreement within each camp. The emergence of the axiom of determinacy (which contradicts AC) caused a few flutters among the platonists: the axiom couldn't simply be ignored: it was far too interesting for that. And to accept it would be to reject AC. They found instead a way of domesticating it: certain large cardinal hypotheses imply that it is true in a natural substructure of the universe. That way they get the best of both worlds.

5.3 Are there Principled Reasons for Believing AC to be true?

We don't seem to be getting very far with making AC look plausible by deducing obvious truths from it. So can one argue for it directly? Are there principled reasons for believing AC to be true?

As we have just noted, it seems to be the case that most of the people who believe that the Axiom of Choice has a truth-value at all tend to believe that that truth-value is 'true'. I think this is a common-cause phenomenon: the forces that lead people to believe that the axiom of choice has a truth value tend also to make them think that that truth-value is 'true'. The forces at work here are various kinds of belief in the ultimate reality of mathematical objects, and ways of thinking about those objects. If a set is real, then you can crawl all over it and get into all its nooks and crannies. And by doing that, you perforce wellorder it. After all, if—having time on your hands as one does when one is trying to fall asleep by counting sheep—you count members of your set then you will wellorder it. You never run out of ordinals to count the sheep with (that is Hartogs' lemma) so your endeavour to wellorder the set cannot fail. And if you didn't count Tweedledum before you counted Tweedledee that can only be because you counted Tweedledee before you counted Tweedledum. Again, a supertask.

On this view the axiom of choice is just plain true, and the intuitive argument for it is that one can boldly go and straightforwardly just wellorder the universe *by hand* as it were. To be more precise, the axiom of choice (on this story) follows from realism about mathematical objects. The force of this story derives from the plausibilty of the idea that we can just go on picking up one thing after another until we have picked up everything. We can do it with material objects and so—being realists about sets as we are—we expect to be able to do it to sets.

Supertask

If you are platonist you believe that every set is out there, somewhere, to be pawed and pored over. If you paw it long enough you can probably wellorder it. If you examine the set of pairs of socks long enough, you will be able to pick one sock from each pair. At least that's what it looks like to most platonists. If you are a platonist you believe that it is possible (at least for a suitably superior intelligence) to know everything there is to know about a mathematical object such as a set, so you know how to wellorder any set. Why should you be able to wellorder it? Nobody seems to know. It's probably something to do with an ill-formulated intuition about the ultimately deterministic nature of mathematical entities. This intuition may have the same roots as the intuition behind what philosophers call *bivalence* . . . and it may of course be a mistake! There just might be mathematical objects that are of their essence sufficiently nondeterministic for us not to be able to wellorder them but we don't seem to be able to imagine any at the moment. Indeed we might not be able to *imagine* any—ever. If we could imagine them, one feels, one would be able to wellorder them. (Might this be something to do with the fact that 'imagine' seems to mean 'visualise' and once we visualise something we can wellorder it? In this connection see the discussion on the significance of our intuitions of space on page **??**.) There is an echo here of the phenomenon of *self-refutation* as in "It is raining and I don't believe it"; "I can't say 'breakfast"' and perhaps Berkeley's master argument for idealism.

But this is just the supertask mistake

This way of thinking about sets is nevertheless entirely consonant with the way in which the *sutra* of the socks is recounted. To the mathematical realist it seems perfectly clear that the set of socks is countable, even at the same time as it is clear to the realist that lesser mortals might be unable to count them and might well come to believe that they form an uncountable or Dedekind-finite collection. The Bounded Being remains unconvinced that the set of socks is countable but that is only because the Bounded Being has incomplete information. Should the Bounded Being ever be given the full story about the socks (s)he will see immediately that the socks are wellordered. Sets are like that: I can hear siren voices saying things like . . . "*being wellordered is part of our conception of set*"; or "*if you can conceive it you can wellorder it*"; or "*if you can't wellorder it then it's a not a completed totality*".

There are two things wrong with this story. The first is that the imagery of picking things out of a set *in time* is restricted to sequences of choices whose length can be embedded in whatever it is that measures [our conception of] time, presumably $\mathbb{R}$. We cannot embed into $\mathbb{R}$ any wellorderings of uncountable length so this story never tells us how to wellorder uncountable sets.[1] This doesn't mean that the story is wrong, but it does demonstrate that its intuitive plausibility is entirely spurious—even if you believe in supertasks.

The other problem is this. For it to be plausible that we can wellorder the universe by brute force we have to be sure that as long as we can pick α things for every $\alpha < \lambda$ then we can pick λ things. This is all right if λ is a successor ordinal: as long as there is something left after we have picked α things then we can pick an $(\alpha + 1)th$ thing. That's just straightforwardly true, and it's the argument we saw in the proof of theorem 1. Our realist intuitions get us this far, and this far they are correct. The problem is that this is not enough: we still have to consider the case when λ is limit, and then we need something that says that all the possible ways of picking α things for $\alpha < \lambda$ can be somehow stitched together. And for that one needs the axiom of choice. The point is that, at each successor stage the assertion "I can pick something" is just syntactic sugar for "there is still stuff left"; the difference between the two sounds substantial but it isn't. If one makes the successor step look *more* significant than it really is (by using syntactic sugar) then a side effect is that the difference between the successor stage and the limit stage is made to seem *less* significant than it really is.

We are back in exactly the situation we saw on page 14. Realism doesn't get you the axiom of choice: what it gets you is the right to tell the story on page 14 in beguilingly concrete terms. This argument for the axiom of choice derives all its plausibility by artfully concealing the assumption that *the infinite resembles the finite in the way required*. The italicised assumption turns out to be precisely the axiom of choice. This is not to say that the platonists are wrong when they claim that AC holds for their conception of set, merely that this story isn't an argument for it.

