Discussion Notes for Prof Leader's 2018 Examples Sheets

Thomas Forster

March 15, 2018

A lot of these answers come from Qiaochu Yuan. He is not responsible for their present form, co's i've hacked them about.

Sheet 1

Question 1

1

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.

2

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

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

3

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.

Do not expect later questions in this sequence to be answered in this much detail!

Question 2

Write down a proof of $(\bot \to q)$ in the propositional calculus [hint: observe the result of question 4 below], and thence write down a deduction of $(p \to q)$ from $\{\neg p\}$.

[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 $\bot \vdash q$. The following is a proof:

t_1	$\bot$	(in S)
t_2	$\bot \to ((q \to \bot) \to \bot)$	K
t_3	$(q \to \bot) \to \bot$	(modus ponens from t_1, t_2)
t_4	$((q \to \bot) \to \bot) \to q$	(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 $\bot \to q$:

1	$\bot \to (\bot \to \bot)$	K
2	$\bot \to ((\bot \to \bot) \to \bot)$	K
3	$(\bot \to ((\bot \to \bot) \to \bot)) \to ((\bot \to (\bot \to \bot)) \to (\bot \to \bot))$	S

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

Question 3

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

Question 4

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

(i) By the deduction theorem, it suffices to show that $\{p,\ q,\ p\to(q\to\bot)\}\vdash\bot$. 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 $\nu(q\to\bot)=0$, whence $\nu(p\to(q\to\bot))=0$, from which it follows that $\nu((p\to(q\to\bot))\to\bot)=1$.

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

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. $(x \to x) \to ((x \to p) \to (x \to (q \to \bot)))$ S

13. $(x \to p) \to (x \to (q \to \bot))$ (modus ponens from 5, 12)

14. $x \to (q \to \bot)$ (modus ponens from 8, 13)

15. $(x \to (q \to \bot)) \to ((x \to q) \to (x \to \bot))$ S

16. $(x \to q) \to (x \to \bot)$ (modus ponens from 14, 15)

17. $x \to \bot$ (modus ponens from 11, 16).

Now, from the premise $\neg p$, (or $p \to \bot$), together with a proof that $\bot \to q$ 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'. What Professor Leader 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 there are people who deny 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 $\{p, p', p'', p''' \ldots\}$. Your propositional language now has only *six* characters: ')', '(', '$\to$', '$\bot$', 'p' and '$'$'—rather than a countable infinity of them. Number these characters with the numbers 0 to 5. Now any number written in base 6 corresponds to a unique string from this alphabet. [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.

Question 7

The beliefs of each member i of a finite non-empty set I of individuals are represented by a consistent, deductively closed set S_i of propositional formulæ. Show that the set

$$\{t : \textit{all members of } I \textit{ believe } t\}$$

is consistent and deductively closed. Is the set

$$\{t : \textit{over half the members of } I \textit{ believe } t\}$$

deductively closed or consistent?

Discussion

Let P, Q, R be three consistent and deductively closed sets—the beliefs of the three parties. Then it is not possible to prove $\bot$ from any of P, Q, R, whence it follows that it is not possible to prove $\bot$ from any subset of any of P, Q, R; in particular it is not possible to prove $\bot$ 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 $\bot$, 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 p; bundles 2, 3, 4 all believe $p \to q$; bundles 3, 4 and 1 all believe $q \to r$; finally bundles 4, 1 and 2 all believe $\neg r$. 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

If we can deduce an expression ϕ from the first two axioms, where ϕ has occurrences of '$\bot$', then we can also deduce the result of replacing in ϕ every occurrence of '$\bot$' by some random propositional letter not appearing anywhere in the proof. So if we could deduce $((p \to \bot) \to \bot) \to p$ 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.

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 $\{\neg t_n : n < N\} \vdash \bot$. But that is to say that every valuation must make true one of the t_n with $n < N$.

Why is the compactness theorem for propositional logic like the compactness of the space of valuations? The space of valuations is compact. 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 $\Gamma' \models \bot$.

Question 10: Independence

For the first part observe that if the propositional alphabet P is finite then—*altho' there are infinitely many formulæ in* $\mathcal{L}(P)$—there are only finitely many *logically distinct* formulæ. (Think: truth tables.)

Let the propositional alphabet P be $\{p_i : i \in \mathbb{N}\}$. Then the set $\{\bigwedge_{i \le n} p_i : n \in \mathbb{N}\}$ is a 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.

Question 11

The answer is 'no' but there is no obvious reason to expect it. 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*. 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: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

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 some (unspecified and so far undiscovered) tautology contining only '$\to$'. 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

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 on the family of proofs).

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, **not** 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`.

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

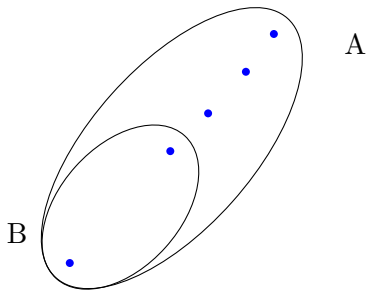
There is a more subtle, more beautiful and more enlightening—but much harder—proof using Curry-Howard, but we probably won't get round to it. However, if we *did* get round to talking about Curry-Howard in the supervision then the remainder of this section will make sense to you. I wrote it up from a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

Dana Scott's clever proof

The idea is to think of the arrow as function-space, so that $A \to B$ is the set of all functions from A to B. If we think of A, B and C as sets then there are uniformly definable functions inside $A \to (B \to C)$ (obviously) and inside $A \to (B \to C)$. $\to (A \to B) \to (A \to C)$ (slightly less obviously. By 'uniformly definable' we mean definable in a way that doesn't rely on special features of A, B and C.

Now for Peirce's Law: $((A \to B) \to A) \to A$.

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 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 an 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.

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

Question 12

This first bit comes from Sean Moss, Senior Wrangler not that long ago... He's now bunked off to The Other Place. Boo! Hiss!!

For concreteness, we'll consider the length $l(\phi)$ of a formula to be the total number of primitive propositions (counted with multiplicity), and we won't worry about 0.

Main idea: for any formula ϕ, if v is any valuation then $v \vDash \phi$ or $v \vDash \neg\phi$.

Thus for any choice of pluses and minuses $\pm p_1, \ldots, \pm p_m \vdash \phi$ or $\pm p_1, \ldots, \pm p_m \vdash \neg\phi$, where the p_i are primitive propositions including all of those occuring in ϕ (and $\pm p$ means one of p or $\neg p$).

We first find a bound $g(n)$ on the length of a proof of $\pm p_1, \ldots, \pm p_m \vdash \phi$ or $\neg\phi$.

We abbreviate $\pm p_1, \ldots, \pm p_m$ as v (as in a valuation).

Claim We can take $g(n) = 2^{n+3} - 15$

Proof. If $n = 1$, then $\phi = p$ and $\phi = \neg p$ each have one-line proofs from $\pm p$, so $g(1) = 1$.

Suppose $\phi = (\psi \to \chi)$ and $v \vdash \phi$, $l(\phi) = n + 1$.

Then if $v \vdash \chi$, write down a $\leq g(n)$-line proof of $v \vdash \chi$, followed by:

1	$\chi \to (\psi \to \chi)$	(K)
2	$\psi \to \chi$	(MP)

If $v \vdash \neg\chi, \neg\psi$, then write down a $\leq g(n)$-line proof of $\neg\psi$ followed by the 7-line proof of $\bot \to \chi$ and then the 6-line proof of $\psi \to \chi$.

Alternatively, if $v \vdash \neg(\psi \to \chi)$, then $v \vdash \psi, \neg\chi$.

Write down the two $\leq g(n)$-line proofs of ψ and $\neg\chi$. Then

$$\psi, \neg\chi, (\psi \to \chi) \vdash \bot$$

in only five lines

ψ	(Hyp)
$\psi \to \chi$	(Hyp)
χ	(MP)
$\chi \to \bot$	(Hyp)
$\bot$	(MP)

By the proof of the deduction theorem, we can prove

$$\psi, \neg\chi \vdash \neg(\psi \to \chi)$$

in $3 \times 5 + 2 = 17$ lines.

Thus we can prove $v \vdash \neg(\psi \to \chi)$ in $2g(n) + 15$ lines (we save 2 by not repeating the hypotheses in the last 17 lines). Solving the recurrence gives us the stated bound. ∎

Now we will use the fact that $T, p \vdash \phi$ and $T, \neg p \vdash \phi$ implies $T \vdash \phi$.

