Starred exercises have model answers. The following relevant tripos questions also have model answers in the answer file.

Maths tripos questions
1988:6:9E, 1988:6:10E, 1995:5:4X,
Comp Sci tripos questions
1990:1:9, 1990:1:11, 1993:11:11, 1994:10:11, 1996:1:8

1 Some Nice Structured Proof Exercises

You will not need to use the contradiction rule for any of these.

(1)

Find structured proofs of the following. They are in increasing order of difficulty, and the later ones are really quite hard. Nicely LaTeX-ed correct answers to (5) and (6) earn a bottle of college port each. Even .pdfs of JAPE output will be acceptable.

1. $\neg(\exists x)(\forall y)(R(y,x) \longleftrightarrow \neg R(y,y))$;
2. $(\forall x)[(\forall y)(R(y,x) \rightarrow \neg(\forall z)R(z,y)) \ \rightarrow \ \neg((\forall w)R(w,x))]$.
3. $(\exists x)(\forall y)(R(y,x) \longleftrightarrow (R(y,y) \rightarrow p)) \rightarrow p$

   (This is just a spiced up version of (1). Simrun Basuita has suppplied a .ps file of a JAPE proof)
4. "Everybody loves my baby, but my baby loves nobody but me".

   Formalise this in first-order logic, and then construct a structured proof with your formula as a premiss, and "my baby = me" as a conclusion.
5. Now this one is quite tough. If you can get on top of this one you are doing very well! It is recommended only for structured-proof-geeks. Find a structured proof of:

   $$\neg(\exists x)(\forall y)(R(y,x) \longleftrightarrow \neg(\exists z)(R(y,z) \wedge R(z,y))).$$
6. This one is only for structured-proof-geeks. It is seriously nasty. No, really!

   Find a proof of the sequent

   $\forall x \exists y R(x,y) \ \rightarrow \ (\forall x_1)(\exists y_1)(\forall x_2)(\exists y_2)(R(x_1,y_1) \wedge R(x_2,y_2) \wedge (x_1 = x_2 \rightarrow y_1 = y_2))$

2 Elementary

"Elementary" doesn't mean 'easy'. It means that on the whole for the questions in this section no very sophisticated ideas are needed.

2.0.1 Exercises on (binary) relations

1. (Do not do more than a sample of the bits of this question: if you are making any mistakes they will always be the same mistakes, and there is no point in making the discovery more than once!)

   Given the operations of composition and union, express the following relations in terms of brother-of, sister-of, father-of, mother-of, son-of, daughter-of. (You may use your answers to earlier questions in answering later questions.)

   (a) i. parent-of
   ii. uncle-of
   iii. aunt-of
   iv. nephew-of
   v. niece-of
   vi. grandmother-of
   vii. grandfather-of
   viii. first-cousin-of

   You can also express some of the relations in the original list in terms of others by means of composition and union. Do so.

   (b) Do the same to include all the in-law and step relations, by adding spouse-of to the original list. This time you may use intersection and complement as well.

   (c) If the formalisation of "x is a parent of y" is "(father-of$(x, y) \vee$mother-of(x, y))" (i.e., use logical connectives not $\cup$ and $\cap$. You will also need to use quantifiers) what is the formalisation of the other relations in the preceding list? And for a bonus point, formalise "x is the double cousin of y".[1] Hint: might need new variables!

   (d) Using the above gadgetry, plus set inclusion ("$\subseteq$") formalise

   i. Every mother is a parent.
   ii. The enemy of [my] enemy is [my] friend
   iii. The enemy of my friend is my enemy.
   iv. The friend of my enemy is my enemy.
   v. no friend is an enemy

[1] Fred and Bert are double cousins if they are first-cousins in two different ways.

2. What is a graph? How many graphs are there on n vertices?

3. When doing this question remember that relations are relations-in-extension. You will find it helpful to think of a binary relation on n things as an $n \times n$ matrix whose entries are **true** or **false**.

   (a) How many binary relations are there on a set of size n?

   (b) How many of them are reflexive?

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

   (d) How many of them are symmetrical?

   (e) How many of them are antisymmetrical?

   (f) How many are total orders?

