Logic and Set Theory: Prof Leader's Example Sheets for 21/22

Thomas Forster

March 7, 2022

Think of these notes as *discussions* rather than model answers.

The marzipan pig  means that the theorem or exercise so decorated is extremely tasty. I have tried to decorate extremely dangerous questions with a skull-and-crossbones, as in the margin

but i havent found a way of getting it in line. The LaTeX package for doing that buggers up the mathematical fonts, so i can't use it. The Usual Bribes are on offer for any LaTeX code for skull and crossbones. Your fellow students will thank you for the warnings.

Qiaochu Yuan (may he live for ever) is responsible for some of these answers

Sheet 1

Question 1

Which of the following propositions are tautologies?

(i) $(p_1 \to (p_2 \to p_3)) \to (p_2 \to (p_1 \to p_3))$

(ii) $((p_1 \vee p_2) \wedge (p_1 \vee p_3)) \to (p_2 \vee p_3)$

(iii) $(p_1 \to (\neg p_2)) \to (p_2 \to (\neg p_1))$

(i)

Suppose that the proposition evaluates to 0 under some valuation ν. Then $\nu(p_1 \to (p_2 \to p_3)) = 1$ and $\nu(p_2 \to (p_1 \to p_3)) = 0$, whence $\nu(p_2) = 1, \nu(p_1 \to p_3) = 0$, whence $\nu(p_1) = 1, \nu(p_3) = 0$. It follows that $\nu(p_2 \to p_3) = 0$, whence finally $\nu(p_1 \to (p_2 \to p_3)) = 0$; contradiction. So the proposition is a tautology.

(ii)

Let $\nu(p_1) = 1, \nu(p_2) = \nu(p_3) = 0$. Then $\nu(p_2 \vee p_3) = 0, \nu(p_1 \vee p_2) = 1, \nu(p_1 \vee p_3) = 1$, whence $\nu((p_1 \vee p_2) \wedge (p_1 \vee p_3)) = 1$ and

$$\nu(((p_1 \vee p_2) \wedge (p_1 \vee p_3)) \to (p_2 \vee p_3)) = 0.$$

(iii)

Suppose that the proposition evaluates to 0 under some valuation ν. Then $\nu(p_1 \to (\neg p_2)) = 1$ and $\nu(p_2 \to (\neg p_1)) = 0$, whence $\nu(p_2) = 1, \nu(\neg p_1) = 0, \nu(p_1) = 1$. But this implies $\nu(p_1 \to (\neg p_2)) = 0$; contradiction. So the proposition is a tautology.

This is not a proper question, more a reality check.

Question 2

Write down a proof of $(\perp \to q)$ in the propositional calculus

[PTJ sez (inter alia) *The fact that $\{\neg p\} \vdash (p \to q)$ is needed in the proof of the Completeness Theorem.*]

QY supplies this proof.

By the deduction theorem, it suffices to show that $\perp \vdash q$. The following is a proof:

t_1	$\perp$	(in S)
t_2	$\perp \to ((q \to \perp) \to \perp)$	K
t_3	$(q \to \perp) \to \perp$	(modus ponens from t_1, t_2)
t_4	$((q \to \perp) \to \perp) \to q$	(axiom 3)
t_5	q	(modus ponens from t_3, t_4)

Then by the proof of the deduction theorem, the following is a proof that $\perp \to q$:

1	$\perp \to (\perp \to \perp)$	K
2	$\perp \to ((\perp \to \perp) \to \perp)$	K
3	$(\perp \to ((\perp \to \perp) \to \perp)) \to ((\perp \to (\perp \to \perp)) \to (\perp \to \perp))$	S
4	$(\perp \to (\perp \to \perp)) \to (\perp \to \perp))$	(modus ponens from 2,3)
5	$\perp \to t_1$	(modus ponens from 1, 4)
6	t_2	K
7	$t_2 \to (\perp \to t_2)$	K
8	$\perp \to t_2$	(modus ponens from 6, 7)
9	$(\perp \to t_2) \to ((\perp \to t_1) \to (\perp \to t_3))$	S
10	$(\perp \to t_1) \to (\perp \to t_3)$	(modus ponens from 8, 9)
11	$\perp \to t_3$	(modus ponens from 5, 10)
12	t_4	(axiom 3)
13	$t_4 \to (\perp \to t_4)$	K
14	$\perp \to t_4$	(modus ponens from 12, 13)
15	$(\perp \to t_4) \to ((\perp \to t_3) \to (\perp \to t_5))$	S
16	$(\perp \to t_3) \to (\perp \to t_5)$	(modus ponens from 14, 15)
17	$\perp \to t_5$	(modus ponens from 11, 16).

Question 3

We want to show that $p \vdash (p \to \perp) \to \perp$. By the deduction theorem, it suffices to show that $\{p,\ p \to \perp\} \vdash \perp$. But this follows by *modus ponens*.

Question 4

We want to show that $\{p, q\} \vdash (p \to (q \to \perp)) \to \perp$.

(i) By the deduction theorem, it suffices to show that $\{p,\ q,\ p \to (q \to \perp)\} \vdash \perp$. But this follows by two applications of *modus ponens*.

(ii) By the completeness theorem, it suffices to consider a valuation ν with $\nu(p) = \nu(q) = 1$. Then $\nu(q \to \perp) = 0$, whence $\nu(p \to (q \to \perp)) = 0$, from which it follows that $\nu((p \to (q \to \perp)) \to \perp) = 1$.

(iii) By the proof of the deduction theorem, the following is a proof that $\{p, q\} \vdash p \wedge q$, where $x = (p \to (q \to \perp))$:

(1)	$x \to (x \to x)$	K
(2)	$x \to ((x \to x) \to x)$	K
(3)	$(x \to ((x \to x) \to x)) \to ((x \to (x \to x)) \to (x \to x))$	S
(4)	$(x \to (x \to x)) \to (x \to x))$	(modus ponens from 2,3)

(5) $x \to x$ (modus ponens from 1, 4)
(6) p (in S)
(7) $p \to (x \to p)$ K
(8) $x \to p$ (modus ponens from 6, 7)
(9) q (in S)
(10) $q \to (x \to q)$ K
(11) $x \to q$ (modus ponens from 9, 10)
(12) $(x \to x) \to ((x \to p) \to (x \to (q \to \perp)))$ S
(13) $(x \to p) \to (x \to (q \to \perp))$ (modus ponens from 5, 12)
(14) $x \to (q \to \perp)$ (modus ponens from 8, 13)
(15) $(x \to (q \to \perp)) \to ((x \to q) \to (x \to \perp))$ S
(16) $(x \to q) \to (x \to \perp)$ (modus ponens from 14, 15)
(17) $x \to \perp$ (modus ponens from 11, 16).

Now, from the premise $\neg p$, (or $p \to \perp$), together with a proof that $\perp \to q$ for arbitrary q, we conclude that $p \to q$ by the example in class.

(Qiaochu Yuan again)

Question 5

It suffices to set $q := \neg p$. Suppose there were a valuation ν such that $\nu((p \to \neg p) \to \neg(\neg p \to p)) = 0$. Then $\nu(p \to \neg p) = 1$ and $\nu(\neg(\neg p \to p)) = 0$, whence $\nu(\neg p \to p) = 1$. But if $\nu(p) = 1$, then the first condition is impossible, and if $\nu(p) = 0$, then the second condition is impossible; contradiction. So there exists no such valuation.

Question 6

Pay heed to the word 'carefully'. (It would have been much clearer if Professor Leader had challenged you to *show how to count ...*"). What he wants you to do is prove, by induction on n, that the set of formulæ of depth n is countable. He (and I, too) want you to do this by explicitly showing how to obtain an enumeration of the set of formulæ of depth $n+1$ from an enumeration of the set of formulæ of depth n. That will give you an ω-sequence of enumerations which you can stitch together to obtain a wellordering of the union. The stitching together is done in the standard zigzag way that you use to enumerate $\mathbb{N} \times \mathbb{N}$. If you do it that way, then you have explicitly exhibited an enumeration of the language.

You will all of you want to prove by induction on n that the set of formulæ of depth n is countable, but you might feel inclined to appeal to the sirens you heard in Numbers and Sets who told you that a union of countably many countable set is countable, and to use that at each step in the induction, as well as in the final wrap-up stage. Even if that is true (and certainly there are people who believe it) it's bad practice to appeal to it, beco's (i) you don't need it (as we have seen) and (ii) a proof that uses that principle contains less information than the constructive proof I have outlined above.

There are other cute ways of doing it. Here's one of them. Structure your infinite set of primitive propositions as $\{p, pp, ppp, pppp \ldots\}$. Your alphabet now has only *five* characters: ')', '(', '$\to$', '$\perp$' and 'p'—rather than a countable infinity of them. Your set of propositional letters is now (what those of you who did languages and automata would call) a regular language over that alphabet. Number these characters with the numbers 0 to 4. Now any number written in base 5 corresponds to a unique string from this alphabet. Or you could have an alphabet of *six* characters by adding the prime symbol so that your propositional leters are p, p', p'' .... [For pedants: we don't have to worry about leading zeroes beco's no wff starts with a right parenthesis!] [Again—for pedants—the set we have shown to be countable is not the propositional language itself but rather a superset containing some ill-formed formulæ. However it is easy to recover a counting of the propositional language from this: after all, every infinite subset of $\mathbb{N}$ can be effectively counted.]