We can prove $\{p \to \phi, \neg p \to \phi, \neg\phi\} \vdash \bot$ in 10 lines:

1	$\phi \to \bot$	(Hyp.)

2	$(\phi \to \bot) \to (p \to (\phi \to \bot))$	(K)
3	$p \to (\phi \to \bot)$	(MP)
4	$(p \to (\phi \to \bot)) \to ((p \to \phi) \to (p \to \bot))$	(S)
5	$(p \to \phi) \to (p \to \bot)$	(MP)
6	$p \to \phi$	(Hyp.)
7	$p \to \bot$	(MP)
8	$(p \to \bot) \to \phi$	(Hyp.)
9	ϕ	(MP)
10	$\bot$	(MP)

By the deduction theorem there is a proof of $\{p \to \phi, \neg p \to \phi\} \vdash \neg\neg\phi$ in 32 lines.

Adding an instance of (T) and a (MP), we get a proof of $\{p \to \phi, \neg p \to \phi\} \vdash \phi$ in 34 lines.

Starting with N-line proofs of $\{\pm p_1, \ldots, \pm p_{m-1}, p_m\} \vdash \phi$ and $\{\pm p_1, \ldots, \pm p_{m-1}, \neg p_m\} \vdash \phi$ (where the $\pm$'s are fixed), use the deduction theorem to get $\leq (3N+2)$-line proofs for $\{\pm p_1, \ldots, \pm p_{m-1}\} \vdash p_m \to \phi, \neg p_m \to \phi$.

Add 32 lines to get to ϕ.

The process thus gives us a $(6N + 34)$-line proof of

$$\{\pm p_1, \ldots, \pm p_{m-1}\} \vdash \phi.$$

Since the number of primitive propositions in ϕ is bounded by its length, we need only iterate this a total of n times. Round up to $(6N+35)$ for convenience and then the n^{th} iterate is $6^n(N+42)-7$.

Thus the final bound we achieve is

$$\begin{aligned} f(n) &= 6^n(2^{n+3} - 15) - 7 \\ &= 8 \cdot 12^n - 15 \cdot 6^n - 7 \\ &= O(12^n). \end{aligned}$$

Thank you very much, Dr Moss!

You might wonder whether this exponential bound is best possible. Curiously, this is an open question. I have to be careful how to state this, because i suspect that for this particular presentation of propositional logic it probably *is* best possible—and is known (tho' not to me) to be best possible. The open question is whether or not there is a proof system for propositional logic in which there is a polynomial bound on lengths of proofs.

This is related to the P = NP question, or (more precisely) to the NP = *co*-NP question. The set of falsifiable formulæ of propositional logic is in NP (guess a valuation, verify in linear time that it falsifies the candidate). This is beco's a set X of things is NP ("is an NP-set") iff (by definition) you become a member of X in virtue of being related to something by an easily decidable relation; our example here is: you are refutable formula of propositional logic iff there is a valuation that refutes you. It's actually NP-*complete*, which is to say it's as bad a problem as an NP problem can be. (Every NP problem can be coded up—in polynomial time—as a question about satisfiability of a propositional formula). Now the set of tautologies is the complement of the set of falsifiable sentences, and thus is in *co*-NP. (A co-NP set is one whose complement is an NP set). Now, if we could find a proof system for propositional logic in which every tautology had a proof of polynomial length, then the set of tautologies would be in NP: guess a proof, verify in time linear in the proof

(polynomial in the candidate) that it is a proof of the candidate. So we would have a problem that is co-NP and is NP-complete, so every *co*-NP problem would be in NP whence NP = *co*-NP. This is an open problem ... a **hard** open problem!

Question 13

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

Clearly the A_i form an infinite chain.

An uncountable chain wrt deducibility? You must be joking.

Suppose we have uncountably many primitive propositions. Consider the symmetric group on the primitive propositions, and the orbits of its obvious action on compound propositions. Actually, on second thoughts, consider the subgroup consisting of those permutations of finite support (those that move only finitely many propositions). Why? Well, if the permutation σ moves a compound formula A to $\sigma(A)$ it does so only in virtue of a finite bit of σ so there will be a permutation of finite support that moves A to $\sigma(A)$. This will matter....

(Things belonging to the same orbit are said to be *alphabetic variants* [of each other; you may encounter this expression in other contexts] and the equivalence relation is sometimes called *α-equivalence*. In predicate calculus the existence of distinct–yet–α-equivalent formulæ is a pain, but it's one we get beco's we have variables.)

Now suppose *per impossibile* that we had an uncountable chain. Consider its intersections with the orbits. There are only countably many orbits. This is because each orbit corresponds to a "skeleton" of a formula—and there are only countably many skeletons.

The intersections of our putative chain with the orbits partitions it into countably many pieces. How big are the pieces? We want them to be so small that a union of countably many of them cannot be uncountable. Now you may know (and if you didn't you learnt it first here) that if AC fails badly enough then a countable set of pairs might have an uncountable sumset. So what we want to prove is that each piece is a singleton. That will do it.

Let A be a formula. Anything else in the orbit of A is $\sigma(A)$ for some permutation σ of finite support, and accordingly of order n, say, for some $n \in \mathbb{N}$. We claim that A and $\sigma(A)$ are either interdeducible or incomparable. Suppose not, and that $\vdash A \to \sigma(A)$. By composing our valuations (which are functions from primitive propositions to $\{T, F\}$) with the powers of σ we can see that we must also have $\vdash \sigma(A) \to \sigma^2(A)$, and $\vdash \sigma^2(A) \to \sigma^3(A)$ all the way up to $\vdash \sigma^{n-1}(A) \to \sigma^n(A) = A$ So any two comparable things in an orbit are interdeducible. So there are no chains even of length *two*, let alone uncountable chains!

■

Thanks to José Siqueira for compelling me to be clearer than i had been.

Actually here is another proof, due to Cong Chen. 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.

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 want). 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.

Question 14*

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

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.

Leader 2018 Sheet 2

[No notes on questions 1–3 for the moment]

Question 2

Does a picture serve for a proof for these equations? 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.

Question 3

Question 4

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

Ordinal multiplication is associative. 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.

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.

Tho' i s'pose i ought to, really. I think the correct way to prove $(\forall\alpha\beta\gamma)(\alpha\cdot(\beta\cdot\gamma)=(\alpha\cdot\beta)\cdot\gamma)$ by induction is by Universal Generalisation on 'α' and 'β' ("Let α and β be arbitrary") and do an induction on γ. No promises, mind.

However here is the absolutely conclusive reason for doing it synthetically rather than by induction. Doing it by induction relies on the three order-types being ordinals, but that's not why it's true. It's true for *arbitrary* linear order types. So the fact that α, β and γ are ordinals is irrelevant and shouldn't be exploited! You do it just by rearranging the brackets inside the two products.

Question 6

Check these by thinking *synthetically*. It becomes very clear very quickly. Again it's worth pointing out that the equation $\alpha\cdot(\beta+\gamma)$ holds for all linear order types not just ordinals, so it can't be right to try and prove it by induction.

Question 7

"Ordinal subtraction is defined synthetically by taking $\alpha-\beta$ to be the order-type of the set-difference $\alpha\setminus\beta$ (in particular, $\alpha-\beta=0$ whenever $\alpha\leq\beta$). Prove the following identities:

$$(\alpha+\beta)-\alpha=\beta \quad ; \quad \alpha-(\beta+\gamma)=(\alpha-\beta)-\gamma \quad ; \quad \alpha\cdot(\beta-\gamma)=\alpha\cdot\beta-\alpha\cdot\gamma \quad .$$

Show also that for any ordinal α there are only finitely many ordinals of the form $\alpha-\beta$. [Hint: consider the order-type of the set $\{\alpha-\beta:\beta\in\mathbf{On}\}$.]"

Discussion

Let's think about how to prove that $(\beta+\alpha)-\beta=\alpha$. You take a well order of length α and stick it on the end of a well order of length β. Then you remove from the bottom end a well order of

length β and what is left (the thing that is going to be of length $(\beta+\alpha)-\beta$) is obviously the thing of length α that you stuck on the end in the first place.