Finally here is something one can say to people who think the axiom of choice is true for sets. *Take very seriously the idea that there might be lots of datatypes of set; what you are currently thinking of as one datatype is in fact many.*. Is their concept of set the absolutely rock-bottom concept of `naked-set`? Or is it not perhaps one of the assorted richer datatypes of `decorated-set`? [decoration unspecified for the present] If there is a rock-bottom, minimalist type of `naked-set` then it is plausible that AC might fail for that type even if it holds for others, so the intuition that AC holds for sets might instead be an intuition about one of the datatypes of `decorated-set`. That's not to say that, of all the various concepts of set we need in mathematics, the rock-bottom concept of `naked-set` is the one that will loom largest in the thinking of mathematicians, but it does offer a way of representing the believers and the unbelievers as not actually disagreeing.

[1] An embedding of an uncountable wellordering into $\mathbb{R}$ would partition $\mathbb{R}$ into uncountably many half-open intervals, each of which would have to contain a rational. There aren't enough rationals to go round.

Does this belong in the other volume?

The Consistency of the Axiom of Choice?

Let us return to the idea that, if we have perfect information about sets, we can well-order them. This may be wrong-headed, but it does give rise to an idea for a consistency proof for the axiom of choice. Recall the recursive datatype WF: its sole constructor adds at each stage *arbitrary* sets of what has been constructed at earlier stages. If we modify the construction so that at each stage we add only those sets-of-what-has-been-constructed-so-far about which we have a great deal of information, then with luck we will end up with a model in which every set has a description of some sort, and in which we can distinguish socks *ad libitum*, and in which therefore the axiom of choice is true. This even gives rise to an axiom for set theory (due to Gödel) known as "$V = L$". $V = L$ is the axiom that asserts that every set is *constructible* in a sense to be made clear. No-one seriously advocates this as an axiom for set theory: none of the people who think that formulæ of set theory have truth-values believe that $V = L$ is true; it is taken rather as characterising an interesting subclass of the family of all models of set theory.

There are various weak versions of the axiom of choice that the reader will probably need to know about. **The axiom of countable choice** ("AC_ω") says that every countable set of (nonempty) sets has a choice function.

Both these versions are strictly weaker than full AC. DC seems to encapsulate as much of the axiom of choice as we need if we are to do Real Analysis—well, the minimal amount needed to do it sensibly. DC does not imply the various headline-grabbing pathologies like Vitali's construction of a nonmeasurable set of reals nor the Banach-Tasrki paradoxical decomposition of the sphere. There are also other weakened versions of AC, but these two are the only weak versions that get frequently adopted as axioms in their own right.

In this connection one might mention that people have advocated adopting as an axiom the *negation* of Vitali's result, so that we assume that every set of reals is measurable. Since this is consistent with DC we can adopt DC as well, and continue to do much of Real Analysis as before, but without some of the pathologies. Indeed one might even consider adopting as axioms broader principles that imply the negation of Vitali's result—such is the Axiom of Determinacy, However that is a topic far too advanced for an introductory text like this.

5.3.1 IBE and some counterexamples

Can we argue for AC by IBE? There is a *prima facie* problem in that there are some consequences of AC that people have objected to at one time or another. We have already mentioned Vitali's theorem that there is a non-measurable set of reals, and the more recent and striking Banach-Tarski paradox[2] on the decompositions of spheres. Nor should we forget that when Zermelo [23] in

[2]Q: What is a good anagram of 'Banach-Tarski'?
A: 'Banach-Tarski Banach-Tarski'.

1904 derived the wellordering theorem from AC the reaction was not entirely favourable: the wellordering of the reals was then felt, initially, to be as pathological as Banach-Tarski was later.

However, one can tell a consistent and unified story about why these aren't really problems for AC. There is, granted, a concept of set which finds these results unwelcome, but that concept is not the one that modern axiomatic set theory is trying to capture. The view of set theory that objects to the three results mentioned in the last paragraph is one that does not regard sets as fully extensional and arbitrary. How might it come about that one does not like the idea of a non-measurable set of reals, or a Banach-Tarski–style decomposition of the sphere, or a wellordering of the reals? What is it that is unsatisfactory about the set whose existence is being alleged in cases like these?[3] It's fairly clear that the problem is that the alleged sets are not in any obvious sense definable.[4] If you think that a set is not a mere naked extensional object but an extensional-object-with-a-description then you will find some of the consequences of AC distasteful. But this means that in terms of the historical process described in section **??** you are trapped at stage (2). Once you have achieved the enlightenment of stage (3) these concerns evaporate. Nowadays mathematicians are happy about *arbitrary* sets in the same way that they are happy about *arbitrary* reals.

Constructive Mathematicians do not like AC

There are communities that do not accept the axiom of choice, and the reasons they have are diverse.

One such community is the community of constructive mathematics. If one gets properly inside the constructive world view one can see that it requires us to repudiate the axiom of choice. However, getting properly inside the constructive world-view is not an undertaking for fainthearts, nor by any to be taken in hand lightly or unadvisedly, and it is not given to all of us to succeed in it. Fortunately for unbelievers there is a short-cut: it is possible to understand why constructivists do not like the law of excluded middle or the axiom of choice, and to understand this without taking the whole ideology of constructive mathematics on board. It comes in two steps.

First we deny excluded middle

First we illustrate why constructivists repudiate the law of excluded middle.

Some readers may already know the standard horror story about $\sqrt{2}^{\sqrt{2}}$. For those of you that don't—yet—here it is.

[3]The (graph of the) wellordering of the reals and the (collection of pieces in the) decomposition of the sphere are of course sets too.

[4]There is a very good reason for this, namely that there is no definable relation on $\mathbb{R}$ which provably wellorders $\mathbb{R}$. This theorem wasn't known in 1904 but people in 1904 could still realise that they didn't know of any wellorderings of $\mathbb{R}$.

Suppose you are given the challenge of finding two irrational numbers α and β auch that α^β is rational. It is in fact the case that both e and $log_e(2)$ are transcendental but this is not easy to prove. Is there an easier way in? Well, one thing every schoolchild knows is that $\sqrt{2}$ is irrational, so how about taking both α and β to be $\sqrt{2}$? This will work if $\sqrt{2}^{\sqrt{2}}$ is rational. Is it? As it happens, it isn't (but that, too, is hard to prove). If it isn't, then we take α to be $\sqrt{2}^{\sqrt{2}}$ (which we now believe to be irrational—had it been rational we would have taken the first horn) and take β to be $\sqrt{2}$.