That proof used the clever trick that made the alphabet finite, but you actually don't need to do that. You can exploit unique factorisation of natural numbers to make every natural number encode a sequence of smaller natural numbers, namely the exponents of $2, 3, 5 \ldots$ in its unique representation as a product of prime powers.

For the sake of those of you who did AFL last term it may be worth pointing out that on both these accounts of propostional letter—the p, pp, ppp account and the $p, p', p'' \ldots$ account—the set of propositional letters is a regular language, and the set of propositional formulæ is a context-free language.

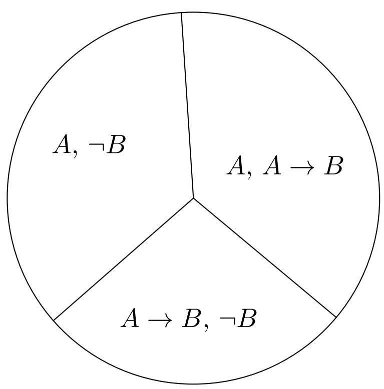
Question 7

Let P, Q, R be three consistent and deductively closed sets—the beliefs of the three parties. Then it is not possible to prove $\perp$ from any of P, Q, R, whence it follows that it is not possible to prove $\perp$ from any subset of any of P, Q, R; in particular it is not possible to prove $\perp$ from $P \cap Q \cap R$. It follows that $P \cap Q \cap R$ is consistent. Similarly, if t is a proposition which can be proven from $P \cap Q \cap R$, then it can be proven from P or Q or R, so it is in $P \cap Q \cap R$. It follows that $P \cap Q \cap R$ is deductively closed.

However, if P, Q and R are three consistent deductively closed sets of propositions, there is no guarantee that $(P \cap Q) \cup (P \cap R) \cup (P \cap R)$ is deductively closed or consistent. For consider:

P is the deductive closure of $\{A, \neg B\}$
Q is the deductive closure of $\{A, A \to B\}$
R is the deductive closure of $\{A \to B, \neg B\}$

A majority now believe A, $A \to B$, $\neg B$. This is not consistent. And, since the majority doesn't believe $\perp$, it isn't deductively closed either.



Observe (this is a check on your comprehension) that this can be extended to any finite number of sets—asking for larger majorities doesn't change anything. Divide the world into four bundles. Bundles 1, 2 and 3 all believe A; bundles 2, 3, 4 all believe $A \to B$; bundles 3, 4 and 1 all believe $B \to C$; finally bundles 4, 1 and 2 all believe $\neg C$. Each bundle has consistent beliefs but the beliefs held by a 3/4 majority are not consistent.

Mind you, if you have *infinitely* many people the then set of things believed by *cofinitely many* of them is consistent!

Question 8

We can prove by induction that if A is derivable from K and S and contains $\perp$ then $\perp$ can be replaced in A—and indeed throughout the proof of A—by some new letter not in the proof of A; the transformed proof is still a proof within the meaning of the act. So the modified A is still deducible from K and S. However the result of modifying the third axiom in this way is not a propositional tautology, and therefore cannot be deduced from K and S.

****

Actually one—no, *three*—of my supervisees came up with this. I had neglected to tell them it wouldn't work, so they just went ahead and did it anyway, and it worked. Quite embarrassing really.

They say: Read '$p \to q$' as '$(\neg p) \wedge q$', read '$\perp$' as '$\perp$' and take the designated truth-value to be 0. Then axioms K and S (aka 1 and 2) always take truth-value 0, and MP preserves the property of always taking truth-value 0. That ensures that axiom 3 does not take the designated value.

Question 8

If we can deduce an expression ϕ from the first two axioms, where ϕ has occurrences of '$\perp$', then we can also deduce the result of replacing in ϕ every occurrence of '$\perp$' by some random propositional letter not appearing anywhere in the proof. So if we could deduce $((p \to \perp) \to \perp) \to p$ we would be able to deduce $((p \to q) \to q) \to p$. At the risk of making a mountain out of a molehill i will, at this point, say that the set of things deducible from axioms 1 and 2 is an inductively defined set and supports an induction principle, and we can use this induction principle to show that everything in this set is a tautology: the two axioms are tautologies, and tautologousness is preserved by *modus ponens*. $((p \to q) \to q) \to p$ is not a tautology and therefore cannot be deduced from the first two axioms.

In earlier editions of this sheet there was a further question along these lines ... "if A is a tautology not containing '$\perp$' must it be deducible from the first two axioms?". This is a hard question. You might wish to pursue it. If you do, here is a slightly cuddlier version of it. "Find a tautology not containing '$\perp$' which is not derivable from the first two axioms, and use structural induction on the inductively defined set of deductive consequences of the first two axioms to prove that underivability." I have handouts on this with pretty pictures that it cost me blood to draw, so i'm hoping some of you will ask me about it.

But i'm going to insert here my discussion of that earlier impossible question ...

Impossible version of Question 8

The answer is 'no' and the proof(s) is (are) very cute, but there is no obvious way in; you just have to know. If you wanted to guess that the answer is 'no' you could reflect that the collection of deductive consequences of the first two axioms using *modus ponens* is an inductively defined set and so supports a kind of induction, so you might try to find some property possessed by the first two axioms that is preserved by *modus ponens* that is not possessed by some special tautology. And this is in fact exactly what we will do.

The counterexample is $((A \to B) \to A) \to A$, commonly known as *Peirce's law*. (*One* of the reasons why this question is ridiculously hard is that—even if you guess that the answer to this question is 'no' there is no way for you to know that Peirce's law is a counterexample... let alone guess that it is, in fact, the *simplest* counterexample.) Easy to check that it is a tautology... less easy to see that it does not follow from K and S.

Axiom K: $A \to (B \to A)$.

Axiom S: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

One of my students asks me what it means. Good question. I find myself replying that the reason why it's hard to understand is that it isn't really a fact about implication at all, it's a fact about negation and disjunction. Classical Logic has this odd feature that all the connectives are definable in terms of each other, so $\to$ is definable in terms of $\vee$ and $\neg$, giving us the rewrite rule:

$$(\neg p) \vee q \implies p \to q$$

It turns out that there are some classical truths about $\neg$ and $\vee$ that can be rewritten by repeated applications of this rule into expressions purely in the language of $\to$. Such expressions can masquerade as facts about $\to$ when in fact they are nothing of the sort. So Peirce's Law starts off as

$$\neg(\neg(\neg A \vee B) \vee A) \vee A \qquad (P')$$

which you can easily check to be a tautology. (Mind you, P' is not exactly a model of lucidity either). It just so happens that it is in the domain of the interpretation that sends $\neg p \vee q$ to $p \to q$.

The idea that is key to cracking this question is the thought that there might be more than one notion of validity, *i.e*, there might be some other property that is possessed by K and S and which is preserved by *modus ponens* but is not possessed by Peirce's Law. There is a ready supply of these notions in the form of *many-valued truth-tables*. We will use the following three-valued truth-table for the connective '$\to$'.

$\to$	1	2	3
1	1	2	3
2	1	1	3
3	1	1	1

(The figures in the column below the '$\to$' are the truth-values of the antecedent, and the figures in the row to the right of the '$\to$' are the truth-values of the consequent, and the figure in the matrix array is the truth-value of the conditional with that antecedent and that consequent.)

For our purposes, think of truth-value 1 as `true` and the other two truth-values as two flavours of `false`.

Notice that, in this truth table, if A and $A \to B$ both take truth-value 1, so does B. Notice also that K and S take truth-value 1 under all assignments of truth-values to the letters within them. So if ϕ is deducible from K and S, it must take value 1 under any assignment of truth-values to the literals within it (by structural induction).

Then check that, if A is given truth-value 2 and B is given truth-value 3, $((A \to B) \to A) \to A$ then gets truth-value 2, rather than 1.

So Peirce's law is not deducible from K and S.

(Notice that if we ignore the truth-value 2 (so that we discard the second row and the second column) what remains is a copy of the ordinary two-valued table, with 3 as `false` and 1 as `true`. Also, if we similarly ignore the truth-value 3 what remains is a copy of the ordinary two-valued table with 1 as `true` and 2 as `false`.)

This three-valued logic caper looks entirely *ad hoc*—and indeed it is. Or was. Originally. It turned out later that the funny truth-values have genuine mathematical meaning. (Something to do with possible world semantics). But that wasn't clear to the people who dreamt them up. There's a moral there ... (If you want to know about possible world semantics look at the chapter in `www.dpmms.cam.ac.uk/~tf/chchlectures.pdf`)

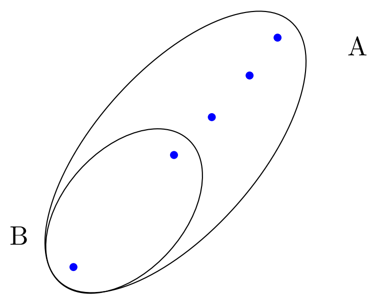
The other moral of this example is that some kinds of Mathematics really need formalisation. Unless we had a concept of *proof*—and of proof by induction on the structures of proofs, indeed—we would have no way of demonstrating that $((A \to B) \to A) \to A$ cannot be derived from K and S.