For this operation of ordinal subtraction to be well defined we need to be confident that when we subtract β (by chopping off an initial segment of length β) then there is only one initial segment of length β to chop off. If there is more than one, then there might be more than one answer to the question "What is $(\beta+\alpha)-\beta$'?" This is where we have to exploit the fact that we are dealing with wellorderings. After all if we try to subtract ω^* from ω^* (ω^* is ω "upside-down", the order type of the negative integers) we can get any natural number. The uniqueness we want can be had beco's we are dealing with ordinals not arbitrary linear order types.

Let's prove it.

If $\alpha \geq \beta$ then any well order $\langle A, <\rangle$ of length α has a initial segment of length β. We need this initial segment to be unique. Suppose $\langle B, <\rangle$ is a well order of length β. It is isomorphic to an initial segment of $\langle A, <\rangle$, and if it were isomorphic to more than one initial segment of $\langle A, <\rangle$ then the isomorphism between the two would give rise to an subset of A with no least element. (Think of the trajectory under the isomorphism of an element in the symmetric difference of the two initial segments). The length of the terminal segment is $\alpha - \beta$. The uniqueness of the initial segment ensures that the terminal segment is unique, so this operation is well-defined.

[*the rest of this discussion concerns the* uniqueness *of subtraction, something that was deleted from the current version of this question. I'm leaving it it in co's it's good for your soul*]

Why, for each α, are there only finitely many ordinals of the form $\alpha - \beta$? Why is this so plausible? Well, suppose that, for some α, there were infinitely many ordinals of the form $\alpha - \beta$. Then there would be infinitely many β with all the $\alpha - \beta$ distinct. Lots of β might give the same $\alpha - \beta$ so just pick the least. But then these finitely many β must form an increasing sequence. Reflect now that $\beta \mapsto \alpha - \beta$ is *decreasing* is *antimonotonic* so we would get an infinite *decreasing* sequence of values of $\beta \mapsto \alpha - \beta$.

I have struggled to find the cutest proof of this fact, but in the final analysis i decided it's best to do it by induction on ordinals.

Let α be the smallest ordinal s.t. there are infinitely many ordinals of the form $\alpha - \beta$, and let $\beta < \alpha$ be the first ordinal s.t $\alpha - \beta \neq \alpha$. Observe now that every ordinal of the form $\alpha - \delta$ is of the form $\alpha - (\beta + \gamma)$, which is to say of the form $(\alpha - \beta) - \gamma$. Now there are infinitely many ordinals of the form $\alpha - \delta$ but only finitely many of the form $(\alpha - \beta) - \gamma$.

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. This question is from Dr Russell, and I don't know what examples he had in mind. Prof Leader wants to make lots of things of order type ω and ω^* and add up finitely many of them in annoying ways. That's probably more to your taste. I think with a little work you can show, just using lots of copies of $\mathbb{N}$ and $\mathbb{N}$ upside-down (the negative integers) you can get finite antichains as wide as you like. Here's how to get an antichain of width 2^n. Take any n-bit word, and replace the 0s by ω and the 1s by ω^*, and concatenate them. (Thus, when $n = 2$ you get $\omega + \omega$, $\omega + \omega^*$, $\omega^* + \omega$ and $\omega^* + \omega^*$). 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. This

is corollary of a beautiful theorem of the late and much lamented Richard Laver. 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. This has connections with Question 14 on this sheet.

Question 9

Recall that a normal function is a function that is strictly increasing and continuous at limits.

To prove Cantor's Normal Form theorem we will need to make frequent use of the following important triviality. *On* is the collection of all ordinals. Don't worry at this stage about whether it's a class or a set.

Remark 1. *If $f : On \to On$ is normal, then for every $\beta \in On$ there is a maximal $\alpha \in On$ such that $f(\alpha) \leq \beta$.*

Proof: Let α_0 be $\mathtt{sup}\{\alpha : f(\alpha) \leq \beta\}$. By continuity of f

$$f(\alpha_0) = f(\mathtt{sup}\{\alpha : f(\alpha) \leq \beta\})$$

which, by continuity of f, is

$$\mathtt{sup}\{f(\alpha) : f(\alpha) \leq \beta\}$$

which of course is $\leq \beta$ since the ordinals are totally ordered. So α_0 is the largest element of $\{f(\alpha) : f(\alpha) \leq \beta\})$. ∎

The way into Cantor Normal Forms is to think of remark 1 as a rudimentary result of the kind "Given an ordinal β and a normal function f, $f(\alpha_0)$ is the best approximation to β from below that I can give using f." Cantor Normal form is an elaboration of this idea into a technique. Let us first minute a few normal functions to see what sort of things we can attack β with. For every $\alpha > 0$ the functions

$$\gamma \mapsto \alpha + \gamma; \qquad \gamma \mapsto \alpha \cdot \gamma; \qquad \gamma \mapsto \alpha^\gamma$$

are all normal, and each is obtained by iteration from the preceding one.

We are given β and we want to express it in terms of a normal function. Let α be some random ordinal below β. Then $\gamma \mapsto \alpha^\gamma$ is a normal function and since $\alpha < \beta$ we know by remark 1 that there is a largest γ such that $\alpha^\gamma \leq \beta$. Call this ordinal γ_0. Then $\alpha^{\gamma_0} \leq \beta$. If $\alpha^{\gamma_0} = \beta$ we stop there.

Now consider the case where $\alpha^{\gamma_0} < \beta$. By maximality of γ_0 we have

$$\alpha^{\gamma_0} < \beta < \alpha^{\gamma_0+1} = \alpha^{\gamma_0} \cdot \alpha \qquad (*)$$

We now attack β again, but this time not with the normal function $\gamma \mapsto \alpha^\gamma$ but the function $\theta \mapsto \alpha^{\gamma_0} \cdot \theta$. So by remark 1 there is a maximal θ such that $\alpha^{\gamma_0} \cdot \theta \leq \beta$. Call it θ_0. By (*) we must have $\theta_0 < \alpha$.

If $\alpha^{\gamma_0} \cdot \theta_0 = \beta$ we stop there, so suppose $\alpha^{\gamma_0} \cdot \theta_0 < \beta$, and in fact

$$\alpha^{\gamma_0} \cdot \theta_0 < \beta < \alpha^{\gamma_0} \cdot (\theta_0 + 1) = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_0} \qquad (**)$$

by maximality of θ_0.

Now $\beta = \alpha^{\gamma_0} \cdot \theta_0 + \delta_0$ for some δ_0, and we know $\delta_0 < \alpha^{\gamma_0}$ because of (**).

What we have proved is that, given ordinals $\alpha < \beta$, we can express β as $\alpha^{\gamma_0} \cdot \theta_0 + \delta_0$ with γ_0 and θ_0 maximal. If $\delta_0 < \alpha$ we stop. However if $\delta_0 > \alpha$ we continue, by attacking δ_0 with the normal function $\gamma \mapsto \alpha^\gamma$.

What happens if we do this? We then have $\delta = \alpha^{\gamma_1} \cdot \theta_1 + \delta_1$, which is to say

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \delta_1$$

One thing we can be sure of is that $\gamma_0 > \gamma_1$. This follows from the maximality of θ_0.

We now go back and repeat the process, this time with δ_1 and α rather than β and α.

Therefore, when we repeat the process to obtain:

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \delta_3$$

and so on:

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \ldots \alpha^{\gamma_n} \cdot \theta_n + \ldots$$

Now we do know that this process must terminate, because the sequence of ordinals $\{\gamma_0 > \gamma_1 > \gamma_2 > \ldots \gamma_n \ldots\}$ is a descending sequence of ordinals and must be finite, because $<_{On}$ is wellfounded.

So we have proved this:

THEOREM 1. *For all α and β there are $\gamma_0 > \ldots > \gamma_n$ and $\theta_0 \ldots \theta_n$ with $\theta_i < \alpha$ for each i, such that*

$$\beta = \alpha^{\gamma_0} \cdot \theta_0 + \alpha^{\gamma_1} \cdot \theta_1 + \alpha^{\gamma_2} \cdot \theta_2 + \ldots \alpha^{\gamma_n} \cdot \theta_n$$

■

We can also prove it by using only the first part of this proof, by extracting the largest power of α that is less than β and subtracting it—thereby obtaining something smaller—and appealing to induction.

In particular, if $\alpha = \omega$ all the θ_i are finite. Since every finite ordinal is a sum $1 + 1 + 1 + \ldots$ this means that every ordinal is a sum of a decreasing finite sequence of powers of ω.