α^β is now

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2$$

which is rational, as desired. However, we haven't met the challenge. We were asked to *find* a pair $\langle\alpha,\beta\rangle$ of irrationals such that α^β is rational, and we haven't found such a pair. We've proved that there *is* such a pair, and we have even narrowed the candidates down to a short list of two, but we haven't completed the job.[5]

What does this prove? It certainly doesn't straightforwardly show that the law of excluded middle is *false*; it does show that there are situations where you don't want to reason with it. There is a difference between proving that there is a widget, and actually getting your hands on the widget. Sometimes it matters, and if you happen to be in the kind of pickle where it matters, then you want to be careful about reasoning with excluded middle. But if it doesn't matter, then you can happily use excluded middle—or AC.

The Axiom of Choice implies Excluded Middle

In proving this we must play fair: the classical concept of *nonempty set* multifurcates into lots of constructively distinct properties. Constructively x is **nonempty** if $\neg(\forall y)(y \notin x)$; x is **inhabited** if $(\exists y)(y \in x)$, and these two properties are distinct constructively: the implication $(\neg\forall\phi \to \exists\neg\phi)$ is not good in general.

Clearly if every family of nonempty sets is to have a choice function then if x is nonempty we can find something in it, This would imply that every nonempty set is inhabited. We shall not resort to such smuggling. If we are to eschew smuggling we will have to adopt AC in the form that every set of *inhabited* sets has a choice function.

Let us assume AC in this form, and deduce excluded middle. Let p be an arbitrary expression; we will deduce $p \vee \neg p$. Consider the set $\{0,1\}$, and the equivalence relation $\sim$ defined by $x \sim y$ iff $x = y \vee p$. Next consider the quotient $\{0,1\}/\sim$. (The suspicious might wish to be told that this set is $\{x : (\exists y)((y = 0 \vee y = 1) \wedge (\forall z)(z \in x \longleftrightarrow z \sim y))\}$). This is an inhabited set of inhabited sets. Its members are the equivalence classes $[0]_\sim$ and $[1]_\sim$—which admittedly

[5] We can actually exhibit such a pair, and using only elementary methods, at the cost of a little bit more work. $log_2(3)$ is obviously irrational: $2^p \neq 3^q$ for any naturals p, q. $log_{\sqrt{2}}(3)$ is also irrational, being $2 \cdot log_2(3)$. Clearly $(\sqrt{2})^{(log_{\sqrt{2}}(3))} = 3$.

may or may not be the same thing—but they are at any rate inhabited. Since the quotient is an inhabited set of inhabited sets, it has a selection function f. We know that $[0]_\sim \subseteq \{0,1\}$ so certainly $(\forall x)(x \in [0]_\sim \to x = 0 \lor x = 1)$. Analogously we know that $[1]_\sim \subseteq \{0,1\}$ so certainly $(\forall x)(x \in [1]_\sim \to x = 0 \lor x = 1)$. So certainly $f([0]_\sim) = 0 \lor f([0]_\sim) = 1$ and $f([1]_\sim) = 0 \lor f([1]_\sim) = 1$. This gives us four possible combinations. $f([0]_\sim) = 1$ and $f([1]_\sim) = 0$ both imply $1 \sim 0$ and therefore p. That takes care of three possibilities; the remaining possibility is $f([0]) = 0 \land f([1]) = 1$. Since f is a function this tells us that $[0]_\sim \neq [1]_\sim$ so in this case $\neg p$. So we conclude $p \lor \neg p$.[6]

Observe, however, that if we define the family of N-finite sets recursively by:

> The empty set is N-finite;
> if X is N-finite and $x \notin X$ then $X \cup \{x\}$ is N-finite.

then we can prove by structural induction on the N-finite sets that every N-finite set of inhabited sets has a choice function.

There is a moral to be drawn from this: whether or not you want to include AC (or excluded middle) among your axioms depends at least in part on the use you are planning to put those axioms to. (This is of course a completely separate question from the question of whether or not AC (or excluded middle) is *true*).

Uplifting though this moral is, it is not the point that I was trying to make. The fact that AC implies excluded middle and that there are principled reasons sometimes to eschew excluded middle means that there are principled reasons for (sometimes) wishing to eschew the axiom of choice.

The difference between various forms becomes obscured. Countable choice is a very different beast from full choice.

- Analysis without AC_ω is a disaster area. Analysis without full AC but with AC_ω is a very interesting prospect, particularly if we add nice things like LM—there are even people who advocate it; (Imre says that all such people are logicians);

- WQO theory without countable choice is a train-wreck—but very very few theorems in WQO theory need full choice;

- NF refutes full choice but doesn't seem to refute AC_ω (Not sure about the various choice-contradicting nice conditions on models of TZT);

- We need AC_ω to identify the two definitions of wellfoundedness—and thereby to make sense of games of finite length. Games of length ω are supertasks.

- Don't we need AC_ω to do forcing?

[6] Thanks to Douglas Bridges for the right steer on this exercise! The theorem is due to Diaconescu [2].

Skolemisation and Choice

This is an important topic, and there is an extensive technical literature on it. A good place for the determined interested reader to start would be `https://plato.stanford.edu/entries/epsilon-calculus/`

Let $\phi(,)$ be a binary relation such that $(\forall x)(\exists y)\phi(x, y)$. A skolem function for ϕ is a function f such that $(\forall x)\phi(x, f(x))$. The assertion that for any such ϕ we can find a skolem function does look very much like an application of the axiom of choice. Remarkably one does not need the axiom of choice if one wishes to pretend that such ϕ have Skolem functions. What is going on is this. Suppose T is a first-order theory in $\mathcal{L}(\phi)$, the language that contains the expression ϕ, and $T \vdash (\forall x)(\exists y)\phi(x, y)$. Suppose further that we expand $\mathcal{L}(\phi)$ by adding a symbol 'f' and an axiom $(\forall x)\phi(x, f(x))$, giving us a new theory T' in the expanded language. Then T' is consistent if T is, and there is no use of the axiom of choice in the proof!

