Discussion Notes for Prof Leader's 2018 Examples Sheets

Thomas Forster

February 18, 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.

Some of the questions on Prof. Leader's sheet are the same as some of the questions on Prof. Johnstone's sheets ... or mine, for that matter. (Great minds think alike). Where such duplication arises the reader will be directed to the first appearance of the question.

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.

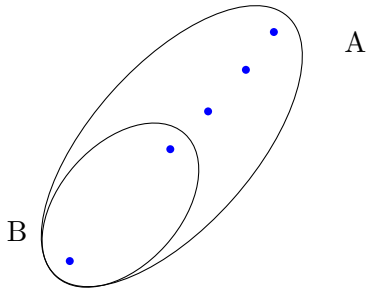
There is a more subtle, more beautiful and more enlightening—but much harder—proof using Curry-Howard, but we probably won't get round to it. However, if we *did* get round to talking about Curry-Howard in the supervision then the remainder of this section will make sense to you. I wrote it up from a 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.



The pigeonhole principle now tells us that, for any function $f : A \to B$, there is a unique $b \in B$ such that $|f^{-1}\text{“}(\{b\}) \cap (A \setminus B)| \geq 2$. (A unique member of B that is hit by at least two members of $A \setminus B$). 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.