Quite how useful this fact is when dealing with an arbitrary ordinal β will depend on β. After all, if $\beta = \omega^\beta$ then—if we run the algorithm with ω and β—all Cantor's normal form theorem will tell us is that this is, indeed, the case. Ordinals β s.t. $\beta = \omega^\beta$ are around in plenty. They are called *ϵ-numbers*. They are moderately important because if β is an ϵ-number then the ordinals below β are closed under exponentiation. The smallest ϵ-number is called 'ϵ_0'. For the moment what concerns us about ϵ_0 is that if we look at the proof of Cantor's Normal Form theorem in the case where β is an ordinal below ϵ_0 and $\alpha = \omega$ the result is something sensible. This is because, ϵ_0 being the *least* fixed point of $\alpha \mapsto \omega^\alpha$, if we apply the technique of remark 1 to some $\alpha < \epsilon_0$ the output of this process must be an expression containing ordinals below α.

I think you can also do it by wellfounded induction over $<_{On}$. (NOT by the two-flavoured induction that considers successors and limits).

Suppose every ordinal $< \alpha$ has a CNF. Then either α is a power of ω (in which case we have a CNF immediately) or it isn't ... in which case it's a sum of two smaller ordinals, and again we get a CNF. Why is it a sum of two small ordinals? beco's there is a maximal β s.t. $\omega^\beta \leq \alpha$!

In this treatment one then has to prove that the CNF one obtains is unique. (One should really do it anyway, but in the other treatment it's sort-of obvious that it's unique). I might try to find something enlightening to say about this later.

Question 10

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.

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 ordinals has cofinality ω.

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 about 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 ω, ω^ω, ω^{ω^ω} ....

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)

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 $\mathbb{N}$!

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.

Question 11

(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.

There can be no subsets of $\mathbb{R}$ that is of order-type ω_1 in the inherited order beco's the reals in it would give rise to uncountably many pairwise disjoint open intervals (the gap between the αth point and its successor, for every $\alpha < \omega_1$) contradicting separability.

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. 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 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`

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, Q14 on This Very Sheet.)

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

Question 12

This is hard. If it were me putting this sheet together i'd star it, but Prof Leader is Hungarian. Say no more. If there is a key steer on this then it's the thought that if you want $\alpha * \beta$ to be always defined then you need a principle that says that every normal function not only has a fixed point

but has arbitrarily late fixed points. It's not difficult to persuade yourself that this is true, but turning this intuition into a proof is a surprisingly tricky affair, and results in a delicate expository problem for the lecturer. Proving nthis principle properly requires an appeal to the axiom scheme of replacement. This is beco's the fixed points that you want are obtained as the sup of particular sequences of ordinals. The problem is: how do you know that those sequences actually exist? Some students will be happy with a fairly informal proof that just ignores this question in favour of just pressing on with the *idea* whereas more thoughtful (or more anxious) students may worry about the fact that we seem to need set theoretical principles that we haven't seen yet and won't see until the last quarter of the course. When i lecture this stuff i leave Q12 material until after we've seen some set theory, but perhaps i'm being over cautious: there is no one right way of doing it.

A word on motivation. Q 12 is the result of a line of thought arising from the fact that Cantor Normal Form isn't always informative. It "crashes" at ϵ_0, as you have seen. Of course you can restart at ϵ_0, using ϵ_0 as the base for your exponentiation instead of ω but then you crash at ϵ_1. And so on. What you want is a system of notation that doesn't have to have its tyres and oil changed every time you reach a fixed point for $\alpha \mapsto \omega^\alpha$. That's what the * system of notation does.

And here is the rather scary thought. How many ordinals can you notate using just the symbols '0', '*', and '+'? Obviously only countably many... and there are uncountably many countable ordinals (how many??). So at some point this system of notation will crash too. In fact *any* system of notation for countable ordinals will crash sooner or later. Look back at Q11 and your proof, by induction on countable ordinals, that for every countable α there is a set of reals of that order type. At limit α you needed a fundamental sequence for α. But you get fundamental sequences for ordinals from systems of ordinal notations (that reach that ordinal). But no system of ordinal notation covers all countable ordinals, so you cannot *uniformly* assign fundamental sequences to countable ordinals. That's why you need AC!

Look at `www.dpmms.cam.ac.uk/~tf/fundamentalsequence.pdf`. You could also look up the *Veblen hierarchy*.

Question 13

Suppose f : countable limit ordinals to countable ordinals is pressing down and 1-1. This f organises the second number class[2] into a family of disjoint descending ω^* sequences of limit ordinals ending in a successor ordinal; each member of the family is $\{f^{-n}(\alpha) : n \in \mathbb{N}\}$ for some successor α. Now join the family up by sending each successor ordinal to the last limit ordinal below it. This organises the whole of the second number class into a gigantic tree which is countably branching and of height ω. A wee bit of AC_ω is enough to secure a contradiction... specifically you prove by induction on the levels (and there are ω of them) that each level is countable

It is not hard to show that nevertheless such an f can always be found for any initial segment of the second number class. Think of a countable ordinal α. Well order $\mathbb{N}$ in order type α. Send the limit ordinal β to the βth natural in this funny order. This leaves some room, so you can repeat the process, but if you iterate ω times you reach a fixed point.

Here is Professor Leader's proof.

Let f be an injective function defined on countable limit ordinals, and "pressing-down" $f(\alpha) < \alpha$. Set β_0 to be ω. Thereafter set $\beta_{n+1} := \sup\{\alpha : f(\alpha) < \beta_n\}$. (Observe that $f(\omega) < \omega$). f is

[2]Cantor's name for the set of countable ordinals

injective, so the set of which β_n is the sup is countable, so (using AC_ω which tells us that any sup of countably many countable ordinals is countable—miniexercise: why?), β_n is countable. Then consider what f must do to $\beta_\omega := \sup\{\beta_n : n \in \mathbb{N}\}$. Need i say more.

Actually i *do* need to say a bit more. As Catherine Willis of Pembroke has been astute and unkind enuff to point out, there is a problem with the definition of β_n given above, in that n might be such that, for all α, $f(\alpha) \leq \beta_n$ might imply $\alpha \leq \beta_n$, so we have to cast our net out a little further. I might try to sort out this glitch. On the other hand i might leave it to you.

Observe that this proof works even if f is allowed to be countable-to-one. We need AC_ω but we needed it all along anyway.

This fact is a favourite fact of Prof. Leader's; it has something of the flavour of "ordinals are wellfounded" but in spades. And very useful it is too—look up *Fodor's* theorem and *Neumer's* theorem. This question contains the germ of the proofs of those two results.

I think (and you might like to prove this) that if α is any countable limit ordinal at all then, by using a fundamental sequence $\langle \alpha_n : n < \omega \rangle$ for α as in question 10, one can spin f out to last at least for the ordinals below α.

Question 14^+

This is a lovely question. When it was sprung on me the first time Prof Leader lectured this course I didn't know the answer, and it took me a long time to work it out. Once you know what the answer is, it's not *that* hard to do it, but how can you tell what this answer is? This question gives you the flavour of research mathematics.

If you are reading this then you probably didn't manage to work it out either, so you are probably in the market for a hint!

Hint: Precisely how many order-preserving injections are there $\mathbb{R} \to \mathbb{R}$?

If you want another hint you should bear in mind that any set that can be wellordered at all can be wellordered in such a way that all its proper initial segments are smaller (have lesser cardinal) than the whole set. (Can you prove this fact to our shared satisfaction?)

I have a discussion answer to this question, but i have removed the link to it in response to Prof Leader's entreaties.