Sadly the matter involves some fairly technical logic (proof theory in particular) and is probably not to the taste of most readers of this book. However clarification cannot be evaded altogether, because the thoughtful reader will immediately want to apply this relative consistency result to the "countable union of countable sets is countable" situation. Let us suppose we are reasoning in some theory T that empowers us to perform certain manipulations on sets. Let $\{X_i : i \in \mathbb{N}\}$ be a counted family of countable sets. Saying that the X_i are all countable is to say that $(\forall i)$(there is a counting of X_i). But then we can consistently suppose that there is a Skolem function f sending each i to a counting of X_i, and we can use f in the zigzag construction to obtain a counting of the union. What's not to like? What's not to like is that the authorisations T gave us to do whatever-it-was that it authorises do not extend to manipulating f since f is not mentioned in the language that T lives in.

Say something about skolemisation in resolution proofs in first-order logic!

5.4 Some thoughts about certificates

My point of departure is the idea of a recursive datatype or *rectype* for short. A rectype has *founders* and is built up by *constructors*. All the usual examples are **free** in the sense that each object in the rectype is denoted by a unique word in the constructors. Examples are the natural numbers, or lists and trees. Such rectypes are always initial objects in a suitable category. Computer scientists, for obvious reasons, tend to be interested only in rectypes of **finite character**: finitely many founders and finitely many constructors each of finite arity. However there is no mathematical reason not to consider rectypes of infinite character, and the cumulative hierarchy of sets is a natural example. It has no founders at all, and has one constructor—`set-of`—of unbounded arity. This is a free rectype and is well-behaved.

slight change here

So, thus far, we have two parameters with which we classify rectypes. They may be of finite character vs infinite character, and they may be free *vs* not-free.

	Free	Not Free
Finite Character	The naturals lists, trees	?? ??
Infinite Character	The cumulative hierarchy of sets	The ordinals

Need to fill in the question marks.

Next I need the idea of a *certificate* or *proof*. If you are a member of a rectype there is always a good reason for you to be, and a certificate-or-proof is that reason—presented as a mathematical object. If the rectype is free (so it's an initial object in a suitable category) every object in it has a unique certificate. If the rectype is not free there may be a multiplicity of certificates. (Or there may even be none, as we shall see). Notice that even if the rectype R is not free, the rectype of certificates-for-R is always free. Perhaps I should be a bit more explicit about what a certificate is to be. A certificate-that-x-belongs-to-the-rectype is: the constructor used in the last step in the construction of x, together with a list of arguments to that constructor, with certificates for each of those arguments. So a certificate is a word in the constructors and founders. And the family of certificates for a rectype is another rectype—indeed a free rectype.

Now we need a slightly finer distinction, within the family of rectypes of infinite character. Specifically I shall be interested in the following rectypes.

1. The collection of wellfounded hereditarily countable sets. The single constructor is countable-set-of. This collection is often called HC[7];

2. The rectype whose founder is the ordinal number 0, with constructors `successor` and `sup-of-`ω`-sequence-of`. This is a substructure of the ordinals;

3. The rectype whose founders are all the countable sets, and whose constructor is `union-of-countable-set-of`;

4. The rectype whose founders are all the ω-sequences and whose constructor is ω`-sequence of`;

5. The cumulative hierarchy of sets.

(1), (4) and (5) are free. (2) and (3) are not.

Now any rectype admits a wellfounded quasiorder which in my introductory book [5] "Logic Induction and Sets" I call the **engendering relation**, and which is the transitive closure of the relation that x bears to each of things it is immediately constructed from. For example, in $\mathbb{N}$ the engendering relation is $<$. (I am a bit worried by the fact that there doesn't seem to be a standard name for this engendering relation in the literature .... If one isn't needed, when I think it is, then I must have misunderstood something very badly). The engendering relation is wellfounded, and has a canonical rank function, which is

[7] I prefer '$H_{\aleph_1}$'

a map to the ordinals, whereby the rank of any object in the rectype is the least ordinal bigger than the ranks of all the things that bear the engendering relation to it. In case (5) the rectype rank is literally the same as the set-theoretic rank.

Now let's think about free rectypes of infinite character, but *bounded* character, so their constructors have bounded appetites.

Jech [9] has a wonderful theorem that says that every set in HC has rank less than ω_2. It's very important that the proof does not use AC at all. It exploits the fact that the rectype HC is free: each object has a unique certificate. I think that in general Jech's theorem shows that in any free rectype of countable character every object must have rank $< \omega_2$.

The freeness is important here. It is a theorem of Gitik [6] that the rectype (2) can contain all ordinals.

There is another result that is useful in this connection. I noticed it myself, but i'm sure it's folklore. If AC_ω holds, then $|HC| = 2^{\aleph_0}$. In a sense this isn't really the theorem; the theorem that underlies it goes like this:

Each of these rectypes is the least fixed point for a suitably chosen operation $\mathcal{O}$. So if you can find another fixed point ("pick a fixed point, any fixed point"!) or even something x with $|x| = |\mathcal{O}(x)|$ you should be able to embed the rectype in it and thereby bound its size. (There's a certain amount of small print to this: not all of which have I checked). Consider not HC but the rectype (3). The reals is the same size as the set of ω-sequences of reals. That means that we can define by recursion on the rectype (3) an injection into the reals. We need the freeness of (3) to get an *in*jection. If we can choose a certificate for each hereditarily countable set then we can embed HC into the reals. Hence the fact that $|HC| = 2^{\aleph_0}$.

I don't think this depends on special properties of countable sets; i think Jech's argument can be generalised to apply to all free rectypes of bounded character. I think it will say something like: if κ is an aleph then in any free rectype generated by fewer than κ founders and fewer than κ constructors each of arity less than κ every object has rank $< \kappa^{++}$ and the rectype itself is of power 2^κ. Something like that, anyway.