There is a more subtle, more beautiful and more enlightening—but much harder—proof using Curry-Howard, but we probably won't get round to it. However, if we *did* get round to talking about Curry-Howard in the supervision then the remainder of this section will make sense to you. I wrote it up from a brief paragraph in an article of Dana Scott's[1] partly for my own good, and it may well benefit from critical eyes such as yours, Dear Reader.

[1] Scott, D.S. Semantical Archæology, a parable. In: Harman and Davidson eds, Semantics of Natural Languages. Reidel 1972 pp 666–674.

Dana Scott's clever proof

Suppose *per impossibile* that there were a uniformly definable (and, accordingly, invariant) function P for Peirce's law. Let B be a two-membered set, and let A be obtained from B by adding three new elements.



A has five members and B has two, so any function $A \to B$ identifies a distinguished member of B, namely the one with larger preimage. This defines a function from $A \to B$ to B, which is to say (since $B \subseteq A$) a function from $A \to B$ to A. So what we have, in this rather special case, is a distinguished function $(A \to B) \to A$. Let us call this function F. F exists only because of the special circumstances we have here contrived, and it's not the sort of thing that P would normally expect to have to deal with, so we should expect P to experience difficulty with it ...which of course is exactly what we want! But, if we have a term P, we can apply it to F to obtain a distinguished member of A. But clearly there is no way of picking a member of A in this way. The alleged existence of a uniformly definable P is trying to tell us that whenever we have a set of five things divided into two parts, one with two things in it and the other with three, then one of the five things is distinguished. And that's clearly not true.

On what features of A and B does this counterexample rely? A function $A \to B$ has to give us (*via* the pigeonhole principle) a distinguished element of B, so we need B to have two elements, and A (and therefore $A \setminus B$) to have an odd number. $|A \setminus B| = 1$ is no good, beco's then A has a distinguished element, which we don't want. $|A \setminus B| = 3$ is the smallest number that will do, and that is what Dana Scott gives us.

Question 9

Suppose not ...

Consider $\{\neg t_n : n \in \mathbb{N}\}$. This is an inconsistent theory, since every v makes at least one t_n true. So by compactness there is a n such that $\{\neg t_m : m < n\} \models \perp$. But that is to say that every valuation must make true one of the t_m with $m < n$.

Why is the compactness theorem for propositional logic like the compactness of the space of valuations? The space of valuations is compact. That is beco's it is the product of lots of copies of the two-point space (one copy for each propositional letter) and the two-point space is compact. And a product of compact spaces is compact. (That's Tikhonov—in fact a subtly weaker version of Tikhonov that sez that a product of compact *Hausdorff* spaces is compact *Hausdorff*). For any propositional formula ϕ the set $[[\phi]]$ of valuations making it true is closed (in fact clopen). Suppose now that Γ is an inconsistent set of formulæ. Then $\{[[\phi]] : \phi \in \Gamma\}$ is a family of closed sets with empty intersection. So some finite subset of it has empty intersection. So there is a finite $\Gamma' \subseteq \Gamma$ with $\Gamma' \models \perp$.

Question 10

Any finite set of sentences has an independent subset. You can discard a sentence that follows from the remaining sentences. You can do this deterministically or non-deterministically, it doesn't matter. It doesn't matter in the sense that you will get an independent subset whatever happens, but which independent subset you get might depend on the order in which you do your weeding. For example if you start with

$\{p,\, p \longleftrightarrow q,\, q\}$ you can drop any one of the three to obtain an independent subset. (This is a repurposing of a standard illustration of three events any two of which are independent; you may know it from elsewhere).

Let the propositional alphabet P be $\{p_i : i \in \mathbb{N}\}$.

Then the set $\{\bigwedge\limits_{i \leq n} p_i : n \in \mathbb{N}\}$ is a(n infinite) set of formulæ with no equivalent independent subset.

For the second part, suppose $\{A_i : i \in \mathbb{N}\}$ axiomatises a theory T. Perform a *weeding* operation by removing any A_i that follows from $\{A_j : j < i\}$. Then renumber.

Next consider the axioms

$$B_i := (\bigwedge_{j<i} A_j) \to A_i.$$

(Observe that B_1 is just A_1—beco's the empty conjunction is just the `true`). Clearly the B_i axiomatise T. We will show that they are independent.

Fix i and consider B_i, which is $(\bigwedge_{j<i} A_j) \to A_i$. Beco's of the weeding it is not a tautology. So there is a valuation making it false. Any such valuation both

(i) makes A_j true for $j < i$ (and thereby makes all the B_j with $j < i$ true by making the consequents true) and

(ii) makes A_i false (and thereby makes true all the B_k with $k > i$ by making all their antecedents false).

Thus, for every i, there is a valuation making B_i false and all the other B_j true. So no B follows from any of the others.

Observe the pleasing fact that if you apply this process to the example we saw above $\{\bigwedge\limits_{i \leq n} p_i : n \in \mathbb{N}\}$ of a set of formulæ with no equivalent independent subset, then you just get back the set of primitive propositions.

One of my students came up with this rather nice following proof. (It would never have occurred to me!)

We are given the $\langle A_i : i \in \mathbb{N}\rangle$. Order the entire propositional language in order-type ω as $\langle B_i : i \in \mathbb{N}\rangle$.

At each stage we have a finite axiomatisation-in-hand, called F_n. At stage n look at B_n and see if it is derivable from the A_i. If it is, we add it to our finite axiomatisation-in-hand, and then do the shakedown as in the first half of the question, thereby possibly discarding some formulæ. The independent axiomatisation we desire in then the limit of these finite axiomatisations-in-hand. Sounds cool, doesn't it? And i think it works, but we have to be very careful indeed. The axiomatisation we want isn't just $\bigcup_{i \in \mathbb{N}} F_n$ (which is what my student carelessly wrote down) beco's that includes all the things we discarded as part of our shakedown. What we want is the set of those formulæ that belong to all sufficiently late F_n.

I think, Dear Reader, that it could do you no harm to have to work out how to say this in symbols, this being a logic course.

You could try

$$\{\phi : (\forall n)(\phi \in F_n \to (\forall m \geq n)(\phi \in F_m))\}$$

which is the set of things that never get rejected. But i suspect it might also pick up all the things that never got put in in the first place. You sort it out!

You may be wondering whether or not you need countability: might it not be the case that *every* set of propositions has an equivalent independent set? See the (unlucky!) Q13 below!

Question 11

[Not sure whence cometh this proof; i don't remember writing it.]

Let S be a set of propositions. We want to show that if $S \models t$, then S has a finite subset S' such that $S' \models t$. Suppose this is true whenever $t = \bot$. If $S \models t$, it follows that $S \cup \{\neg t\} \models \bot$, so there is a finite subset S' of $S \cup \{\neg t\}$ such that $S' \models \bot$. If S' does not contain $\neg t$, then it is a subset of S, so $S \models \bot$, hence $S \models t$. Otherwise, no valuation is equal to 1 on S', so if a valuation ν is equal to 1 on $S' \setminus \{\neg t\}$ then $\nu(\neg t) = 0$, whence $\nu(t) = 1$, so $S' \models t$.

So it suffices to prove the claim when $t = \bot$. Let P be the set of primitive propositions. Since a valuation ν is determined by what it does on P, the set of valuations can be identified with the set $\{0, 1\}^P$. If $\{0, 1\}$ is given the discrete topology, then $\{0, 1\}^P$ is compact by Tikhonov's theorem.

A proposition in L determines a function $f : \{0, 1\}^P \to \{0, 1\}$. Since the truth of a proposition can only depend on finitely many elements of P, any such function f has the property that the preimages of both $\{0\}$ and $\{1\}$ must be open, whence f is continuous.

Now let S be a set of propositions which determine a set of functions $f_s : \{0, 1\}^P \to \{0, 1\}$, $s \in S$. We are given that $S \models \bot$, whence there is no valuation which takes the value 1 on all of S. This is equivalent to the statement that the open sets $f_s^{-1}``\{0\}$ form an open cover of $\{0, 1\}^P$ and, by compactness, this open cover has a finite subcover $f_{s_1}, \ldots f_{s_n}$. Then $\{s_1, \ldots s_n\} \models \bot$.

Looking at this again, in february 2022 ...

The compactness theorem states that the space of valuations is compact. So: what is the topology on the set of valuations? Well, what is a valuation? It's a function from primitive propositions to truth values. Thus you can think of a valuation as a member of the product space of a hatful of two-point spaces (think: `true, false`) each labelled with a primitive proposition. Give each copy of {`true, false`} the discrete topology. Now the discrete two-point space is compact, and a product of compact spaces is compact. You might well not be as familiar with this fact as other cohorts have been. Partly this is COVID disruption, and part of it may be a failure of baton-passing when the department abolished Met-&-Top and put it all into Analysis II. Anyway the result is called *Tikhonov's theorem* and it's a version of the axiom of choice. "Every product of compact spaces is compact".