Sheet 3

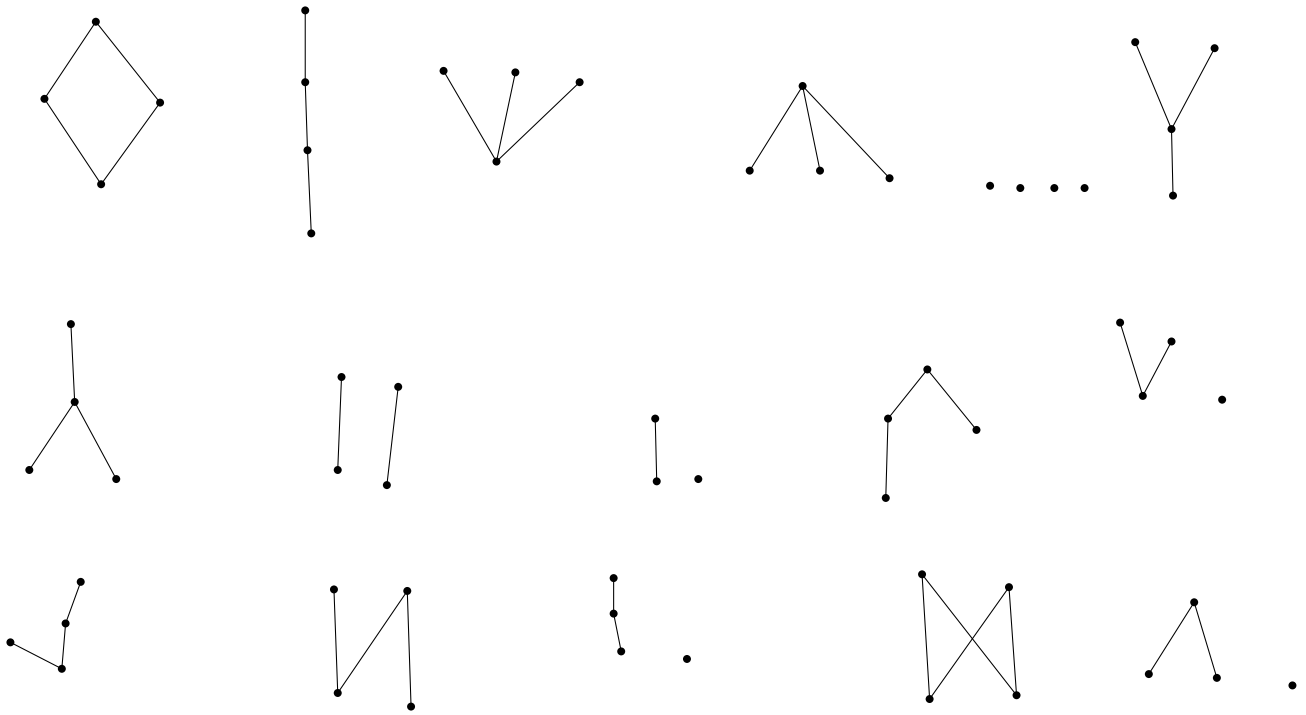
Question 1

Is there a systematic way of generating them? No easy way, that's for sure. (The set of Hasse diagrams for posets with four elements is a quotient of the set of posets with four elements and in general the cardinalities of quotients are hard to compute.) I find myself wondering how many isomorphism types of partial orders there are on a set of n elements. Not *exactly* of course, for i see no prospect for an exact formula, but it would be nice to know whether or not there is an exponential lower bound, or a polynomial upper bound. There are $2^{\binom{n}{2}}$ reflexive relations on n elements. How many of them are transitive? My guess is: exponentially many, but i have no exact figure. Let me see... How many transitive relations on $n+1$ things does a given transitive relation on n things extend to? There are $2n$ places where one might put in an edge. The only constraints arise as follows.

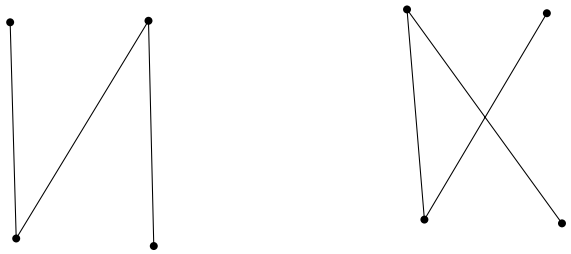
(i) Suppose there is no edge from x to y, where x and y are of the original party of n. Then we cannot have an new edge from x to a (a is our new chap) as well as a new edge from a to y.

(ii) If there is an edge from x to y and we add a new edge from y to a then we have to add a new edge from x to a.

Anyway, there are 16 isomorphism classes of posets on 4 elements, 2 of which are complete (the two with both a top and a bottom element, co's the empty subset has to have a sup!)



One of my students distinguished



. . . which are two embeddings of the same poset into the plane. This makes the same interesting point that my Pittsburgh colleague Ken Manders likes to make. When you formalise (= represent something concretely, or *concretise*) you add extra structure and this structure may be spurious. However I don't think this was the point that the question setters were trying to make. . . apparently the *real* reason for this question is that you weren't taught about Hasse diagrams in 1a. What is the world coming to??

There is a general question here: *How do i know when i've got them all?* This particular instance (before us) of this *general* question isn't *so* hard that we are prompted to think much about the general question, but a bit of thought won't go amiss. The answer of course is that you have to find a fairly robust way of thinking of these things as mathematical objects and then find a way of classifying them. In this case the obvious thing to do is to identify them with their Hasse diagrams and then classify them—perhaps—in terms of the number of edges they have. But the question still lurks in the shadows: "How can i give a *mathematical* proof that i have got all of them?"

Question 2

Which of the following posets are complete?

(i) The set of finite and cofinite subsets of $\mathbb{N}$, ordered by inclusion.

It's not a complete poset, since the set $\{\{1\},\{3\},\{5\},\ldots\}$ does not have a supremum. That example also shows that it is not chain-complete.

(ii) The set of independent subsets of a given vector space.

The two elements $\{(1,0),(0,1)\}$ and $\{(1,0),(1,1)\}$ do not have a supremum, since any upper bound must include their union, and that is not linearly independent. However the collection of independent subsets of a vector space is of course *chain*-complete.

(iii) The set of subspaces of a vector space, ordered by set-inclusion.

This poset is complete. The supremum of any subset is the subspace spanned by the union of its elements.

(Observe that the *sup* and *inf* of this complete poset do not distribute. This is beco's **inf** is "honest" [it's just $\bigcap$] but **sup** is not: it's sometimes bigger than $\bigcup$.)

Question 3

The nicest and most natural example of an order-reversing map with no fixed point is complementation in a boolean algebra.

For the second part, if f is an order-reversing function from a complete poset into itself then f^2 is order preserving and has a fixed point.

Why on earth would you be looking for an order-reversing function to have a fixed point? More often than you might think. (And I don't just mean trivial cases like 1/2 is a fixed point for the order-reversing function $x \mapsto (1-x)$.) If you think a *species* in Biology is defined in terms of "can mate to produce viable offspring" you rapidly discover a characterisation in terms of fixed points for an order-reversing function. Have a look, too at this old tripos question (It was 2002:B2:11b).

1. State Zorn's lemma.

2. Let U be an arbitrary set and $\mathcal{P}(U)$ be the power set of U. For X a subset of $\mathcal{P}(U)$, the **dual** $X^\vee$ of X is the set $\{y \subseteq U : (\forall x \in X)(y \cap x \neq \emptyset)\}$.

3. Is the function $X \mapsto X^\vee$ monotone? Comment.

4. By considering the poset of those subsets of $\mathcal{P}(X)$ that are subsets of their duals, or otherwise, show that there are $X = X^\vee$.

5. What can you say about the fixed points of $X \mapsto X^\vee$ on the assumption that U is finite?

Question 4

Give the set of partial orders on S the containment partial order as subsets of $S \times S$. The resulting partial order is chain-complete, since the union of a nested sequence of partial orders is still a partial order. To see this, let $\leq_n$ be a nested sequence of partial orders. The union partial order $\leq$ is clearly reflexive. It is antisymmetric because $x \leq y$ and $y \leq x$ if and only if $x \leq_n y$ and $y \leq_m x$ for some m, n, and then it follows that $x =_{\max(m,n)} y$, whence $x = y$. Similarly, it is reflexive because $x \leq y$ and $y \leq z$ if and only if $x \leq_n y$ and $y \leq_m z$ for some m, n, and then it follows that $x \leq_{\max(m,n)} z$, whence $x \leq z$.

By Zorn's lemma, it follows that there exists a maximal partial order $\leq'$ containing any given partial order $\leq$ on S. For any $x, y \in S$, if x, y are incomparable then $\leq'$ is not maximal since we can take the transitive closure of $\leq'$ together with the relation $x \leq y$ to obtain a partial order strictly containing $\leq'$, so x, y are comparable and $\leq'$ is a total order.

You can also do it by considering the poset of **total** orders of subsets of S that are compatible with the given partial ordering.

Question 5

Zorn's Lemma for countable posets.

You use the enumeration to ensure that the process of trying to reach a maximal element will succeed in finitely many steps.