Moral: every free rectype of *bounded* character is a set. and by Jech's argument we have tight control of the ranks of the ordinals used.

But what about the non-free rectypes? One would expect that even in a non-free rectype every object should have a certificate. How could this not be true? Since everything in the rectype is there for a good reason, there must be a good reason one can point to. Although this is true for rectypes of finite character it appears not to be straightforwardly true for rectypes of infinite character. It seems that unless we assume AC we have no reason to suppose that a rectype of infinite character is a projection (in the obvious way) of its rectype of certificates. For example, in the model of Gitik's where every limit ordinal has cofinality ω the rectype (2) generated from 0 by `succ` and ω-sups contains all ordinals, and the rectype of certificates for it is a free rectype of countable character, so every certificate has rank $< \omega_2$. In those circumstances we cannot rely on ordinals beyond ω_2 having certificates.

Free rectypes of infinite bounded character are well-behaved, but we need

AC to show that every infinite rectype is a surjective image of a free one. So in the absence of AC the task of establishing the sethood of a non-free rectype of infinitary-but-bounded character is nontrivial. For example in NF we do not know if the rectype (2) is the universe. And this despite the fact that we know that not every set can be a projection of a member of rectype (3).

Presumably AC is equivalent to the assertion that every rectype is a surjective image of its rectype of certificates.

So I think my questions to you are along the lines: (i) how much of this is known? Can I improve bits of it by expressing it in a more category-theoretic way..? Any helpful comments gratefully received...

Dear Thomas,

Thanks for your "Letter to Jamie". If I've understood it correctly, an answer is this:

Note that AC in the category of sets is that every surjection has a right inverse. I.e. if $f : A \to B$ then there exists a $g : B \to A$ such that $f \circ g : B \to B$ is the identity.

There's a powerful theory of initial algebras which gives functions from free objects (essentially, your certificates) to other objects (your non-free rectypes). AC implies (and almost certainly is equivalent with) the property that every one of these functions has a right inverse.

So what you describe probably can all be expressed in categorical language. I think what you've written amounts to observing (correctly or falsely I cannot judge off-the-cuff) that in the category of sets without AC, there are certain functions which do not have initial algebras, but they do have initial algebras in the category of sets with AC. This makes sense; in the category of sets without AC there are simply fewer functions!

There's one little niggling thing. An object in the category of sets is a set because it's an object in the category of sets. You might have to set up two categories; a category of sets ("small things") and a category of collections ("big things").

Dear Thomas,

FYI here's the page about the axiom of choice in Set (the category of sets)

`http://books.google.co.uk/books?id=KaXmMjwBulgC&pg=PA17&lpg=PA17&dq=axiom+of+choice+epi+split+epi&source=web&ots=kuyJgzb9_v&sig=UJdRbYAOHZVXbzxiYjWE9pXnxwY&hl=en&sa=X&oi=book_result&resnum=4&ct=result`

Excellent. Thanks *very* much. Now the next thing I need to know is what an initial algebra is, so that I can say all this stuff in talk like that of the bi-coloured python rock-snake. You should not feel obliged to tell me. It's my responsibility to inform myself!

You can read about initial algebras almost anywhere. I'd expect explanations to be in Saunders MacLane's book "Categories for the working mathematician", or Paul Taylor's book "Practical Foundations of Mathematics".

Here's a resume: * A *functor* is, basically, a function-class F from sets to sets.

* The *functor category* over F is, basically, the class $\bigcup_X FX \to X(X$ ranges over sets, $\to$ is function-sets).

* An *initial algebra* is a function $f \in FZ \to Z$ for some Z, such that f and Z inject into every other g and X in the functor category in a suitable sense (think of Z injecting into X such that g restricts to f on the image of the injection). In a suitably generalised sense, the initial algebra is the intersection of (initial element amongst) all objects in the functor category.

Jamie

5.4.1 AC and Certification

Blend these two sections properly

Once we have taken on board the rôle played the concept of *datatype* in explaining the difference between the theorem that needs choice and the theorem that does not need choice, one can see that the axiom of choice weaves its magic by showing how, when we are given an object of one datatype (a `naked set` that happens to be countable), we can see it as a reduct of an object of the richer datatype `counted set`.

The next step after consciously acknowledging that mathematical objects typically and usefully have identifiable datatypes is the step of thinking of those datatypes as mathematical objects themselves. When we do this we find another rôle for the axiom of choice.

Let us help ourselves to the concept of *certificate*. It is useful primarily in connection with recursive datatypes [. . .] but it is actually slightly more general.

A certificate that a particular object is a member of a particular datatype is something that will convince a skeptical reader that the object in question is, indeed, an object of the datatype it is alleged to belong to. If we want to set up a subtype of `naked-set` called `countable-naked-set` a certificate for an object of that type would be a counting of it. Similarly, a certificate for a counted set X is a counting of X. This makes it sound as if the two types `counted-set` and `countable-set` are the same, but they aren't, and the certificate-talk gives us a way of illustrating the difference. If x is a `counted-set`, the certificate that x is so is part of the object x; if x is `countable-set` it isn't. A `countable-set` is a `naked-set` that *could* be expanded by decorating it with a counting (and that counting is a certificate that it is of type `countable-set`), but it remains a `naked-set` and the counting is not a part of it—it hovers around attentively but is not part of the kit; in contrast a `counted-set` is a `naked-set` *that has been* expanded by decorating it with a counting. . . and that counting is a certificate that the expanded object—of which it is a part—is of type `counted-set`).

Clearly objects of either of these types have certificates.

Now consider the datatype

`set-that-is-a-union-of-countably-many-countable-sets`.

It is a subtype of the type `naked-set`. Let's call this type `C` for short. A certificate that an object X really is of type `C` must be a counted set $\{\langle C_i, X_i\rangle : i \in \mathbb{N}\}$

of pairs where each X_i is a countable set with C_i a counting of it, such that $\bigcup_{i \in \mathbb{N}} X_i = X$.[8]

Now this certificate will give rise to a counting of X, by means of the zigzag construction on the C_i. So if every object of type `C` has a certificate it follows that a union of countably many countable sets is always countable, so every element of `C` is actually countable.