   (g) How many are trichotomous? (A relation R on X is *trichotomous* iff $(\forall x, y \in X)(\langle x, y\rangle \in R \vee \langle y, x\rangle \in R \vee (x = y))$.

   (h) How many are antisymmetrical and trichotomous?

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

   (j) (for the thoughtful student) If you have done parts 3h and 3d correctly the answers will be the same. Is there a reason why they should be the same? (Revisit this later in connection with *natural bijections*.)

   (k) What is a partial order? *Do not answer the rest of this question.* How many partial orders are there on a set of size n?

   (l) *Do not answer this question.* A *strict* partial order is a transitive relation R satisfying

   $$(\forall x \forall y)(\neg R(x, y) \vee \neg R(y, x))$$

   How many strict partial orders are there on a set of size n?

   (m) Should the answers to the two previous questions be the same or different? Give reasons. (Compare this with your answer to question 3j above.)

   (n) An *extensional* relation on a set X is a binary relation R satisfying

   $$(\forall x, y)(x = y \longleftrightarrow (\forall z)(zRx \longleftrightarrow zRy))$$

      i. If R is extensional is R^{-1} also extensional?

      ii. How many extensional relations are there on a set of size n?

      iii. Show that the proportion of relations on a set with n members that are extensional tends to 1 as $n \to \infty$.

(o) The five properties *symmetrical*, *transitive*, *reflexive*, *trichotomous*, *antisymmetrical* give rise to 2^5 possible combinations of properties. In each case find relations exhibiting the appropriate combination of properties or explain why there cannot be one. On second tho'rts do this only for a random sample of such combinations, or you will exhaust your supervisor's patience!

4. Can a relation be both symmetrical and antisymmetrical?

5. * Write out a formal proof that the intersection of two transitive relations is transitive.

6. * Let R be a relation on A. ('r', 's' and 't' denote the reflexive, symmetric and transitive closure operations respectively.)

   (a) Prove that $rs(R) = sr(R)$.

   (b) Does R transitive imply $s(R)$ transitive?

   (c) Prove that $rt(R) = tr(R)$ and $st(R) \subseteq ts(R)$.

   (d) If R is symmetrical must the transitive closure of R be symmetrical? Prove or give a counterexample.

7. Think of a binary relation R, and of its graph, which will be a directed graph $\langle V, E\rangle$. On any directed graph we can define a relation "I can get from vertex x to vertex y by following directed edges" which is certainly transitive, and we can pretend it is reflexive because after all we can get from a vertex to itself by just doing nothing at all. Do this to our graph $\langle V, E\rangle$, and call the resulting relation S. How do we describe S in terms of R?

8. * Show that—at least if $(\forall x)(\exists y)(\langle x, y\rangle \in R)$—$R \circ R^{-1}$ is a fuzzy. What about $R \cap R^{-1}$? What about $R \cup R^{-1}$?

9. * Given any relation R there is a least $T \supseteq R$ such that T is transitive, and a least $S \supseteq R$ such that S is symmetrical, namely the transitive and symmetric closures of R. Must there also be a unique maximal (aka **maximum**) $S \subseteq R$ such that S is transitive? And must there be a unique maximal (maximum) $S \subseteq R$ such that S is symmetrical? The answer to one of these last two questions is 'yes': find a cute formulation.

10. What are the transitive closures of the following relations on $\mathbb{N}$?

    (a) $\{\langle 0, 1\rangle, \langle 1, 2\rangle, \langle 2, 3\rangle, \ldots\}$: i.e., $\{\langle n, n+1\rangle : n \in \mathbb{N}\}$,

    (b) $\{\langle n, 2n\rangle : n \in \mathbb{N}\}$.

11. What is an antichain? Let D_n be the poset whose elements are the divisors of n, with $x \leq y$ if $x|y$. Find a maximum antichain in D_{216}.

12. * Define xRy on natural numbers by

    xRy iff $x \leq y + 1$

    What are the following relations?[2]

    (a) $R \cap R^{-1}$

    (b) $R \setminus R^{-1}$

    (c) The transitive closure of the relation in (a)

    (d) The transitive closure of the relation in (b)

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

    (a) $(\forall xyz)(z < x \not\leq y \not\leq x \rightarrow z < y)$

    (b) $(\forall xyz)(z > x \not\leq y \not\leq x \rightarrow z > y)$.