Question 12

Let $\{p_i : i \in \mathbb{N}\}$ be distinct primitive propositions. For $i \in \mathbb{N}$ define A_i to be $\bigwedge\limits_{j \le i} p_i$.

Clearly the A_i form an infinite chain.

An uncountable chain wrt deducibility? You must be joking.

I found a proof, but i think this one—from Cong Chen—is better. This is not how he presents it, but the result of my doctoring. He does it in terms of probabilities, can you imagine! This is a *Logic* course for heavan's sake.

To each propositional formula with n distinct letters we can associate a rational number with denominator 2^n, namely the number of rows of its truth-table in which it comes out true divided by the number of rows in the truth-table. (OK, you can call it its probability if you insist). If $\phi \vdash \psi$ but not the other way round then the "probability" of ϕ must be less than the "probability" of ψ. Every valuation making ϕ true also makes ψ true. So the "probability" of ϕ is less-than-or-equal-to the "probability" of ψ. If the probabilities are the same then ϕ and ψ must be validated by the same valuations, and they ain't. This means that the map from the putative chain to the dyadic rationals is injective. And, as we all know, the set of dyadic rationals is countable, so the chain was countable.

So no uncountable chains.

Question 13*

Do not attempt this question. No, *really*.

☠

1

Oh, all right: have a look at `www.dpmms.cam.ac.uk/~tf/cam_only/rickard.pdf`.

* *

You see what i mean? Next time perhaps you'll believe me.

Answers to Fun Extra Questions

???

"Establish that the class of all propositional tautologies is the maximal propositional logic in the sense that any superset of it that is a propositional logic (closed under $\models$ and substitution) is trivial (contains all well-formed formulæ)."

Without loss of generality we can suppose that our language contains '$\top$' and '$\bot$'. There is no loss of generality co's we can always introduce them by definition if they aren't already there.

Suppose our Logic contains a formula Φ which is not a tautology. Since Φ is not a tautology, its CNF is not the empty conjunction, so Φ is a conjunction of finitely many ϕ_i, each of which is a disjunction of propositional letters and negations of propositional letters. So each of these ϕ_i is a theorem of our logic. Now we use the rule of substitution. Let ϕ be any of the ϕ_i. Replace all the letters with a positive occurrence in ϕ by $\perp$, and all those with negative occurrences by $\top$. ϕ now simplifies to $\perp$. So $\perp$ is a valid expression of our logic. But then anything follows.

■

Notice that this proof relies on every formula having a CNF, and therefore doesn't work for constructive logic... which is just as well!

???

"Show how $\wedge$, $\vee$ and $\neg$ can each be defined in terms of $\to$ and $\perp$.
Why can you not define $\wedge$ in terms of $\vee$?
Can you define $\vee$ in terms of $\to$?
Can you define $\wedge$ in terms of $\to$ and $\vee$?"

A:
You can define $\vee$ in terms of $\to$, perhaps surprisingly. $p \vee q$ is truth-functionally the same as $(p \to q) \to q$.

You can't define $\wedge$ in terms of $\vee$ because any formula built up solely using $\vee$ is true in more than half of its rows and $p \wedge q$ is true in only one quarter of its rows.

The following proof that you can't define '$\wedge$ in terms of '$\to$' and '$\vee$' is due to one of my students.

Think of the four element boolean algebra with its two extra elements `left` and `right`. Reflect that `left` $\to$ `right` is `right` and that `right` $\to$ `left` is `left`. And `left` $\vee$ `right` is of course $\top$. Consider any complex expression `fake-and`(p, q) with the two letters 'p' and 'q' in it, that comically aspires to be conjunction. Consider the valuation that sends p to `left` and sends q to `right`. There is no way it can send `fake-and`(p, q) to $\perp$, but that's what it would have to do if `fake-and`(p, q) really were $p \wedge q$.

???

This is a sleeper for **NP-completeness**

Prove that, for every formula ϕ in CNF, there is a formula ϕ' which
(i) is satisfiable iff ϕ is;
(ii) is in CNF where every conjunct contains at most three disjuncts.
(Hint: there is no assumption that $\mathcal{L}(\phi') = \mathcal{L}(\phi)$.)
A:
You have to make repeated use of the following trick. The clause $(p_1 \vee p_2 \vee p_3 \vee \cdots p_{2n})$ is satisfiable iff the two clauses $(p_1 \vee p_2 \vee p_3 \vee \cdots p_n \vee q)$ and $(p_{n+1} \vee p_{n+2} \vee p_{n+3} \vee \cdots p_{2n} \vee \neg q)$ are simultaneously satisfiable. Observe the use of the extra propositional letter! That way you can replace a single long clause by two smaller clauses, and you can get the size of the largest clause down to 3.

???

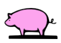
"Explain briefly why every propositional formula is equivalent both to a formula in CNF and to a formula in DNF.

Establish that the class of all propositional tautologies is the maximal propositional logic in the sense that any superset of it that is a propositional logic (closed under $\models$ and substitution) is trivial (contains all well-formed formulæ)."

A:

Suppose our Logic contains a formula Φ which is not a tautology. Since Φ is not a tautology, its CNF is not the empty conjunction, so Φ is a conjunction of finitely many ϕ_i, each of which is a disjunction of propositional letters and negations of propositional letters. So each of these ϕ_i is a theorem of our logic. Now we use the rule of substitution. Let ϕ be any of the ϕ_i. Replace all the letters with a positive occurrence in ϕ by p, and all those with negative occurrences by $\top$. So $\perp$ is a valid expression of our logic. 'Nuff said.

Notice that this proof relies on every formula having a CNF, and therefore doesn't work for constructive logic. . . which is just as well!



"A *type* in a propositional language $\mathcal{L}$ is a countably infinite set of formulæ.

For T an $\mathcal{L}$-theory a *T-valuation* is an $\mathcal{L}$-valuation that satisfies T. A valuation v *realises* a type Σ if v satisfies every $\sigma \in \Sigma$. Otherwise v *omits* Σ. We say a theory T *locally omits* a type Σ if, whenever ϕ is a formula such that T proves $\phi \to \sigma$ for every $\sigma \in \Sigma$, then $T \vdash \neg\phi$.

(a) Prove the following:

Let T be a consistent propositional theory, and $\Sigma \subseteq \mathcal{L}(T)$ a type. If T locally omits Σ then there is a T-valuation omitting Σ.

(b) Prove the following:

Let T be a consistent propositional theory and, for each $i \in \mathbb{N}$, let $\Sigma_i \subseteq \mathcal{L}(T)$ be a type. If T locally omits every Σ_i then there is a T-valuation omitting all of the Σ_i."

Answer:

(a)

THEOREM 1. *The Omitting Types Theorem for Propositional Logic*

Let T be a consistent propositional theory, and $\Sigma \subseteq \mathcal{L}(T)$ a type. If T locally omits Σ then there is a T-valuation omitting Σ

Proof:

By contraposition. Suppose there is no T-valuation omitting Σ. Then every formula in Σ is a theorem of T so there is an expression ϕ (namely '$\top$') such that $T \vdash \phi \to \sigma$ for every $\sigma \in \Sigma$ but $T \not\vdash \neg\phi$. Contraposing, we infer that if $T \vdash \neg\phi$ for every ϕ such that $T \vdash \phi \to \sigma$ for every $\sigma \in \Sigma$ then there is a T-valuation omitting Σ. ■

However, we can prove something stronger.

(b)

THEOREM 2. *The Extended Omitting Types Theorem for Propositional Logic*

Let T be a consistent propositional theory and, for each $i \in \mathbb{N}$, let $\Sigma_i \subseteq \mathcal{L}(T)$ be a type. If T locally omits every Σ_i then there is a T-valuation omitting all of the Σ_i.

Proof:

We will show that whenever $T \cup \{\neg\phi_1, \ldots \neg\phi_i\}$ is consistent, where $\phi_n \in \Sigma_n$ for each $n \leq i$, then we can find $\phi_{i+1} \in \Sigma_{i+1}$ such that $T \cup \{\neg\phi_1, \ldots \neg\phi_i, \neg\phi_{i+1}\}$ is consistent.

Suppose not, then $T \vdash (\bigwedge\limits_{1 \leq j \leq i} \neg\phi_j) \to \phi_{i+1}$ for every $\phi_{i+1} \in \Sigma_{i+1}$. But, by assumption, T locally omits Σ_{i+1}, so we would have $T \vdash \neg \bigwedge\limits_{1 \leq j \leq i} \neg\phi_j$ contradicting the assumption that $T \cup \{\neg\phi_1, \ldots \neg\phi_i\}$ is consistent.

Now, as long as there is an enumeration of the formulæ in $\mathcal{L}(T)$, we can run an iterative process where at each stage we pick for ϕ_{i+1} the first formula in Σ_{i+1} such that $T \cup \{\neg\phi_1, \ldots \neg\phi_i, \neg\phi_{i+1}\}$ is consistent. This gives us a theory $T \cup \{\neg\phi_i : i \in \mathbb{N}\}$ which is consistent by compactness. Any model of $T \cup \{\neg\phi_i : i \in \mathbb{N}\}$ is a model of T that omits each Σ_i.