There are two more illustrations, slightly less unnatural. There is $H_{\aleph_1}$, the (wellfounded) hereditarily countable sets, aka HC; there is also the class of hereditarily wellordered sets.

A certificate that x is a member of HC is a counted subset X of HC s.t. $X = \bigcup X$, equipped with a function that assigns to each $y \in x$ a certificate that $y \in$ HC.

Remark 2 *If every element of HC has a certificate then every member of HC has a countable transitive closure.*

Proof: By induction on set-theoretic rank. ■

The significant feature common to all these cases is of course the fact that these rectypes are not free. Explain freeness

Thus, existence of certificates implies choice principles! Consideration of other, more complex datatypes will show [i think!] that the principle "for every datatype, every object of that datatype has a certificate" will imply full AC. AC should follow from the assertion that there is a global function assigning to each hereditarily wellordered set a wellordering of it. First step would be to show that AC follows from the assertion that there is a function assigning to each wellordered set a wellordering of it.

H I A T U S

Dependent Choice

You need to be clear about what you are picking *from*. You can go on picking from a set as often as you like—through all the ordinals, even—as long as you don't remove them once you've picked them. After all, there's nothing wrong with a function from a wellordered set X to a set Y! If you remove your chosen element each time (so you pick a different member of X every time) then you are constructing a wellordered subset of X, and of course the size of any such subset is bounded by $|X|$.

"But" (i can hear the reader exclaiming) "the second choice is made from a set that is *different* from the first set!" If the first set is X, and x is chosen from it then the second choice is made from $X \setminus \{x\}$. This leads us to principles of *dependent* choice, where the set on which the choice fuunction is being defined has some structure that arises from the choice function itself.

But this has no bearing on the axiom of choice, because AC talks about making choices from lots of *different* sets.

[8] Or perhaps just a countable set of such certificates. . . ?

5.5 Leftovers

There is the point that the counterexamples to AC are things that it's impossible to describe completely, simply beco's of the order structure built into our language.

That is to say, the negation of AC is a sort-of self-refuting sentence like "I can't say 'breakfast"' which cannot be true if uttered and "It is raining and I do not believe it" which cannot be true if believed by the speaker. $\neg$AC resembles them in that the point is not that it can't be true, it's that it cannot be understood—or perhaps that if understood cannot be believed.

H I A T U S

It might be claimed the picture above misrepresents the thought processes of the people who think that the axiom of choice is obvious. Yes—it will be admitted—there is a danger of a fallacy of equivocation as sketched above, but the argument for choice relies on the cases where it is provable. It's a different kind of IBE: the reason why we can prove all these instances of the axiom of choice is simply that the axiom of choice is true. We can't prove that the set of socks is wellordered but that's only because we have not been given enough information about it. Any set about which we know enough reveals itself—under the close examination that we are able to give it—to be wellordered. Why is this? Is this just coincidence on a cosmic scale? Of course not! There is a simple explanation: the truth of the axiom of choice.

However this line of talk isn't really supported by the data. Not all observed sets are observed to be wellordered. Some sets provably have selection functions: the power set of the naturals for example. But some don't *provably* have them: the power set of $\mathbb{R}$ for example. (One could try claiming that the power set of the reals is not observable in the relevant sense, but since the only reason for arguing this is that it fails to support this argument, this would be too obviously circular for most tastes).

What is the correct concept of "observable" here? (We obviously don't mean *literally* "observable"! (It's worth thinking about whether or not the only things that are observable in the relevant sense are things that have enough order structure: you perforce wellorder a set in the course of observing it.)

We might mean something like

observed-to-be-ϕ = provably ϕ

observable set = definable set

Clearly we are thinking here of sets-in-intension, or descriptions of sets. Perhaps we can here put to good use the expression from possible-world rhetoric. 'V_ω' is a **rigid designator** (it denotes the same thing in all standard models); '$\mathbb{R}$' is not.

So what precisely is the general observation whose truth is to explained by the axiom of choice? It's not the fact that every observable set is known to be wellordered, since that is not a fact. Nor is it the fact that every definable set can consistently be wellordered, since AC would explain a lot more than that, and Inference to the *Best* Explanation would point us not at AC itself but rather at *the statement that AC is consistent*. Sadly that last observation is something we already know and don't need any arguments for. If we want an argument for AC we won't find it here.

The argument isn't really IBE at all (in contrast to the genuine IBE argument used for replacement, for example) but is a kind of induction by simple enumeration, or whatever is the argument that we use to refute the scepticism that says that unobserved objects might suddenly go out of existence, or misbehave in other ways, like the unobserved wallpaper in the drawing room of the magician Mr. Leakey in J. B. S. Haldane's childrens' book. My Friend Mr Leakey Puffin Books 1944

This is an attempt to tar with a radical sceptic's brush the people who say that you know AC to hold only for sets (finite, definable etc) for which you have privileged information. All observed sets are wellordered, so all unobserved sets are wellordered too.

(Is ther a parallel here with attempts to prove that all emeralds are grue?)

There is a problem with arguments for the truth or falsity of set theoretic axioms. It is fairly general, but we can illustrate it here with the axiom of choice, since that is the axiom under discussion.

If you believe that the axiom of choice is the kind of thing that has a truth-value then you probably believe that it is noncontingent. If it's true it's necessarily true and if it's false it's necessarily false. If you have house room for such ideas of metaphysical neccessity then you probably try to capture them by talk about possible worlds. Conveniently there are obvious candidates for the possible worlds we would use to explain the necessary truth or necessary falsehood of AC, namely models of set theory, or perhaps *standard* models of set theory only. This terminology also gives us vocabulary to say things like " 'V_ω' is a rigid designator" and " '$\mathbb{R}$' is not a rigid designator" which (if our possible worlds are standard models) enable us to capture some things that set theorists recognise as facts.