14. * Show that $R \subseteq S$ implies $R^{-1} \subseteq S^{-1}$

15. * Show that composition of relations is associative: *i.e.* if R, S and T are relations, show $(R \circ S) \circ T = R \circ (S \circ T)$.

16. (a) Consider the following non-deterministic algorithm. A bag contains b black balls and w white balls. Two balls are removed. If they are both white, a white ball is replaced. If they are both black, an arbitrary and unspecified quantity of white balls from an inexhaustible supply is put in the bag. If one is black and one is white, the black ball is replaced. This process is repeated till the bag has only one ball. Show that the colour of the ball is determined by b and w alone and hence the algorithm determines a function of b and w.

    (b) * How can you be sure that the algorithm always terminates whatever you pluck out of the bag at each stage? *hint: think about the lexicographic order of* $\mathbb{N}^2$.

    (c) The purpose of this question was to make a point about lexicographic orders: in this case, about the order on $\mathbb{N} \times \mathbb{N}$. Check that you have really understood what is going on by rewriting the question for the scenario in which the balls come in three colours $\ldots k$ colours.

    (d) (abstruse: not for a first pass) Extend the product order of $\mathbb{N} \times \mathbb{N}$ by stipulating that $\langle x, y\rangle < \langle y, S(x)\rangle$ and taking the reflexive transitive closure. Write the result $\leq_{\mathcal{B}}$. Is $\leq_{\mathcal{B}}$ a total order? Define $\leq$ between finite subsets of $\mathbb{N} \times \mathbb{N}$ by $X \leq Y$ iff $(\forall x \in X)(\exists y \in Y)(x \leq_{\mathcal{B}} y)$. Is $\leq$ wellfounded?

[2]The structure $\langle \mathbb{N}, R\rangle$ is known to students of modal logic as the *Recession Frame*.

17. Functions are just special kinds of relations, okay? What can you say about a function that is also a symmetrical relation? What about a function that is also a transitive relation? (That is, $f(x) = y \wedge f(y) = z \rightarrow f(x) = z$) Embarrass your supervisor by demanding explanations of the words *involution* and *idempotent*.

18. Let $K = \lambda x.(\lambda y.x)$. Evaluate $K8$, $K(K8)$ and $(KK)8$.

19. This question concerns *(binary) games of length n*. For each set $X \subseteq \{0, 1, 2, 3, 4 \ldots 2^n - 1\}$ we have a game G_x of length n; there are two players `I` and `II`; they play by writing down either 0 or 1, *ad libitum*, alternating (with `I` starting), and carry on until n 0s and 1s have been written down (that's why the game is of length n); the result is a a string of n 0s and 1s, which is to say, a binary number $k < 2^n$. The rule is that `I` wins iff $k \in X$. Show that for every $n \in \mathbb{N}$ and for every game of length n, one of the two players must have a winning strategy. How many (binary) games of length n are there? (Easy) Let $\texttt{II}_n$ be the proportion of these games for which player `II` has a winning strategy: what is the limit of $\texttt{II}_n$ as n gets large? (Easy).

20. What is a wellordering? What is an initial segment of an ordering? (If you don't know what a **chain** in a poset is you probably won't know what an initial segment in a total ordering is either.) If $\langle X, \leq \rangle$ is a total order, then a *suborder* of it is a subset $X' \subseteq X$ ordered by the obvious restriction of $\leq$. Prove that $\langle X, \leq \rangle$ is a wellordering if every suborder of it is isomorphic to an initial segment of it. (The converse is also true but involves more work.)

21. Consider the argument: "If Anna can cancan or Kant can't cant, then Greville will cavil vilely. If Greville will cavil vilely, Will won't want. But Will will want. Therefore, Kant can cant." By rewriting the statement in terms of four Boolean variables, show it is tautologous and hence a valid argument. (*There are loads of similar exercises in any number of introductory logic books. Try, for example, Lewis Carroll*, Symbolic Logic.)

22. Bracket '$[(a \rightarrow b) \vee (a \rightarrow d)] \rightarrow (b \vee d) \longleftrightarrow a \vee b \vee d$' and test all versions for validity.