■

Propositional Omitting Types is helpful when considering Yablo's Paradox. See `https://en.wikipedia.org/wiki/Yablo's_paradox` and perhaps `http://www.dpmms.cam.ac.uk/~tf/yabloomittingtypes.pdf`

Its rôle here is as a sleeper for the Omitting Types Theorem for first-order logic... which you *aren't* going to be lectured but which you will one day want to know, if you are ever to do more logic. Think of this as a bit of future-proofing.

Sheet 2

For this second sheet specifically i would recommend that you have a look at `www.dpmms.cam.ac.uk/~tf/ordinalsforwelly.pdf`, or at any rate the first forty-or-so pages. Prof Leader simply doesn't have time to do ordinals in the leisurely way the material ideally requires, and a lot of the interesting ideas get introduced in the exercises rather than in the lectures. Needs must when the Devil drives.

Some thoughts and advice is in order on this first crop of questions on ordinals and order types. It's a racing certainty that there will be a question about ordinals in your Part II exams. I am not in favour of mark-grubbing but it seems pointless to turn down a free α. You will be asked questions about equations and inequations, and invited to prove the true ones and find counterexamples to those that are false. Some of the true ones (like distributivity on the right of $\times$ over $+$, and associativity of $\times$ and $+$) work for arbitrary linear order types and therefore can be proved by hand and you don't need induction. *Don't use induction if you don't have to!* Some of them work only for ordinals and then you need to exploit the fact that you are dealing with ordinals. $\alpha + 1 > \alpha$ is true for ordinals but not for arbitrary linear order types (think of ω^*) *so you have to exploit somehow the fact that α is an ordinal.* Exploiting the fact that the characters in your play are ordinals doesn't necessarily mean you have to be doing an *induction*...tho' it usually does.

One thing worth keeping clear in your mind is which operations preserve strict inequality. You will need this when considering the old tripos question (set by your humble correspondent) that $\alpha^2\beta^2 = \beta^2\alpha^2$ iff $\alpha\beta = \beta\alpha$.

Question 1

Write down subsets of $\mathbb{R}$ of order types $\omega + \omega$, ω^2 and ω^3 in the inherited order.

The purpose of this question is really just to give you an idea of what wellorderings of these order types might look like. That is a worthwhile exercise beco's you have probably never had to think about wellorderings of transfinite length before. It also prepares you for Question 10 below where you are invited to show that every countable ordinal is the ordertype of some subset of $\mathbb{R}$.

For $\omega+\omega$ one of my students came up with $\{1-1/n : n \in \mathbb{N}\} \cup \{10-1/n : n \in \mathbb{N}\}$. Why that rather than $\{1-1/n : n \in \mathbb{N}\} \cup \{2-1/n : n \in \mathbb{N}\}$, i wondered ...? *His* answer is the range of an order-preserving map from the ordinals below $\omega + \omega$ into $\mathbb{R}$. *My* preferred answer is the range of a *continuous* order-preserving map from the ordinals below $\omega + \omega$ into $\mathbb{R}$. [What is the topology on the ordinals in virtue of which this map is cts?] Actually it later occurred to me thet his 10 was probably binary, so the inject is cts after all!

ω^2 is not that hard: $\{n - 1/m : n, m \in \mathbb{N}\}$, but ω^3 requires a bit of work. Fortunately most of you were up to it. The key observation is that, in each copy of ω, the gap between the mth and the $m+1$th point is $\frac{1}{m(m+1)}$ wide, so if you want to squeeze an extra copy of ω in there you do

$$\{n - \frac{1}{m} - \frac{1}{km(m+1)} : n, m, k \in \mathbb{N}\}$$

Actually an answer i have just seen from one of my students (thank you Louie Gabriel!) suggests that you can get ω^n by continued fractions of length n. I think that works, and that the key is to show that the set of continued fractions of length n with coefficients from $\mathbb{N}\setminus\{0\}$, (using subtraction not addition!) is legicographically ordered to order type ω^n:

$$a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{a_3 + \cdots}}} \tag{CF1}$$

For example:

$$\{a_0 - \frac{1}{a_1} : a_0, a_1 \in \mathbb{N} \setminus \{0\}\} \tag{CF2}$$

gives ω^2.

Key observation: multiplicative inversion and additive inversion are both order-reversing, so their composition is order-preserving, with the effect that expressions like (CF1) and (CF2) above are monotone increasing in all the a_i. We can make this explicit by rearranging $a_0 - \frac{1}{a_1}$ to $(a_0 \cdot a_1 - a_1)/a_1$ and $((a_0 - 1) \cdot a_1)/a_1$; finally ignoring the denominator since is it positive and doesn't affect the order (and ignore the '-1' similarly) to get $a_0 \cdot a_1$ which looks like $\mathbb{N} \times \mathbb{N}$. So the next term we want is

$$a_0 - \frac{1}{a_1 - \frac{1}{a_2}} \tag{CF3}$$

which is $(a_0 \cdot a_1 \cdot a_2 - 1 - a_2)/(a_1 \cdot a_2 - 1)$ which we can analogously process into $(a_0 \cdot a_1 - 1) \cdot a_2$ which looks like $\mathbb{N}^3$

If the order is genuinely to be lexicographic we need to know that altering a_2 *ad lib* cannot have as much effect as altering a_1 by even 1. And this is clear: however small we make a_2 (and it cannot be smaller than 2) we cannot get the effect of altering a_1.

So the claim is that

$$\{a_0 - \frac{1}{a_1 - \frac{1}{a_2 - \frac{1}{a_3}}} : a_0, a_1, a_2, a_3 \in \mathbb{N} \setminus \{0\}\}$$

is a subset of $\mathbb{Q}$ of order type ω^4 in the inherited order. And so on!

I think it's pretty clear that this works for continued fractions of this (rather restricted) style for all n, so we get—for each $n \in \mathbb{N}$—a set of rationals of length ω^n in the inherited order. Let us call the nth subset of the rationals thus obtained W_n, so that the displayed set is W_0.

Notice that we do *not* have $W_n \subseteq W_{n+1}$! This is an infelicity rather than a bug. When we replace W_n by W_{n+1} we do not so much put a copy of $\mathbb{N}$ at each place where we had a point before, as *delete* that point and then insert a copy of $\mathbb{N}$ *after* the hole we have just made. W_0 contains all the natural numbers, but W_1 doesn't contain any natural numbers. So really the representation of ω^n that we want is not so much W_n as $\bigcup_{m \leq n} W_m$.

It is natural to expect that if we redefine W_n in this way then the order type of the union must be ω^ω. A word of warning is perhaps in order here. It is not generally clear that the union of a nested family of wellorderings is a wellordering. After all, the negative integers is the union of the nested finite wellorderings $[-n, 0]$.

In fact we do *not* get ω^ω. This is because lots of things have stuff inserted *below* them at later stages, so one obtains infinite descending sequences in the union. There is an old tripos question about this is which it will do you no harm to look at: 2009 paper 3 16G. I have a discussion answer to this question which is linked from my home page. `https://www.dpmms.cam.ac.uk/~tf/cam_only/oldLSTtriposquestions.pdf`

I don't think there is any real mathematics in this, but it is quite cute.

Question 2

"Let α, β and γ be ordinals. If $\alpha \leq \beta$, must we have $\alpha + \gamma \leq \beta + \gamma$? $\alpha < \beta$, must we have $\alpha + \gamma < \beta + \gamma$?"

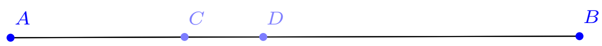
One of you was asking me about this question ahead of the supervision. It made me think that the first thing to do is to prove a helpful factoid that the two definitions of $\leq$ for ordinals are equivalent. One says that $\alpha \leq \beta$ iff a thing of length α can be injected in an order-preserving way into a(ny) thing of length β; the other definition insists further that the injection should be onto an initial segment of the thing of length

β. These two definitions are equivalent for ordinals, but not for arbitary linear order types (think: open and closed intervals in the reals).

You might like to prove that a total order $\langle A, <_A \rangle$ is a wellorder iff every subordering is an initial segment. Suppose $\langle A, <_A \rangle$ injects isomorphically into $\langle B, <_B \rangle$. You do the "Othello" (falling discs) trick to the range of the injection to collapse it down to an initial segment of $\langle B, <_B \rangle$.

Does a picture serve for a proof for questions like these? Depends partly on whether you are (i) trying to persuade yourself of the truth of the allegation (by gaining understanding) in which case it's probably all right, or (ii) trying to remove all doubt, in which case it might not be.

In any case, the way to understand these questions is by thinking of ordinals as isomorphism classes of wellorderings. Don't even think about trying to prove them by reasoning about von Neumann ordinals. There are many reasons for this. One fairly compelling one is that there is no corresponding way of concretising order types of total orders that don't happen to be wellorderings. So if you think of ordinals as von Neumann ordinals not only do you burn in hell for all eternity (which is quite bad enough) but you lose the connection with order types in general, and that starts to mess with your mathematics.