How inconvenient it is, therefore, that on this account AC turns out to be true in some possible worlds and false in some others, and therefore not to be noncontingent after all. Not only that, but we don't know which of these models is the actual world, so we have no idea whether it is true *simpliciter* or not.

Clearly there is some explaining to be done

Can we argue that it is false? Argument to the effect that if it were true then counterexamples would be unimaginable?

OK, even if we cannot argue that the axiom of choice is true (at least by arguments like this) is there nevertheless a case to be made for adopting it as an axiom? (You would have reached this stage long ago if you had never been that kind of realist and never believed you had any epistemic access to arbitrary infinite extensional objects).

What are the pros and cons? On the pro side is the point that it makes the arbitrary infinite extensional objects behave like the cuddly familiar, nonarbitrary finite ones and thereby makes the world a tidy place. (Well, there is still this fact about $\mathbb{R}$ but believers in AC are greedy) It is true that $\mathbb{R}$ is not naturally wellordered, but if anything this is a point in AC's favour, since by wellordering $\mathbb{R}$ it gives us another way of reasoning about $\mathbb{R}$ and proving things about it.

On the con side is the fact that models in which every set of reals is measurable are quite cute in various ways.

I want to make a connection here with what i was telling you in the first lecture about the three stages entities go through on their way to becoming mathematical objects. We have noted that AC for *finite* objects is true. So it's only *infinite* objects we are ever going to get our knickers in a twist about. And we didn't start manipulating/calculating-with infinite objects until the days of Cantor and Dedekind. At the earliest stages of this process the infinite objects we had to deal with were all naturally motivated, naturally occurring, objects with enough internal structure—so we find that all the instances of AC that we wanted were true. Well, almost all of them: $\mathbb{R}$ has no definable wellordering as we have seen.

What this means is that, with hindsight, we should have expected people to notice that they needed the Axiom of Choice as an extra principle at precisely that stage when they started reasoning about/calculating-with *arbitrary infinite objects-in-extension*. And this is indeed exactly what happened.

Let's take an example: Vitali's construction of a non-measurable set. This could only arise once one had the concept of an arbitrary set of reals.

So if you only ever deal with finite sets and sets with enough internal structure you will hardly ever encounter one that doesn't come ready wellordered, and the issue doesn't arise. The question about whether or not AC is *true* can arise for you only if you are a realist about arbitrary infinite extensional objects.

Tie together Grue emeralds with expansion and self-refutation connect with Berkeley

AC and regimentation. No accident that you use BPI to prove a representation theorem

AC implies the existence of God

[12] One direction: God implies Choice, since if God existed, it would be possible to construct a choice set for each set, since God could just think about it for a bit and do the choosing, being omnipotent and all. The other direction: take a causal sequence - by Zorn's lemma (an equiv. of Choice), it will have a unique first member. Thus we have a cosmological argument which establishes a First Cause. (God, of course).

Another example of people using AC when they don't need to.

How do you prove that there is no subset of $\mathbb{R}$ that is of order-type ω_1 in the inherited order? Suppose there were such a set, X. Then $\mathbb{R} \setminus X$ is partitioned into open intervals, each of which must contain a rational, so pick a rational from each one, using AC. Then we have an uncountable set of rationals, which is impossible. (I have actually had students say this to me). But AC is not needed: since $\mathbb{Q}$ is countable we can (one choice!) pick an enumeration of it and select the first rational in each interval according to that enumeration.

Connect with logic-and-rhetoric the point that: just beco's the p i am telling you about isn't (as it happens) going to be a problem for you (beco's of your choice of pathway) it doesn't follow that p wasn't true!

Be sure to find some rude things to say about axioms of plenitude. What is an axiom of plenitude anyway? What is an axiom of restriction, a *Beschrükheitsaxiom*?

Conversation with Peter Smith 7/iii/2018

EXplain propetly why it was only after we acquired the idea of arbitrary set/function-in-extension that AC could blow up in our faces (B-T)

It's beco's of the belief that the infinite resembles the finite that they believe AC. All else is post-hoc rationalisation.

A case where you don't need Ac but use it anyway: can't embed the second number class into $\mathbb{R}$

Look up traffic on stackexchange

Talk about skolem functions?

If $\sim$ is a congruence relation for an infinitary [total] operation f then in general you need AC to show that f is total on the quotient. Two examples:
(i) Infinitary sums of cardinals and ordinals—"multiplicative" axiom!
(ii) The Cauchy reals are order-complete. (perhaps we can do this without choice)
(iii) Also power set axiom in APG models

Even if God can wellorder $\mathbb{R}$, you can't. A bit like the cigarette addict: "Look, i can quit whenever i choose". Maybe you can-in-principle, but you don't know how to!

There are natural examples where you can't *just keep buggering on*. There are games where Player II can choose to stay alive for n steps, for any n, but is doomed to lose sooner or later.

The fact that WF is rigid sets you up for AC, because the existence of a definable wellorder of V enforces rigidity.

5.6 Chapter on AC lifted from vol 1

To properly understand AC we need the notion of **discrete transfinite process**. Wossat? Let's start with a nice example. Cantor derived set intersections at limits. Reach a set with no isolated points.

Cantor's construction is nice in two ways: it is *monotone* and it is *deterministic*. It is monotone in the sense that nothing that is taken away is ever put back. One could say that, thought of as a function from dates/times (or ordinals) to sets (or rather sets-"opposite") it obeys $t_1 \leq t_2 \rightarrow f(t_1) \leq f(t_2)$. It is *deterministic* in the sense that the person executing the process never has to make a choice about which points to remove next. Processes like this that are deterministic and monotone can be unproblematically executed. If they have a termination condition they will terminate. That is the extra–set-theoretical meaning of the lemma of Hartogs' that says that for every set X there is a von Neumann ordinal that will not inject into X: *if a monotone deterministic process ever fails to terminate properly it's not because you have run out of ordinals.* It may crash for other reasons of course: the thing you are trying to construct might not exist, for example.