23. "Brothers and sisters have I none, but this man's father is my father's son" *What?!*

24. You know that lists can be thought of as ordered pair of head and tail. By using the pairing function $\langle x, y \rangle = 2^x \cdot (2y + 1)$ show how to encode a list of natural numbers as a single natural.

2.1 Countability and Uncountability

Which of the following sets are countable and which are uncountable?

(i) The set of complex numbers
(ii) The set of partitions of $\mathbb{N}$ into finite pieces
(iii) $\{X \subseteq \mathbb{N} : 0 \in X\}$
(iv) The set of partitions of $\mathbb{N}$ into finitely many pieces
(v) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = 0$ for all but finitely many n
(vi) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = 0$ or 1 for all but finitely many n
(vii) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = n$ for all but finitely many n
(viii) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $(\forall n)(f(n) \leq n)$
(ix) The set of subsets of $\mathbb{N}$ with finite complement ("cofinite")

The set $\mathbf{Q} \to \mathbb{R}$ of functions from the rationals to the reals is obviously uncountable. What is its cardinality?

2.2 Slightly less elementary

1. * Show that $\bigcup_{n \in \mathbb{N}} R^n$ is the smallest transitive relation extending R.
2. $t(R)$ is the transitive closure of R.[3]
   (a) * Give an example of a relation R on a set of size n for which $t(R) \neq R^1 \cup R^2 \cup \ldots \cup R^{n-1}$.
   (b) Give an example of a set and a relation on that set for which $t(R) \neq R^1 \cup R^2 \cup \ldots \cup R^n$ for any finite n.
   (c) If R is reflexive then $t(R)$ is clearly the reflexive transitive closure of R (often called just the transitive closure): if you are not happy about this, attempt to write out a proof.
   (d) Find an example of an *irreflexive*[4] relation R on a set such that $t(R)$ is indeed the reflexive transitive closure of R.
3. Think about $\mathbb{N}$ and S (the successor function on $\mathbb{N}$). What is the transitive closure of S? For integers n and m when do we have $(S^n)^* \subseteq (S^m)^*$? When do we have $(S^n \cup (S^n)^{-1} \cup S^m \cup (S^m)^{-1})^* = (S \cup S^{-1})^*$?
4. * Show that the smallest equivalence relation containing the two equivalence relations R and S is $t(R \cup S)$.

[3] Misleadingly people often use the expression "transitive closure of R" to mean the transitive reflexive closure of R.

[4] You don't know what 'irreflexive' means? There are only two things it can possibly be, so what are they? Answer this question for *both* versions! That'll teach you ask silly questions!

5. If $R \subseteq X \times X$ is a fuzzy on X, is there a largest equivalence relation on X that $\subseteq R$? Is there a smallest equivalence relation on X that $\supseteq R$?

6. (a) Suppose that for each $n \in \mathbb{N}$, R_n is a transitive relation on a (presumably infinite) set X. Suppose further that for all n, $R_n \subseteq R_{n+1}$. Let R_∞ be $\bigcup_{n \in \mathbb{N}} R_n$, the union of all the R_n. Prove that R_∞ is also transitive.

   (b) Give an example to show that the union of two transitive relations is not always transitive.

7. For all the following choices of allegations, prove the strongest of the correct options; explain why the other correct options are not best possible and find counterexample to the incorrect ones. If you find you are doing them with consummate ease, break off and do something else instead.

   (a) An intersection of a fuzzy and an equivalence relation is (i) an equivalence relation (ii) a fuzzy (ii) neither

   (b) A union of a fuzzy and an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (c) An intersection of two fuzzies is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (d) An intersection of the complement of a fuzzy and an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (e) An intersection of a fuzzy and the complement of an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (f) A union of a fuzzy and the complement of an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (g) An intersection of a fuzzy and the complement of a fuzzy is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (h) An intersection of the complement of a fuzzy and the complement of an equivalence relation is (i) an equivalence relation (ii) a fuzzy (iii) neither

   (i) A union of two fuzzies is (i) an equivalence relation (ii) a fuzzy (iii) neither.

8. A PER ('*P*artial *E*quivalence *R*elation') is a binary relation that is symmetrical and transitive. Is the complement of a PER a fuzzy? Is the complement of a fuzzy a PER? In each case, if it is false, find sensible conditions to put on the antecedents that would make it true.