AC is of length α;
AD is of length β;
DB is of length γ.

This picture makes it obvious that the answer to the first part is 'yes'; so of course you expect the answer to the second part to be 'no', and you are correct: $1 < 2$ but $1 + \omega = 2 + \omega = \omega$.

Notice that adding on the right preserves strict inequality: $\omega + 1 < \omega + 2$

Question 3

Is there a non-zero ordinal α with $\alpha\omega = \alpha$? What about $\omega\alpha = \alpha$?

These are easy if you have correctly understood the (synthetic definition) of ordinal multiplication. Just in case you need a reality check, there is no α s.t. $\alpha \cdot \omega = \alpha$, whereas there are lots of α s.t. $\omega \cdot \alpha = \alpha$. Let β be any ordinal s.t. $1 + \beta = \beta$. Then $\omega^\beta = \omega^{1+\beta} = \omega \cdot \omega^\beta$.

Why is there no ordinal α s.t. $\alpha = \alpha \cdot \omega$? Various ways of seeing this. You can argue that, beco's α is an ordinal, you have $\alpha < \alpha + 1 \leq \alpha \cdot \omega$. Or you can do this:

Suppose α is a linear (aka total) order type satisfying $\alpha = \alpha \cdot \omega$. Then there is a linear order $\langle A, <_A \rangle$ which is isomorphic to a proper initial segment of it. Let π be the isomorphism. Consider any $x \in A \setminus \pi``A$. We must have $\pi(x) <_A x$, so $x >_A \pi(x) >_A \pi^2(x) \ldots$ is a subset of A lacking a least member. So $\langle A, <_A \rangle$ is not a wellorder, so α is not an ordinal.

Moral: no wellordering can be isomorphic to a proper initial subset of itself.

I am making two points here. One is that when it comes to proving things about ordinals *that rely on the things being ordinals* you don't have to do induction; there may be another way of exploiting the fact that these things are ordinals. The other point is that some of things that don't happen with ordinals might happen with other order types: $\alpha = \alpha \cdot \omega$ can happen if α is not an ordinal.

(Can you find an example? You should be able to...)

Question 4

"Show that the inductive and synthetic definitions of ordinal multiplication agree."

This question goes to the heart of how to think of ordinals.

The correct way to prove that the two definitions are equivalent is to fix α and prove by induction on β that the two definitions agree on $\alpha \cdot \beta$.

Well it's obviously true for $\beta = 0$! (OK, it's trivial, but at least it's a start.)

Suppose $\beta = \gamma + 1$. Then the recursive definition tells us that $\alpha \cdot \beta = \alpha \cdot \gamma + \alpha$. But this is clearly the length of a wellorder (any wellorder) obtained by putting a wellorder of length α on the end of a wellorder of length $\beta \cdot \gamma$.

It's at the limit stage that we have to do some work. So suppose the inductive and synthetic definitions of $\alpha \cdot \gamma$ agree for all $\gamma < \beta$. Consider a wellorder that is of length $\alpha \cdot \beta$ according to the synthetic definition. Up to isomorphism we can think of it as the lexicographic product of $\langle A, <_A \rangle \times \langle B, <_B \rangle$ for two wellorderings $\langle A, <_A \rangle$ and $\langle B, <_B \rangle$ of lengths α and β. Now let γ be an ordinal below β. Every such ordinal is the order type (length) of a unique initial segment of $\langle B, <_B \rangle$; let us write this as $\langle B, <_B \rangle \restriction \gamma$. Our lexicographic product $\langle A, <_A \rangle \times \langle B, <_B \rangle$ is now a colimit of all the $\langle A, <_A \rangle \times \langle B, <_B \rangle \restriction \gamma$ for $\gamma < \beta$. Each $\langle A, <_A \rangle \times \langle B, <_B \rangle \restriction \gamma$ is of length $\alpha \cdot \gamma$—and that is according to *either* definition, by induction hypothesis. So the length of $\langle A, <_A \rangle \times \langle B, <_B \rangle$ must be the supremum of $\{\alpha \cdot \gamma : \gamma < \beta\}$, and this is the recursive definition of $\alpha \cdot \beta$.

Question 5

This is easy as long as you are not seduced into attempting to do it by induction. It's true for all linear order types. So you do it by rearranging brackets

Question 6

Let α, β, γ be ordinals.

Must we have $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$?

Must we have $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$?

The first is false and the second is true. Remember what multiplication is: $\alpha \cdot \beta$ is the order-type of a thing that is β copies of thing of length α—not the other way round. The definition is not symmetrical so you shouldn't expect multiplication of order types to be commutative. The only sane way to prove this is by using the synthetic definition. In fact it is *always* best to prove facts about ordinals synthetically (wherever possible) rather than by induction. Let me say a bit about why this is so. Doing it by induction relies on the three order-types being ordinals (or at last one on which you are doing the induction being an ordinal) but that's not why it's true. It's true for *arbitrary* linear order types; the fact that α, β and γ are ordinals is irrelevant and shouldn't be exploited!

If you want to do it by induction there are some things you should think about. For a start there are two kinds of induction you can do over the ordinals. There is structural induction, where you consider three cases: (i) $\alpha = 0$, (ii) α successor, and (iii) α limit. Then there is *wellfounded* induction where you prove that α is F as long as every smaller ordinal is F. These correspond to the two kinds of induction you can do over $\mathbb{N}$, and they are of course equivalent—just as those two kinds of induction over $\mathbb{N}$ were. But in practice of course it's sometimes much easier to do it one way rather than the other.

Now suppose you are trying to prove that $\phi(\alpha, \beta)$ holds for all ordinals α and β. There are six ways you could do it.

(i) Say: "let α and β be arbitrary", reason about them, conclude the things you want

(ii) You could fix α, and prove by induction on β that $(\forall \beta)(\phi(\alpha, \beta))$, where your induction hypothesis is $\phi(\alpha, \beta)$; then say "but α was arbitrary..."

(iii) You could fix β, and prove by induction on α that $(\forall \alpha)(\phi(\alpha, \beta))$ where your induction hypothesis is $\phi(\alpha, \beta)$; then say "but β was arbitrary..."

(iv) You could prove by induction on α that $(\forall\beta)(\phi(\alpha,\beta))$ where your induction hypothesis is $(\forall\beta)(\phi(\alpha,\beta))$;

(v) You could prove by induction on β that $(\forall\alpha)(\phi(\alpha,\beta))$ where your induction hypothesis is $(\forall\alpha)(\phi(\alpha,\beta))$;

(vi) You could perhaps do a wellfounded induction on the lexicographic product... infer $\phi(\alpha,\beta)$ from the assumption that $\phi(\alpha',\beta')$ holds for all pairs α',β' below α,β in the lexicographic product.

That's bad enough. The thing we are challenged to prove here has *three* variables in it. I don't want to think about how to do it by induction: life is too short.

Actually, one of my 2021 students (Tsz Lo Fong) made a rather good remark about this. He says: "always do the induction on the rightmost variable". Admittedly this sounds a bit hand-wavy but it looks like a good guide to me[2]. The point is that the recursions for + and $\times$ and exp all work on the rightmost variable.

Question 7

Let α, β and γ be ordinals.
(i) Must we have $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$?
(ii) Must we have $\alpha^{\beta^\gamma} = \alpha^{\beta\cdot\gamma}$?
(iii) Must we have $(\alpha\cdot\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$?

Make sure you really understand ordinal exponentiation before you tackle this question ... it's deceptively hard.

The first is pretty obviously true, and you prove it by induction (on 'γ').

It may be worth pointing out that the true equations concerning exponentiation also work for arbitrary linear order types and can be proved synthetically using the synthetic definition of ordinal exponentiation ... which you haven't been given. So you will have to use induction!

Part (ii) is true and you prove it by induction on 'γ'.

Part (iii) is false; take $\alpha = \beta = 2$ and $\gamma = \omega$.

Question 8

You want three tosets none of which embeds in either of the others? Piece of cake. The rationals, the countable ordinals and the countable ordinals turned upside-down. In fact with a little work you can show—just using lots of copies of $\mathbb{N}$ and $\mathbb{N}$ upside-down (the negative integers)—that you can get finite antichains as wide as you like. Here's how to get an antichain of width 2^n. Take all your n-bit words, and in each replace the 0s by ω and the 1s by ω^* (ω^* is the order type of the negative integers) , and concatenate them. Thus, when $n = 2$, you get the 2^2 order types:

$$\omega+\omega,\ \omega+\omega^*,\ \omega^*+\omega \text{ and } \omega^*+\omega^*$$

which form an antichain.

Can you get infinite antichains? Think about what happens if you have things like this made from ω pieces strung together. You don't get an infinite antichain!

Yes, you *can* get infinite antichains, but in every infinite antichain there must be at least one total ordering of an uncountable set (so, in fact, cofinitely many, if you think about it). This is corollary of a beautiful theorem of the late and much lamented Richard Laver. In some years I set a Part III essay on it. If you want to have a look at it (and it is *very* nice) then point your search engine at *Laver's proof of the Fraïssé conjecture*.

[2] Always learn from your students!