Let $\langle X, \leq_X \rangle$ be a countable chain-complete poset. Enumerate X as $\langle x_i : i \in \mathbb{N} \rangle$. Build a $\leq_X$-chain the subscripts of whose elements form an $\leq_{\mathbb{N}}$-increasing sequence. First one is x_0, thereafter if the x-in-hand is maximal, then `HALT`; `else` plonk on the end that x which is $\geq_X$ the x-in-hand which has $\leq_{\mathbb{N}}$-minimal subscripts. If this doesn't `HALT` in finitely many steps the resulting chain has an upper bound and one obtains a contradiction by enquiring about the subscript on the upper bound.

Question 6

$\Leftarrow$: AC implies Zorn's lemma, which we then apply to the chain-complete poset of partial bijections between two given sets.

$\Rightarrow$: Let X be a set. By Hartogs' lemma, there exists a well-ordered set α with no injection $\alpha \to X$. It follows that there exists an injection $X \to \alpha$ which identifies X with a subset of α, which is itself well-ordered; thus X can be well-ordered.

Let S_i be a collection of sets indexed by an index set I, and choose a well-ordering on $\bigcup S_i$. For every i, let $f(i)$ be the least element of S_i relative to this well-ordering. Then $f(i)$ is a choice function.

Question 7

Zorn's lemon. *Alternative answer:* The Wellordering Pineapple.

The subtext to this (as one of you were good enough to point out) is that it is *cowardly* to use Zorn's lemma. But perhaps *lazy* would be better.

Question 8

(i): Fields of Characteristic 2

The language has $\Omega = \{+, \times, 0, 1\}$ with arities $2, 2, 0, 0$ and $\Pi = \emptyset$. The theory can be described by the following axioms:

$$(\forall x)(\forall y)(x + y = y + x)$$
$$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$$
$$(\forall x)(x + 0 = 0)$$
$$(\forall x)(\forall y)(x \times y = y \times x)$$
$$(\forall x)(\forall y)(\forall z)((x \times y) \times z = x \times (y \times z))$$
$$(\forall x)(x \times 1 = x)$$
$$(\forall x)(x \neq 0 \to (\exists y)(x \times y = 1))$$
$$(\forall x)(\forall y)(\forall z)(x \times (y + z) = x \times y + x \times z)\ 1 + 1 = 0.$$

(ii): Posets with no maximal element

The language has $\Omega = \emptyset$ and $\Pi = \{\leq\}$ with arity 2. The theory has the following axioms:

$$(\forall x)(x \leq x)$$
$$(\forall x)(\forall y)((x \leq y \wedge y \leq x) \to x = y)$$
$$(\forall x)(\forall y)(\forall z)((x \leq y \wedge y \leq z) \to x \leq z)$$
$$(\forall x)(\exists y)(x \leq y \wedge x \neq y)$$

Be alert to the difference between maxi**mal** elements and maxi**mum** elements.

(iii): Bipartite graphs

There are two correct answers.

(i) With a colour predicate:

The language has $\Omega = \emptyset$ and $\Pi = \{\sim, B\}$ of arities $2, 1$. The theory has the following axioms:

$(\forall x)(\forall y)(x \sim y \longleftrightarrow y \sim x)$
$(\forall x)(\forall y)(x \sim y \to (B(x) \wedge \neg B(y)) \vee (B(y) \wedge \neg B(x)))$

(ii) But you can also do it without the colour predicate, by asserting that there are no cycles of odd length. This needs infinitely many axioms. You might like to prove that bipartite graphs cannot be finitely axiomatised in the language of graph theory: it's a useful compactness exercise of the kind that you might meet in an exam

(iii) Actually there is a third correct answer which I hadn't considered, but which one of my students came up with. You could have a two-sorted language rather in the way that we might naturally have a two-sorted language for vector spaces. You have one set of variables for ranging over vertices, and another style of variable that ranges over colours. This is a much richer language and you can easily describe much more than just bipartite graphs. If you want a bipartite graph you have an axiom that says there are precisely two colours...

This method is of course extravagant, but the comparison between it and the method with a single colour predicate comes in useful later, with real vector spaces (part vii of this question). In part vii the analogue of method three doesn't work: you have to do it by method one. But that's for later.

(iv): Algebraically Closed Fields

The language has $\Omega = \{+, \cdot, -, 0, 1\}$ with arities $2, 2, 1, 0, 0$ and $\Pi = \emptyset$. The theory has the following axioms:

$(\forall x)(\forall y)(x + y = y + x)$
$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$
$(\forall x)(x + 0 = 0)$
$(\forall x)(x + (-x) = 0)$
$(\forall x)(\forall y)(x \cdot y = y \cdot x)$
$(\forall x)(\forall y)(\forall z)((x \cdot y) \cdot z = x \cdot (y \cdot z))$
$(\forall x)(x \cdot 1 = x)$
$(\forall x)(x \neq 0 \to (\exists y)(x \cdot y = 1)$
$(\forall x)(\forall y)(\forall z)(x \cdot (y + z) = x \cdot y + x \cdot z)$
$(\forall a_0) \ldots (\forall a_n)(\exists x)(a_{n+1} \cdot x^{n+1} + a_n \cdot x^n + \ldots + a_0 = 0)$.

where the last axiom is understood as an axiom scheme ranging over all positive integers n.

(v): Groups of Order 60

The language has $\Omega = \{\cdot, ^{-1}, 1, g_1, g_2, \ldots g_{60}\}$ with arities $2, 1, 0, 0, \ldots 0$ and $\Pi = \emptyset$. The theory can be axiomatised as follows:

$(\forall x)(\forall y)(\forall z)(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
$(\forall x)(x \cdot 1 = 1 \cdot x = x)$
$(\forall x)(x \cdot x^{-1} = x^{-1} \cdot x = 1)$
$(\forall x)(x = g_1 \vee x = g_2 \vee \ldots \vee x = g_{60})$
$g_i \neq g_j$ for all $i \neq j$ (a scheme)

(vi): Simple Groups of Order 60

You might think you can use group presentations to axiomatise the theory of simple groups of order 60, but it's less than completely straightforward.

It's true that writing

$$\langle a^2 = b^3 = (ab)^5 = 1 \rangle$$

in some sense captures A_5 but it isn't enough by itself, since it appeals to the implicit information that no other equations hold, and that isn't first-order. Somehow you have to ensure that everything is in the group generated by a and b and you also have to ensure that no extra equations hold. The second point can be addressed by ensuring that there are 60 elements but that isn't much use unless we ensure that all those extra elements are denoted by words in a and b.

It may be that saying there are precisely 60 elements and every element is of order 2,3 or 5 and there are elements of all those orders is enough. I don't know enough group theory.

However something has emerged recently which is that, in every finite simple group, every element is a commutator. My guess is that the converse is true too, namely that every group where every element is a commutator is simple. If that's true then you add to the axioms of Group theory something to say that there are exactly 60 elements and

$$(\forall x)(\exists yz)(x = yzy^{-1}z^{-1})$$

Anyway the moral is that when you are trying to find a first-order axiomatisation of something that is obviously second-order you can—sometimes—cheat.

(vii): Real vector spaces

The language has $\Omega = \{+, -, 0\} \cup \{m_r : r \in \mathbb{R}\}$ with arities $2, 1, 0, 1, 1, \ldots$ and $\Pi = \emptyset$. The theory has the following axioms:

$(\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z)$
$(\forall x)(\forall y)(x + y = y + x)$
$(\forall x)(x + 0 = x)$
$(\forall x)(x + (-x) = 0)$
$(\forall x)(\forall y)(m_r(x + y) = m_r(x) + m_r(y))$
$(\forall x)(m_{r+s}(x) = m_r(x) + m_s(x))$
$(\forall x)(m_{rs}(x) = m_r(m_s(x)))$

where the last three axioms are understood as axiom schemata ranging over all $r, s \in \mathbb{R}$.

Question 9

Discussion

(i)

I'm assuming that the reader has discovered the back-and-forth construction. I can't be bothered to explain it here, co's it's best done interactively in real time.

It is fairly easy to use the denseness of the rationals to show that every countable linear order can be embedded (in an order-preserving way) into $\mathbb{Q}$. Think of your countable total order as

the members of $\mathbb{N}$ written in a funny order, and then find homes for the natural numbers one by one. That's OK but sadly it isn't quite enough, co's it goes only one way. You might next think "Suppose I have two countable dense linear orders ... I can embed each in the other—so I can then use Cantor-Bernstein!" That doesn't work, beco's Cantor-Bernstein works for *cardinals* not for linear order types—they're far too delicate. (After all, each of the two half-open intervals $(0, 1]$ and $[0, 1)$ embeds in the other but the two are not isomorphic.) So rather than build two embeddings separately, you *interleave* the two constructions in such a way that you construct a single isomorphism—a bijection.