[Consider the project to find an set equal to its power set, in ZF, using Bourbaki-Witt. It fails, and you run out of ordinals, but *that's not why it fails*: it fails beco's of unstratified separation.

Try doing it in NF. It fails beco's the recursion is unstratified and cannot be executed.]

If we discard monotonicity we find ourselves contemplating processes that it is possible to worry about. *Thompson's Lamp* (see [20]) is the following puzzle. At time $t = 0$ the lamp is off. At time $t = 1/2$ it is switched on, at time $t = 3/4$ it is switched off, then on again at time $t = 7/8$ and so on. (Notice that this is deterministic). The puzzle then is: what is the state of the lamp at time $t = 1$? The problem is supposed to be that there are compelling reasons to believe that it cannot be on (because every time it is switched on before time $t = 1$ it is subsequently switched off) and similarly it cannot be off. There is no problem, *really* because of course the state of the lamp at time $t = 1$ is simply *undetermined* by its states are earlier times. And this is because the function from time to states-of-the-lamp is—in an obvious sense—not monotone.

What sort of situation do we find ourselves in if we drop determinism (while keeping monotonicity)? Let $\mathcal{X} = \{X_i : i \in \mathbb{N}\}$ be a family of nonempty sets. Let us consider the project of picking one member from each X_i, with a view to obtaining a function $f : \mathbb{N} \rightarrow \bigcup \mathcal{X}$ satisfying $f(i) \in X_i$ for all $i \in \mathbb{N}$. The discrete transfinite process before us is pretty straightforward: examine the X_i in turn, starting at X_0, and pick a member from each—which we can do because (by assumption) they are all nonempty. This process is nondeterministic because (except in the trivial case where the X_i are all singletons, which I should have excluded at the outset!) there is more than one thing we can pick. It's also clear that it is monotone—at least in the sense that, as we go along, we are building a function (a set of ordered pairs) and we add ordered pairs to this function (so that at stage n we have n pairs, all of the form $\langle X_i, x_i \rangle$ with $x_i \in X_i$) and we never remove any pairs. So the process is monotone and nondeterministic. Can it be completed?

The first point to make is that the elementary set-theoretic apparatus we have used in persuading ourselves that the process can be run successfully for n steps (for every $n \in \mathbb{N}$) is not enough by itself to prove that the process can be completed. "The process can be completed" simply does not follow from the fact that it can be run for n steps for every n. This piece of news will be shocking to many readers, but it really is so. A proof can be found in section

?? below.

The people who will be shocked are the people who say, in pained voices "Why can I not just keep going?". The best response to this is probably another question "How do you propose to do that?" or "What is it that counts as keeping-going?". These people do not realise there is a problem, and this is because they are overlooking the huge difference between deterministic transfinite processes and nondeterministic transfinite processes. If the process is deterministic then you can, indeed, just "keep going". If the process is nondeterministic then the various bits-of-processes between which you are undetermined have to cohere.

What one needs is a kind of coherence principle, something that says that all the finite partial functions can be glued together to obtain an infinite (total) function.

Chapter 6

Appendices etc etc

6.1 Glossary

Wellordering
performative
Contrastive explanation

Bibliography

[1] Peter Clark and Stephen Read "Hypertasks" Synthèse **61** (1984) pp 387–90.

[2] Radu Diaconescu, "Axiom of Choice and Complementation". Proc. AMS **51** (1975) 176–178.

[3] Forster, T. E. "Reasoning about Theoretical Entities". Advances in Logic vol. 3 World Scientific (UK)/Imperial College Press 2003.

[4] Forster, T. E. "The Axiom of Choice and Inference to the Best Explanation". *Logique et Analyse* **194**, 2006 pp 191–197.

[5] Forster, T. E. "Logic, Induction and Sets", LMS undergraduate texts in Mathematics **56** Cambridge University Press.

[6] Gitik, Moshe. All uncountable cardinals can be singular. Israel J of Mathmatics **35**

[7] Nelson Goodman "Fact, Fiction and Forecast"

[8] Horst Herrlich "The Axiom of Choice". Springer Lecture Notes in Mathematics **1876**.

[9] Jech, Thomas. On Hereditarily countable sets. JSL **47** (1982) pp. 43-47

[10] Peter Lipton. "Inference to the best explanation" (second edition) International library of Philosophy, Routledge 2004

[11] J. E. Littlewood "A Mathematician's Miscellany" Revised edition ed Bollobás, Cambridge University Press 1986

[12] Robert K. Meyer "God exists!", Nous **21** (1987), pp 345–361.

[13] Moore, Gregory H. "Zermelo's Axiom of Choice". Studies in the History of Mathematics and Physical Sciences **8**, Springer 1980.

[14] Herman Rubin and Jean E. Rubin. "Equivalents of the Axiom of Choice. II", Studies in Logic and the Foundations of Mathematics, volume 116. North-Holland Publishing Co., Amsterdam, 1985.

[15] Quine, W.V. Mathematical Logic (revised edition) Harper torchbooks 1962

[16] Russell, B. A. W., "*Introduction to Mathematical Philosophy*" Routledge, 1919.

[17] Russell, B. A. W., and Whitehead, A. N, "*Principia Mathematica*" Cambridge University Press 1910.

[18] Rickless, Samuel C., Berkeley's Argument for Idealism OUP 2013. ISBN 978-0-19-966942-4

[19] Peter M. Schuster. "Countable choice as a questionable Uniformity principle". Philosophia Mathematica **12** (2004) pp 106–134.

[20] J.M. Thompson. "Tasks and super-tasks". *Analysis* **15** (1954) pp 1–13.

[21] Jean van Heijenoort: "From Frege to Gödel: A source Book in Mathematical Logic, 1979-1931". Harvard University Press 1967.

[22] Timothy Williamson. Converse Relations. The Philosophical Review, Vol. 94, No. 2 (Apr., 1985), pp. 249-262

[23] Zermelo, E. "Proof that every set can be wellordered". in van Heijenoort [21] pp 199–215.