Question 9

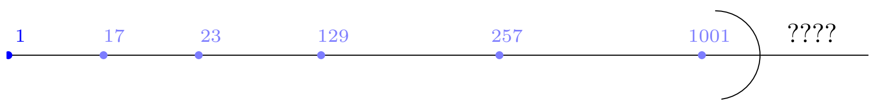
If α is a countable nonzero limit ordinal, it is the order type of a wellordering $<_a$ of $\mathbb{N}$. You now have *two* wellorderings of $\mathbb{N}$. You construct an increasing ω-sequence of naturals by "picking winners" (Prof. Leader's expression). Set a_0, the first member of the sequence, to be 0; thereafter a_{n+1} is to be the $<_{\mathbb{N}}$-least natural that is $>_a a_n$. Now set α_i to be the length of the initial segment of $\langle \mathbb{N}, <_a \rangle$ bounded by a_i.

Actually Michael Savery has a rather cute formulation of this. He says a natural number n is "tall" iff $(\forall m <_{\mathbb{N}} n)(m <_a n)$, and he gets his sequence of α_i from the tall naturals.

For the moment i'm going to leave it to you to verify that we never run out of naturals, and that the sequence $\langle a_i : i \in \mathbb{N} \rangle$ is unbounded in $<_a$. The sequence of ordinals that you have obtained is a **fundamental sequence for** α. This shows that every countable limit ordinal has cofinality ω.

(Actually it shows slightly more than that: notice that we did not exploit the assumption that α is an *ordinal*. All we used was that it was the order type of a countable total ordering with no last element.)

BAD BREAK



The picture shows why every countable limit ordinal has cofinality ω. The long right-pointing arrow represents a countable ordinal manifested as a wellordering of naturals ($\mathbb{N}$ in a funny order). The (unbounded!) increasing sequence of natural numbers reading from the left are the numbers chosen as in the recursion ... 1001 is the least natural number > 257 that is above 257 in both orders. The semicircle represesents where this increasing sequence of naturals comes to a halt, closes off. Are there any natural numbers in the region flagged by the question marks? Suppose there were—347, say. OK, so what were doing declaring 1001 to be the 6th member of the sequence? We should have used 347!

Thus every countable limit ordinal λ is the sup of an ω-sequence $\langle \lambda_i : i < \omega \rangle$ of smaller ordinals.

Definition 1.
Such a sequence of smaller ordinals is a **fundamental sequence** *for* λ.

Fundamental sequences give you a way of using ordinals to measure how rapidly growing a function $f : \mathbb{N} \to \mathbb{N}$ is. One can define a sequence f_α over countable ordinals α by something like $f_0(n) = n + 1$; $f_{\alpha+1}(n) = (f_\alpha)^n(n)$ and (and this is the clever bit) if λ is the sup of $\langle \lambda_n : n < \omega \rangle$ set $f_\lambda(n) = f_{\lambda_n}(n)$.

BAD BREAK

Essentially the same proof (perhaps slightly neater) starts with the reflection (going back to Cantor) that each ordinal α is the ordertype of the set (which i think Professor Leader notates 'I_α') of the ordinals below α in their natural order. If α is a countable ordinal then I_α is a countable set, so you exploit a counting of it (a bijection with $\mathbb{N}$) in the same way. That way you get the fundamental sequence directly. But it's the same proof really.

The interesting fact lurking behind this question is that you cannot compute the ω-sequence-of-smaller-ordinals-whose-supremum-is-α from α itself; you can only compute it from, so to speak, a *manifestation* of α, a wellordering of $\mathbb{N}$ of length α. One is thrown off the scent by the fact that in some cases (in fact in all cases known to you so far) it's perfectly obvious what the ω-sequence should be: for ω^ω it's $\langle \omega^n : n < \omega \rangle$, for ϵ_0 it's $\omega, \omega^\omega, \omega^{\omega^\omega} \ldots$. The problem is that there is no distinguished counting of I_α. There are countings all right (lots of them)[3] but no *distinguished* countings.

In the construction above, the particular ω-sequence you end up with will depend on your choice of $<_a$. How many such $<_a$ are there? (The answer to this riddle is not important, but I want you *to be able* to compute it)

[3]How many?

Observe that Set Theory is no help here. It's true that each countable ordinal has a canonical representative—in the form of the corresponding von Neumann ordinal—but this is no help, beco's these von Neumann ordinals do not come equipped with canonical bijections with $\mathbb{N}$!

Many of you exploited the identification of ordinals β with I_β. This is bad practice, and for a deep and compelling reason. You should never attempt to prove something about a suite of objects by reasoning about their implementation in a particular system—e.g. set theory. The fact that every countable ordinal has a fundamental sequence does not depend on a countable ordinal being the set of ordinals below it, and you should not make use of this fact (if it *is* a fact) in trying to prove your goal.

Finally you might like to check your comprehension by proving analogously that every limit ordinal between ω_1 and ω_2 is a limit of either an ω-sequence or an ω_1 sequence of smaller ordinals.

STOP PRESS!!!

ds903 says: Sse $f : \mathbb{N} \twoheadrightarrow I_\alpha$. Then set $\alpha_i =:$ otype of $\{\beta : \beta < \max\{f(1) \ldots f(i)\}\}$.
I think that works!

Question 10

(Tripos II 93206). For each countable ordinal α, show that there is a subset of $\mathbb{R}$ which is well-ordered (in the usual ordering) and has order-type α. Is there a well-ordered subset of $\mathbb{R}$ (again, in the usual ordering) of order-type ω_1?

It works not just for countable ordinals, but any countable order type whatever!
Take any total order of $\mathbb{N}$. We will define an injection into $\mathbb{Q}$ by recursion on the naturals. Send each natural number as it pops up to, well, the first positive integer if it is to the *right* of stuff already allocated, or the first negative integer if it is to the *left* of stuff already allocated. If it is between two things already allocated send it to the arithmetic mean of the things its immediate upper and lower neighbours were sent to. That is to say we construct the embedding (of the funny order on $\mathbb{N}$) by recursion on $\mathbb{N}$ in the usual order.

That's the correct way to do it. There is a wrong way to do it, which most people pounce on, and that is to try to do it by induction on countable ordinals. It works, but you have to use countable choice to pick fundamental sequences for all limit ordinals. I shall spare you the details, since you may well have worked them out for yourself[4].

If you want the details, I wrote them up in
`https://www.dpmms.cam.ac.uk/~tf/cam_only/fundamentalsequence.pdf`
starting at p 21, section 2. I am not going to repeat myself here.

Let us suppose that we have—by the above ruse, using countable choice—obtained a family $\langle f_\alpha : \alpha < \omega_1 \rangle$ where f_α injects the ordinals below α into $\mathbb{R}$ in an order-preserving way. Fix a countable ordinal ζ and consider the ω_1-sequence $\langle f_\gamma(\zeta) : \gamma > \zeta \rangle$. It would be natural to expect this to be a non-increasing sequence of reals. After all, the more ordinals you squeeze into the domain of an f, the harder you have to press down on its values to fit all the arguments in. But you'd be wrong!

Remark 1. *For each countable ordinal γ, the sequence $\langle f_\gamma(\zeta) : \gamma > \zeta \rangle$ is not monotone nonincreasing.*

[4]For any von Neuman ordinal x living in a model $\mathfrak{M}$ of ZF, we can find a larger model $\mathfrak{M}'$ which contains a bijection between x and $\mathbb{N}$. So x has become countable in the bigger model $\mathfrak{M}'$. This means that there cannot be a way of rummaging around *inside* a von Neumann ordinal to recover a counting of it. Such a method would work in some environments and not in others, so it can't be internal. So you shouldn't expect to be able to find a fundamental sequence for a countable ordinal without some extra outside help. To put it another way, there is no first-order expression ϕ of the language of set theory s.t. a von Neumann ordinal X is countable iff the structure $\langle X, \in, = \rangle \models \phi$.

Proof: Suppose that

$$(\forall\gamma < \gamma' < \omega_1)(\forall\zeta < \omega_1)(f_\gamma(\zeta) \geq f_{\gamma'}(\zeta)). \tag{1}$$

Then, for each $\zeta < \omega_1$, the sequence $\langle f_\gamma(\zeta) : \gamma > \zeta\rangle$ of values given to ζ must be eventually constant. For if it is *not* eventually constant then it has $cf(\omega_1) = \omega_1$ decrements, and we would have a sequence of reals of length ω_1^* in the inherited order, and this is known to be impossible.

So there is an eventually constant value given to ζ, which we shall write '$f_\infty(\zeta)$'. But now we have $\alpha < \beta \to f_\infty(\alpha) < f_\infty(\beta)$. (We really do have '$<$' not merely $\leq$' in the consequent: suppose $f_\infty(\alpha) = f_\infty(\beta)$ happened for some α and β; then for sufficiently large γ we would have $f_\gamma(\alpha) = f_\gamma(\beta)$ which is impossible because f_γ is injective). This means that f_∞ embeds the countable ordinals into $\mathbb{R}$ in an order-preserving way, and this is impossible for the same reasons.