Mind you, there actually *is* a version of Cantor-Bernstein for total orders, even tho' it is no use to us here. If A is iso to a terminal segment of B and B is iso to an initial segment of A then A and B are iso... Actually this is really a theorem about circular orders.

A follow-up thought...

Look at this once you've done sheet 4. Now that you have done ordinals and know what $\aleph_1$ is—the size of the set of countable ordinals—you might like to think about a generalisation of the fact that by a back-and-forth argument you can show that any two countable dense linear orders without endpoints are isomorphic. There is a theorem that says that any two dense linear orders of size $\aleph_1$ without endpoints are isomorphic (by a back-and-forth argument) as long as as they both satisfy a special extra condition. What is that extra condition?

(ii)

QY sez: "No to part (ii). Adjoin to the language a constant c and adjoin to the axioms of Peano arithmetic the sentences $0 < c$, $s(0) < c$, $s(s(0)) < c$, ...to obtain a new theory S. Each finite subset of S has a model, so by compactness S has a model, which is of course infinite. By downward Löwenheim-Skolem, it has a countable model $\mathfrak{M}$. In $\mathfrak{M}$ there is an element c which is greater than 0, $S(0)$, $S(S(0))$ ...but there is no such element in the standard model $\mathbb{N}$, so $\mathfrak{M}$ is a nonstandard countable model of Peano arithmetic."

Thanks for this QY, but classroom experience teaches me not leave it at that. Very well, so we have a model of arithmetic with an extra element. But it doesn't stop there. PA proves a whole lot of theorems saying that $\mathbb{N}$ is closed under a lot of operations: $x \mapsto x^2$, $x \mapsto \lceil 22x/7 \rceil$, $x \mapsto \lceil \sqrt{x} \rceil$ and so on. It is probably quite helpful to think of our model as something containing 0 and c and *generated by them*. At its most basic it is a theorem of the arithmetic of $\mathbb{N}$, after all, that every number has a successor—and that every nonzero number has a predecessor—so we must have $c+1$ and $c-1$. This leads us to the conclusion that c belongs to a copy of $\mathbb{Z}$ stuck on the end of $\mathbb{N}$. Only one copy...? What about $\lceil 22c/7 \rceil$, $\lceil 355c/133 \rceil$ ...? In fact a copy of $\mathbb{Z}$ for every rational!

This has the striking (but as far as i know, useless) consquence that all countable nonstandard models of PA are isomorphic as ordered sets. So every countable nonstandard model of PA has order type $\mathbb{N}+ \mathbb{Q}\cdot\mathbb{Z}$. You might think that you get *more* than $\mathbb{Q}$ copies of $\mathbb{Z}$ beco's of $\lceil \sqrt{c} \rceil$ but—as noted above, $\mathbb{Q}$ is a maximal countable linear order type so you don't get any further copies of $\mathbb{Z}$ by considering $\lceil \sqrt{c} \rceil$. Of course they aren't all isomorphic as structures for $+$ and $\times$—beco's arithmetic is incomplete.

I have just learnt the curious fact that every countable nonstandard model of PA is isomorphic to a proper initial segment of itself!

One point one sometimes has to make in this connection is that these wild and woolly things—

the nonstandard naturals—living in the desolate marches beyond the standard naturals are absolutely **not** the same wild and woolly things living in the desolate marches beyond ω, namely the countable ordinals. This mistaken identification is a common consequence of over-enthusiastic fault-tolerant pattern matching by beginners.

Question 10

Easy to show that the theory of fields of characteristic 0 is axiomatisable. Merely add the scheme

$$\underbrace{1+1+\ldots+1}_{p \text{ times}} \neq 0 \qquad \text{for each } p$$

to the field axioms.

Slightly harder to show that it is not *finitely* axiomatisable. We exploit the following trivial fact:[3] Suppose T is a theory with an infinite axiomatisation A such that no finite subset of A axiomatises T. Then T has no finite axiomatisation. For suppose it did. Let ϕ be the conjunction of the finite set of axioms. We have $A \vdash \phi$. Then, by compactness, we have $A' \vdash \phi$ for some finite $A' \subseteq A$. But this, by hypothesis, we do not have. Observe that the above axiomatisation of the theory of fields of characteristic 0 is an infinite axiomatisation no finite subset of which suffices so we can exploit the trivial fact.

There is a temptation to think that if the theory of fields of characteristic 0 has a finite axiomatisation then it has one in which the field axioms are separately itemised, so that the remaining axioms can be conjoined into a single axiom which in effect says "the field is of characteristic 0". Then you replace this axiom by its negation to obtain an axiomatisation of the theory of fields of positive characteristic, which of course is impossible. This can in fact be made to work, but it is not as straightforward as the proof i have just given. How can we be sure we can corral off the field axioms in this way? There is some work to do. Let our finite axiomatisation be the single formula ϕ. ϕ certainly implies the conjunction—F, say—of the field axioms. Now replace the single axiom ϕ with the two axioms $F \to \phi$ and F.

Are we now home and hosed? The candidate theory of fields of positive characteristic we obtain will be the field axioms F plus the negation of the remaining axiom $F \to \phi$. This negation is $F \wedge \neg\phi$, so this amounts to adding $\neg\phi$ as an axiom. Clearly no model $\mathfrak{M}$ of $F \wedge \neg\phi$ can be a model of ϕ so $\mathfrak{M}$ must be a field [beco's $\mathfrak{M} \models F$] and a field of positive characteristic. Converse? Let $\mathfrak{M}$ be a field of positive characteristic. It's a model of F, because it's a field, but it can't be a model of ϕ beco's it isn't of characteristic 0. So $\{F, \neg\phi\}$ would be an axiomatisations of the theory of fields of positive characteristic [which we know to be impossible] so there really is no such ϕ.

Question 11

No. You can add a constant symbol and appeal to compactness.

[3] I know it is trivial beco's i worked this out for myself when i was a mere philosophy student... a much lower lifeform than *you*, Dear Reader!

Question 12

A group with an element of infinite order.

The language has $\Omega = (\cdot, ^{-1}, 1, g)$ with arities $2, 1, 0, 0$ and $\Pi = \emptyset$. The theory can be described by the following axioms:

$$(\forall x)(\forall y)(\forall z)(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$$
$$(\forall x)(x \cdot 1 = 1 \cdot x = x)$$
$$(\forall x)(x \cdot x^{-1} = x^{-1} \cdot x = 1)$$
$$\overbrace{g \cdot g \cdot \ldots \cdot g}^{n \text{ times}} \neq 1 \text{ (for each } n \in \mathbb{N})$$

Can this be done purely in the language of groups? The answer Prof. Leader wants is 'no' and he is obviously correct, as we will see. However, Prof. Leader is a mere mortal (tho' he might not appear to be, on cursory inspection) and the question contains a mistake. Since it is possible to axiomatise group theory just in the language with a single binary function symbol, you can go ahead and do it that way and—since you now no longer need the symbol 'e' to denote the unit—you can recycle that symbol to denote the element of infinite order! But that's cheating, and the student who did it has been granted name supression.

There now follows a proof of the impossibility of doing this in the language of groups, reconstructed from a recent conversation i had with Prof Leader.

The key is to find two groups one of which has an element of infinite order and the other does not, and yet the two groups are elementarily equivalent (indistinguishable by first-order expressions). To this end consider a group with elements of arbitrarily large finite order but no elements of infinite order. The group FSymm($\mathbb{N}$) of permutations of $\mathbb{N}$ that move only finitely many things will do nicely. Now consider the theory $T = Th(\text{FSymm}(\mathbb{N}))$ consisting of all the expressions in the language of group theory that hold in this group. This theory might not have a decidable set of axioms, but it doesn't matter. What *does* matter—indeed is absolutely crucial—is that it is a **complete** theory. We now add a constant g to the language, and the obvious axioms $g^n \neq e$, for all $n \in \mathbb{N}$. Call the resulting theory T'. T' is clearly consistent by compactness and must have a model, which will be a group, call it G. G is a model of the complete theory $Th(\text{FSymm}(\mathbb{N}))$ and is therefore elementarily equivalent to FSymm($\mathbb{N}$). But G has an element of infinite order and FSymm($\mathbb{N}$) does not.