9. Let $<$ be a transitive relation on a set X. Consider the two relations (i) $\{\langle x, y\rangle : (x \in X) \wedge (y \in X) \wedge (x < y) \wedge (y < x)\}$ and (ii) $\{\langle x, y\rangle : (x \in X) \wedge (y \in X) \wedge (x \not< y) \wedge (y \not< x)\}$.

(a) Are either of these fuzzies, or equivalence relations?

(b) If one of these isn't a fuzzy, but "ought to be", what was the correct definition?

(c) If the relation in (i) was an equivalence relation, what sort of relation does $<$ induce on the equivalence classes? Why is the result a mess? What extra condition or conditions should i have put on $<$ to start with to prevent this mess occurring?

(d) If (the correct definition of) relation (ii) is an equivalence relation, what can we say about the quotient?

10. Explain how to find the two greatest numbers from a set of n numbers by making at most $n + \lfloor \log_2 n \rfloor - 2$ comparisons. Can it be done with fewer? How about the 3 biggest numbers? The k biggest numbers, for other values of k? What happens to your answer as k gets bigger and bigger and approaches n?

11. * Show that the largest and smallest elements of a totally ordered set with n elements can be found with $\lceil 3n/2 \rceil - 1$ comparisons if n is odd, and $3n/2 - 2$ comparisons if n is even.

12. Construct *natural* bijections between the following pairs of sets. (For the purposes of this exercise a natural map is (expressed by) a closed λ-term; a natural bijection is (expressed by) a closed λ term (L, say) with an inverse L'. That is to say, both $\texttt{compose}(L, L')$ and $\texttt{compose}(L', L)$ simplify to $\lambda x.x$. Alternatively, a natural function is one you can write an `ML` program for. If you want to think more about what a natural bijection is, look at your earlier answers to the questions: If A is a set with n members, how many symmetrical relations are there on A, and how many antisymmetrical trichotomous relations are there on A? The answers to these two questions are the same, but there doesn't seem to be any 'obvious' or 'natural' bijection between the set of symmetrical relations on A and the set of antisymmetrical trichotomous relations on A.) You will need to assume the existence of primitive pairing and unpairing functions which you might want to write as '`fst`', '`snd`' and $\langle x, y \rangle$

    $A \to (B \to C)$ and $B \to (A \to C)$;
    $A \times B$ and $B \times A$;
    $A \to (B \times C)$ and $(A \to B) \times (A \to C)$;
    $(A \times B) \to C$ and $A \to (B \to C)$;

    You may wish to try the following pairs too, but only once you have done the `ML` machinery for disjoint unions of types:

$(A \to C) \times (B \to C)$ and $(A + B) \to C$;
$A + (B + C)$ and $(A + B) + C$;
$A \times (B + C)$ and $(A \times B) + (A \times C)$.

Let Z be a set with only one element. Find a natural bijection between $(Y + Z)^X$ and the set of partial functions from X to Y.

Find natural functions[5]

(i) from A into $B \to A$;
(ii) from A into $(A \to B) \to B$;
(iii) from $A \to (B \to C)$ into $(A \to B) \to (A \to C)$;
(iv) from $(((A \to B) \to B) \to B)$ into $A \to B$. (This one is hard: you will need your answer to (ii))
(v) from $(A \to B) \to A$ into $(A \to B) \to B$.

(it might help to think of these as invitations to write `ML` code of types `'a -> 'b -> 'a`, `'a -> ('a -> 'b) -> 'a` etc.)

13. What is a fixed point? What is a fixpoint combinator? Let T be your answer to the last bit of the preceding question. (So T is a natural function from $(A \to B) \to A$ into $(A \to B) \to B$.) Show that something is a fixpoint combinator iff it is a fixed point for T.

14. Let $P = \lambda G.(\lambda g.G(gg))(\lambda g.G(gg))$. Show that P is a fixpoint combinator. Why is it not typed? After all, T was typed!

15. Give `ML` code for a higher-order function `metafact` such that any fixed point for `metafact` will turn out to be good old `fact`. Do the same for something tedious like `fibo`. Delight your supervisor by finding, for other recursively defined functions, higher-order functions for which they are fixed points.