So we conclude that the function $\langle\alpha, \beta\rangle \mapsto f_\alpha(\beta)$ is *not* reliably decreasing in its second argument.[5] ■

But that appealed to the second part of the question, which i had better now prove.

For the second part ("can you do the same for ω_1?") ...

There can be no subset of $\mathbb{R}$ that is of order-type ω_1 in the inherited order. Suppose S were such a set. Observe that to the right of every element of S is an open interval disjoint from S. That is to say $\mathbb{R}$ is naturally partitioned into half-open intervals, and this partition is in 1-1 correspondence with S, each member of S being paired with the half-open interval of which it is the left endpoint. This partition can be injected into $\mathbb{Q}$ by sending each piece to the first rational in it, in the sense of a standard wellordering of the rationals. So S was countable after all.

I have noticed that a surprising number of you use arguments involving countable choice.

One such argument says that, if there were a set X of reals of order-type ω_1 in the inherited order then each of the intersections $X \cap (n, n+1]$ would be countable, meaning that X is a union of countably many countable sets and is therefore countable, contradicting the assumption that it is of length ω_1 and therefore of size $\aleph_1$.

Using AC is bad practice even if AC is true. You don't want to use just any true fact that happens to be lying around: "God exists, so there is no order-preserving map from the second number class into the reals" doesn't quite cut it.

Some of you even managed to muck up the proof of two paragraphs above. OK, you send each countable ordinal to the open interval in $\mathbb{R}$ as above. You then say: each interval contains a rational—which indeed it does—and then shut up shop and go home. That's not really good enough. The contradiction comes from having a function from a set of size $\aleph_1$ (the set of countable ordinals "the second number class") into a set of size $\aleph_0$ (the rationals). You can't stop until you have done it. You have to actually pick a rational from each of these intervals, so that you can send the countable ordinal in question to that rational. Which rational? With many of you it cost blood and threats of the rack to get you to say that the rationals have an ordering of length ω so you pick, from each interval, the first rational in that interval in the sense of that wellordering. (Actually you can do something by thinking about the rationals in that interval with smallest denominator.) Even after I had spelled this out, a lot of you clearly just thought I was barmy. Well, I'm not: what I was trying to get you to do was come up with a proof, not a nondeterministic add-warm-water-and-stir pseudoproof. That's Logic for you!

More temperately [calm down and breathe deeply, tf] what is going on here is that we want to prove that, were there *per impossibile* an object of the conjectured kind (to wit, an order-preserving injection from the second number class into the reals) then there would be an object of a kind we know there cannot be, namely an injection of an uncountable set into a countable one. The proof must describe such a construction of an object of the second kind from an object of the first kind. One should never be *completely* satisfied with a nondeterministic construction if a deterministic construction is available.

If you want to think more about this have a look at chapter 2 (pp 20 *ff*) of `www.dpmms.cam.ac.uk/~tf/fundamentalsequence.pdf`

[5] I suspect that the the sequence $\langle f_\gamma(\zeta) : \gamma > \zeta\rangle$ of values given to ζ describe a nonmeasurable set. I have seen no proof of this, tho'. We needed AC to build it so it might well be nonmeasurable.

One of the things that this shows is that the quasiorder of linear order types (quasiordered by injective homomorphism) is not complete, or anything remotely like it: ω_1 and η (the order type of $\mathbb{Q}$) are distinct upper bounds for the second number class. ω_1 is a mini*mal* upper bound but it is not the mini**mum** upper bound, co's it ain't less than $\mathfrak{c}$. $\mathfrak{c}$ (the order type of the reals) is an upper bound, but it is not a mini*mal* upper bound; there is an infinite strictly descending sequence of upper bounds for the second number class all below $\mathfrak{c}$. (This is a theorem of Sierpinski, using a grubby diagonal argument powered by a wellordering of $\mathbb{R}$. I used to lecture it in my Part III lectures on WQO theory. It also shows its face in an Impossible Imre Question (question 14 on this sheet.)

Actually it's even worse than that: the quasiorder of linear order types isn't even a poset, beco's antisymmetry fails! (Consider the open and closed intervals $(0,1)$ and $[0,1]$.)

Question 12

This is a lovely—but very open-ended—question.

Here is a helicopter pilot's view. I am going to build a table (it's called the *Veblen hierarchy*) It consists of lots of rows. The first consists of the powers of ω: ω, $\omega^2 \ldots \omega^\omega \ldots$. Consider the function that enumerates the first row: $\alpha \mapsto \omega^\alpha$. For reasons that he wants you to think about, this function has fixed points—lots of them, arbitrarily late fixed points in fact. Your second row is now the list of fixed points of he enumeration of the first row, written in increasing order, left to right. The numbers in the second row are called ϵ-numbers. So that's how you get each row from the row immediately above it. Notice that each row—considered as a set of ordinals—is a subset of the row above it, so at limit stages you can take intersections. We write '$\phi(\alpha, \beta)$' for the αth member of the βth row. (Or it might be the other way round—don't take my word for it)

One thing to think about is: how many of these ordinals are countable? It's pretty obvious that the αth member of the first row is countable if α is. (Well perhaps not obvious, but plausible: you need the synthetic definition of ordinal exponentiation; α^β is ctbl if α and β are.) It's less obvious that αth member of the second row is countable if α is, but it's still true. And it becomes ever less obvious that the αth thing in the βth row (aka $\phi(\alpha, \beta)$) is countable if α and β are both countable, tho' (i am reassure by people who know more than me) that it is, even if we don't assume countable choice. (It's easy with countable choice beco's each fixed point is obtained as the supremum of an ω-sequence of smaller ordinals (each of which is countable by induction hypothesis) and is therefore countable by countable choice).

The answer to the last part is 'yes'; it's asking if there is anything in the third row, and there is. (The third row used to be called κ-numbers... until the penny dropped that we would soon run out of Greek letters). A much nastier question is: is there an α s.t. the first ordinal in the αth row is α? The answer to that—amazingly—is *yes* and—even more amazingly—not only is it countable but we even know of definable wellorderings of $\mathbb{N}$ of that—mind-boggling—length.

A good place to start reading is C. Smorynski "Varieties of Arboreal Experience", Mathematical Intelligencer **4** (1982) pp 182–189.`https://link.springer.com/article/10.1007/BF03023553`

Countable ordinals like this matter because there are plenty of countable structures whose complexity is somehow measured by ordinals. You need the device of **rank functions for wellfounded structures**. Look at `https://www.dpmms.cam.ac.uk/~tf/cam_only/partiilectures2016.pdf` p. 14.

Question 13

I have confirmation from Prof. Leader that everybody gets off sooner or later, but not necc at a countable stage, and—altho' only one person gets off at every countable stage—there is no limit to the number of people allowed to get off at stage ω_1.

I suppose that as a courtesy to my readers i should not only reveal the answer but give them some sort of narrative of how i got there, so that they can make progress like mine when they next encounter puzzles like this. So here is my train of thought, complete with false starts.

This is a puzzle about ω_1. What is the salient fact about ω_1? The fact that every increasing ω-sequence of countable ordinals has a countable sup. So how are we going to get an ω-sequence of countable ordinals in this puzzle where the fact that it has a countable sup might be useful? It's got to be something like: the $n+1$th ordinal is the time by which everyone who got on before the nth ordinal has got off. Take that idea and run with it.

I now think that i can show that the train is empty on arrival at the Gare de l'ω_1. Suppose the train is not empty on arrival at the Gare de l'ω_1. Consider the sequence of ordinals defined by the following recursion. α_0 is some ordinal s.t. by[6] that stage some people have got on who will be still on the train as it rolls into ω_1. Consider all the people who get on at stage α_0 and get off before Gare de l'ω_1. Beco's $\text{cf}(\omega_1) = \omega_1$ there will be a countable α_1 by which time all those people have got off. Let α_1 be the least such. Then consider the people who have got on at dates $\leq \alpha_1$ and are going to get off before ω_1. They have all got off by α_2 and so on. Let α be the sup of this sequence. Evidently everyone who has got on and is going to get off before ω_1 has got off before α. So the only people who are on the train when it reaches α are people who are going to remain on until the bitter end. If there are any such people then the train is nonempty and someone has to get off. But none of them can get off! So there are no such people. So everyone who gets on gets off before ω_1. So the train is empty on arrival at ω_1.

Actually—and I should've seen this coming—one of you came up with a proof using Fodor's theorem, a favourite of Prof Leader's. Fodor's theorem is a nice piece of Mathematics (Prof Leader is a man of taste, after all) but it's a bit too sophisticated. At this stage i want you rather to make sure you understand ordinals.

Question 14

This is a good question. As part of my general policy of humouring Prof Leader by not dishing out answers to Impossible Imre Questions I shall rein in my tongue. However i will give a hint! In fact *two* hints.

Hint 1: Exactly how many increasing injections $\mathbb{R} \hookrightarrow \mathbb{R}$ are there?
Hint 2: Why is Hint 1 a hint?

If you want to know about ordinals read the first 40 or so pages of `https://www.dpmms.cam.ac.uk/~tf/ordinalsforwelly.pdf`.

[6] Thanks to Michał Mrugała for clearing up a mistake at this point.