It doesn't much matter that we took our group to be FSymm($\mathbb{N}$). Any group with elements of arbitrarily large finite order but none of infinite order will do.

This works, and it's very pretty, but it's a bit *ad hoc*. Nathan Bowler points out to me that the additive group of the rationals mod 1 ("the rational circle") has no element of infinite order (p/q is of order q) but the reals mod 1 ("the real circle") has elements of infinite order. My guess is that these two groups are elementarily equivalent, and indeed that the inclusion embedding is elementary. By this we mean that, for any expression $\phi(\vec{x})$ in the language of groups, if $\phi(\vec{p})$ holds of some tuple $\vec{p}$ in the additive group of the rationals mod 1, then it holds of the same tuple of rationals in the bigger group of reals mod 1. I might get round to writing out a proof. If it works (and i'm not making any promises) it would be a nicer proof than Prof Leader's (although it's much more involved) beco's it is an introduction to a new technique.

Question 13

I tried to persuade Prof Leader that this question should be starred. He agrees that it's hard, but he says it's not *quite* hard enuff for a star.

The theory T has the following axioms:

$$(\forall x)(\forall y)(f(x) = f(y) \to x = y)$$
$$(\forall y)(\exists x)(f(x) = y)$$
$$(\forall x)(\overbrace{f(f(f\cdots}^{n \text{ times}}(x)\cdots)) \neq x) \text{ (for each } n \in \mathbb{N})$$

Any countable model $\mathfrak{M}$ of T is a disjoint union of at most countably many f-cycles, all of which are of the form $\{\ldots f^{-2}(x),\ f^{-1}(x),\ x,\ f(x),\ f^2(x),\ \ldots\}$ for some x.

Imagine you are living in a world where there is nothing going on other than lots of points joined together by f edges, and all you can ever do is move along f edges (in either direction) from one point to another. What do you discover? By the end of time you have discovered that you are living on a copy[4] of $\mathbb{Z}$. At that's *all* you have discovered: if the model contains another copy of the $\mathbb{Z}$-gon that you could have been on you never learn this fact. There is no way, in the given language, of saying that two vertices lie on distinct $\mathbb{Z}$-gons.

This is an informal picture and is definitely not a proof, but it might lead us to one.

I think that the model consisting of a single copy of $\mathbb{Z}$ is what they call a **prime model**: it injects elementarily into all models of T. Presumably we use quantifier-elimination.

This could serve as an introduction to *Ehrenfeucht Games* but i can't go into that sort of detail here.

But there is a proof using only techniques available to you. (There must be, since this question isn't starred.) You observe that, altho' T can have nonisomorphic *countable* models (one, two or many copies of $\mathbb{Z}$), all its models of size $2^{\aleph_0}$ are isomorphic. This may not be immediately obvious. If $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are two models both of size $2^{\aleph_0}$ then they both consist of $2^{\aleph_0}$ $\mathbb{Z}$-gons. (A detailed proof of this fact needs a little bit of AC but i'll spare you the details). So there is a bijection between the (set of) $\mathbb{Z}$-gons-in-$\mathfrak{M}_1$ and the (set-of) $\mathbb{Z}$-gons-in-$\mathfrak{M}_2$. This isn't *quite* a bijection between M_1 and $\mathfrak{M}_2$, but we are nearly there. All we have to do is pick, for each pair of a-$\mathbb{Z}$-gon-in-$\mathfrak{M}_1$-with-a-$\mathbb{Z}$-gon-in-$\mathfrak{M}_2$, a digraph isomorphism between the two $\mathbb{Z}$-gons, and take the union of all those isomorphisms. This union will be an isomorphism between $\mathfrak{M}_1$ and $\mathfrak{M}_2$.) If T were not complete we would be able to find ϕ such that $T \cup \{\phi\}$ and $T \cup \{\neg\phi\}$ were both consistent. Add $2^{\aleph_0}$ constants and deduce (by compactness) that $T \cup \{\phi\}$ and $T \cup \{\neg\phi\}$ both have models of size at least $2^{\aleph_0}$. Indeed (by downward Skolem-Löwenheim) they must both have models of size *precisely* $2^{\aleph_0}$. These models would have to be nonisomorphic beco's one of them believes ϕ and the other believes $\neg\phi$. But they are both models of T so they are isomorphic.

Sometimes students can be *soooo* annoying. The point of this question (as you have probably guessed by now) is to direct your attention to theories that are categorical in some *un*countable cardinal. However there is a way of answering this question that doesn't exploit this possibility, and some of you found it. That was not in the script at all. Grrr! Suppose $T \vdash \phi$ and $T \nvdash \neg\phi$. Add countably many constants to the language of T, and add axioms to $T \cup \{\phi\}$ and to $T \cup \{\neg\phi\}$ to

[4] Actually it's not really $\mathbb{Z}$ beco's $\mathbb{Z}$ has additive and multiplicative structure, which this thing hasn't. It's really just a digraph. One might call it the $\mathbb{Z}$-**gon**.

say that the denotations of these constants all belong to different $\mathbb{Z}$-gons. These two theories both have countable models by downward Skolemheim, but in both cases there is only one countable model, and it consists of countably many $\mathbb{Z}$-gons with a distinguished element in each $\mathbb{Z}$-gon. But there is only one such model up to isomorphism!!

Question 14

(i) The Theory of connected graphs (in the language of graphs)

One way of doing this is to add two constants and axioms to say, for each n, that the two constants are at least n links apart. Better still is to do without the constants and add to the putative theory of connected graphs axioms to say that precisely two vertices have degree 1 and every other vertex has degree 2. Is there is a first-order theory of connected graphs this theory will be consistent, and it will have arbitrarily large finite models, whence infinite models by compactness. But it has no infinite models (there are no infinite connected graphs wherein precisely two vertices have degree 1 and all the other have degree 2.)

(ii) The Theory of Simple Groups (in the language of groups)

The theory of simple groups is not first-order. If it were, the theory of abelian simple groups would be first order. Then we could argue: there are arbitrarily large finite abelian simple groups (the cyclic groups of order p, p prime), so there must be an infinite abelian simple group. But there isn't: every subgroup of any abelian group is normal!

(iii)$^+$

The Theory of Nonabelian Simple Groups (in the language of groups)

I owse you all an apology. The original version of this starred question was "Show that the theory of simple groups is not axiomatisable". I pointed out to Prof Leader that the way to establish that is to say that if it were axiomatisable one could add the axiom for abelianness and get a theory of abelian simple groups. This theory has arbitrarily large finite models (cyclic groups of order p) but no infinite models (every subgroup of an abelian group is normal) and that contradicts compactness. So Prof Leader inserted the word 'nonabelian'. As i say, my apologies.

I can't see how to show that the theory of nonabelian simple groups isn't first-order without using ultraproducts. My hint is to go and learn about ultraproducts. You could buy my *Logic, Induction and Sets*; you could read Bell-and-Slomson or you could just ask wikipædia!

Accordingly we appeal to the fact that the ultraproduct of a collection of models of a first-order theory T is a model of T (which follows from Łoś's theorem).

Let U be a non-principal ultrafilter on $\mathbb{N}$.)

(This is Q.C's answer).

Fix a prime p and let $G = \prod \mathrm{PSL}_{n+1}(p)/U$. The normal closure of the subgroup generated by elements of the form $\prod E_{n+1}$ where each E_i is an elementary matrix cannot be all of G. Indeed, as $n \to \infty$, there exist matrices which cannot be written using fewer than any given number of elementary matrices (for example upper triangular matrices with 1s on the diagonal and 1s on the superdiagonal). It follows that the ultraproduct of non-abelian simple groups is not necessarily simple.

Here is another proof:

For each $i \in \mathbb{N}$ consider $[1, i]$ (aka $\{k \in \mathbb{N} : k \leq i\}$), and let $\mathfrak{M}_i$ be this set equipped with all even permutations. This is A_i, a simple group. Take an ultraproduct over all the $\mathfrak{M}_i$ for $i \in \mathbb{N}$. This ultraproduct will be an infinite set (basically the carrier set of a nonstandard model of arithmetic) with a group of permutations sitting atop it. This group will not be simple, because the group of elements of finite support (which in fact is the direct limit of the alternating groups) is a nontrivial normal subgroup.