16. Think of '$\to$' as implication: is $(((p \to q) \to p) \to p)$ a truth-table tautology? Now think of $\to$ as "set of all functions from ...". Is there a natural map from $((p \to q) \to p)$ to p? (Very Hard!)[6]

17. * Solve

$$x^{x^{x^{x^{x^{\cdots}}}}} = 2$$

[5]These do not have to be either injective or surjective. They only have to be functions.

[6]Hints: Suppose p has five members and q is a subset of p with two members. Use the pigeonhole principle to find a map $((p \to q) \to p)$. Reflect on how **natural** maps must interact with permutations. See Dana Scott's article "Semantic archæology" in Harman and Davidson (eds.) *Semantics of Natural language* Reidel 197?.

and comment on the notation. Then think about

$$x^{x^{x^{x^{x^{\cdots}}}}} = 4.$$

18. Prove that $2^n - 1$ moves are sufficient to solve the Towers of Hanoi problem.

19. The fellows of Porterhouse ring each other up every sunday to catch up on the last week's gossip. Each fellow passes on (in all subsequent calls that morning) all the gossip (s)he has picked up, so there is no need for each fellow to ring every other fellow directly. How many calls are needed for every fellow to have aquired every other fellow's gossip?

20. A *triomino* is an L-shaped pattern made from three square tiles. A $2^k \times 2^k$ chessboard, whose squares are the same size as the tiles, has one of its squares painted puce. Show that the chessboard can be covered with triominoes so that only the puce square is exposed.

21. Is it possible to tile a standard (8×8) chessboard with thirty-one 2×1 rectangles (dominoes) to leave two diagonally opposite corner squares uncovered?

22. * Let $k \in \mathbb{N}$ and let $\mathcal{F}$ be a family of finite sets closed under symmetric difference, such that each set in $\mathcal{F}$ has at most k elements. How big is $\bigcup \mathcal{F}$? How big is $\mathcal{F}$?

23. Fix a set X. If π_1 and π_2 are partitions of it, we say π_1 *refines* π_2 if every piece of π_1 is a subset of a piece of π_2. What properties from the usual catalogue (transitivity, symmetry, etc.) does this relation between partitions of X have?

24. Let X be a set, and R the refinement relation on partitions of X. Let $\Pi(X)$ be the set of partitions. Why is it obvious that in general the structure $\langle \Pi(X), R \rangle$ is not a boolean algebra?

2.2.1 Boolean Algebra

1. Write down the truth tables for the 16 functions $\{T, \bot\}^2 \to \{T, \bot\}$, and give them sensible names (such as $\wedge, \vee, \to$, `NOR`, `NAND`). Which of these functions `splat` that you have identified have the feature that if p `splat` q and p both hold, then so does q? Why are we interested in only one of them?

2. (a) Show that `NAND` and `NOR` cannot be constructed by using $\wedge$ and $\vee$ and $\to$ alone

   (b) Show that none of `NAND`, `NOR`, $\to$, $\wedge$, $\vee$ can be constructed by using `XOR` alone. (hard)

(c) Show that XOR and $\longleftrightarrow$ and $\neg$ cannot be defined from $\vee$ and $\wedge$ alone.

(d) *(for enthusiasts only)* Can $\wedge$ and $\vee$ be defined in terms of $\longleftrightarrow$ and $\rightarrow$?

(e) *(for enthusiasts only)* Show that all connectives can be defined in terms of XOR and $\rightarrow$.

(f) A *monotone* propositional function is one that will output 1 if all its inputs are 1. Show that no nonmonotone function can be defined in terms of any number of monotone functions. (easy)

3. What is a boolean algebra? Find a natural partial order on the set of functions from question 1 that makes them into a boolean algebra.

4. How many truth-functions of three propositional letters are there? Of four? Of n?

5. Prove that $\mathcal{P}([0,2]$ and $\{T,\perp\}^3$ are isomorphic posets.

2.2.2 Generating functions etc.

1. Let u_n be the number of strings in $\{0,1,2\}^n$ with no two consecutive 1's. Show $u_n = 2u_{n-1} + 2u_{n-2}$, and deduce $u_n = \frac{1}{4\sqrt{3}}[(1+\sqrt{3})^{n+2} - (1-\sqrt{3})^{n+2}]$.

2. Let m_n be the number of ways to obtain the product of n numbers by bracketing. (For example, $((ab)c)d$, $(ab)(cd)$, $(a(bc))d$, $a((bc)d)$ and $a(b(cd))$ show $m_4 = 5$.) Prove $m_n = \frac{1}{n}\binom{2n-2}{n-1}$.

3. Prove that $\mathbb{N} \times \mathbb{N}$, with the lexicographical order, is well-ordered, and that $\mathbb{N} \times \mathbb{N}$ with the product order has no infinite antichain.

4. Say $n \in m$ (where $n, m \in \mathbb{N}$) if the nth bit of m is 1. $n \subseteq m$ is defined in terms of this in the obvious way. Prove that $n \subseteq m$ iff $\binom{m}{n}$ is odd. (Hint: use the fact that $\binom{m+1}{n+1} = \binom{m}{n} + \binom{m}{n+1}$.)

5. Let p_n be the number of ways to add $n-3$ non-crossing diagonals to a polygon with n sides, thus splitting it into $n-2$ triangles. So $p_3 = 1$, $p_4 = 2$, $p_5 = 5$, and we define $p_2 = 1$. Show that

$$p_n = p_2 p_{n-1} + p_3 p_{n-2} + \ldots + p_{n-1} p_2 \quad \text{for} \quad n \geq 3\,,$$

6. and hence evaluate p_n.

7. A question on generating functions which will keep you out of mischief for an entire afternoon![7] Let A_n be the number of ways of ordering the

[7] This comes from a book called "100 great puzzles in maths" or some such title: the author's name is Dörrie, it is published by Dover, and there is a copy in the DPMMS library. This is problem 16 on p 64.

numbers 1 to n such that each number is either bigger than (or smaller than) *both* its neighbours. ("zigzag permutations"). Find a recurrence relation for $(A_n/2)$. (*Hint* Think about how many zigzag permutations of $[1, n]$ there are where n appears in the rth place.) Further hints: you will have to divide the nth term by $n!$ and solve a (fairly simple) differential equation.

8. What can you say about

$$q_0 =: 1; q_{n+1} =: 1 - e^{-q_n}?$$

2.2.3 Truth-definitions

An `ML` question which will prepare you for the 1b courses entitled "Logic and Proof" and "Semantics". You should make a serious attempt at—at the very least—the first part of this question. The fourth part is the hardest part and provides a serious work-out to prepare you for the semantics course. Parts 2 and 3 are less central, but are educational. *If you are a 1b student treating this as revision you should be able to do all these questions.*

Propositional Logic	Predicate (first-order) Logic
A recursive datatype of formulæ	A recursive datatype of formulæ
	An interpretation $\mathcal{I}$ is a domain $\mathcal{D}$ with: for each n-place predicate letter F a subset $\mathcal{I}`F$ of $\mathcal{D}^n$; for each $n$-ary function letter $f$ a function $\mathcal{I}`f$ from $\mathcal{D}^n \to \mathcal{D}$. (Also constants).
`states`: `literals` $\to$ `bool`. A (recursively defined) satisfaction relation `SAT`:`states`$\times$`fmla`$\to$`bool`	(Fix $\mathcal{I}$ then) `states`: $vbls \to \mathcal{D}$; a recursively defined satisfaction function: $sat_{\mathcal{I}}$: formulæ $\times$ `states` $\to$ `bool`
A formula ϕ is **valid** iff for all `states` v, `SAT`$(v, \phi) =$`true`.	ϕ is **true** in an interpretation $\mathcal{I}$ iff for all states v, $sat_{\mathcal{I}}(\phi, v) =$`true`. ϕ is **valid** iff it is true in all interpretations.

1. Write `ML` code to implement the left-hand column. If you are completely happy with your answer to this you should skip the next two questions of this section.

2. (*For enthusiasts*). Expand the propositional language by adding a new unary connective, written '$\Box$'. The recursive definition of `SAT` for the language with this extra constructor has the following additional clause:

   > if s is a formula of the extended language and v is a state then `SAT`$(v, \Box s) = 1$ iff for all states v' we have `SAT`$(v', s) = 1$

   Then redo the first question with this added complication.

3. (*For enthusiasts*). Complicate further the construction of the preceding question by altering the recursive step for $\Box$ as follows. Accept as a new input a (binary) relation R between states (presumably presented as a list of pairs, tho' there may be prettier ways of doing it). The new clause is then:

   > if t is a formula of the form $\Box s$ and v is a state then $\texttt{SAT}(v, t) = 1$
   > iff for all states v' such that $v'\ R\ v$ we have $\texttt{SAT}(v', s) = 1$

4. Declare a recursive datatype which is the language of partial order. That is to say you have a set of variables, quantifiers, connectives etc., and two predicate letters '$\leq$ and '='. Fix an interpretation of it, possibly the `ML` type `int`. Implement as much as you can of the apparatus of states, truth etc.

5. Declare a recursive datatype which is the language of fields. That is to say you have a set of variables, quantifiers, connectives etc.; two constants '0' and '1'; a binary predicate letter '=' and two function symbols, '+' and '$\times$'. Fix an interpretation of it, for example the natural numbers below 17. Implement as much as you can of the apparatus of states, truth etc. You should be able to write code that will accept as input a formula in the language of fields and evaluate to `true` or `false` depending on what happens in the naturals mod 17.[8]

In the last two questions you could make life easier for yourself (but less natural) by assuming that the language has only finitely many individual variables. This would enable you, for example (by somehow generating all the possible states, since there are now only finitely many of them) to verify that the naturals as an ordered set are a model for the theory of total order, and that the naturals mod 17 are a model for the theory of fields.

When you have done this ask the system minders or any member of the hvg group about how to run *HOL* on the machines available to you. In *HOL* is a dialect of *ML* in which all the needed datatypes are predefined.

2.2.4 Other logic: for 1b revision, mainly

1. π and e are transcendental. By considering the equation

   $$x^2 - (\pi + e)x + \pi e = 0$$

   prove a trivial but amusing fact. (If you cannot see what to do, read the footnote for a HINT). [9] What have you proved? Is your proof constructive? If not, does this give rise to a constructive proof of something else?

[8] It won't run very fast!

[9] At least one of $\pi + e$ and πe must be transcendental.

2. The uniqueness quantifier $\exists!x$' is read as "There is precisely one x such that ...". Show how to express the uniqueness quantifier in terms of the old quantifiers $\exists$ and $\forall$ (and $=$).

   (a) Find an example to show that $(\exists!x\exists!y)\phi(x,y)$ is not always the same as $(\exists!y\exists!x)\phi(x,y)$

   (b) Is the conjunction of $\exists!x\phi(x)$ and $\exists!y\psi(y)$ equivalent to something of the form $\exists!x\exists!y\ldots$?

3. You are the computer officer in charge of a system that is not secure, in the sense that it is possible to write viruses for it *ad lib*. (A virus is something that corrupts the operating system). Use a diagonal argument to show that any program running under this system that accepts a body of code as input and outputs 0 if the input is a virus and 1 otherwise must itself be a virus.

Propositions as types

Check that you know what is meant by "natural deduction". In this section, Greek letters will range over expressions built up from 'A', 'B', etc. by putting '$\rightarrow$' between such expressions. Thus they can be read indifferently as propositional formulæ or as types. Call these chaps *formulæ*. Attempt these in connection with question 12 from section 2.

1. Prove that if α is a formula such that there is a closed lambda term of type α then there is a natural deduction proof of α. And conversely!

2. If $\mathcal{D}$ is some natural deduction with conclusion α and premisses $\beta_1\ldots\beta_n$ show that any valuation defined on the propositional letters in $\beta_1\ldots\beta_n$ and α that makes all the $\beta_1\ldots\beta_n$ true must also make α true too.

3. The relation $\neg\neg(x=y)$ is (intuitionistically) distinct from the relation $x=y$. Prove that it is a fuzzy. Is it an equivalence relation? Prove it or explain why you think it isn't

4. Find a natural deduction proof of

   $(X\rightarrow(Y\rightarrow(Z\rightarrow W)))\rightarrow((X\rightarrow(Y\rightarrow Z))\rightarrow((X\rightarrow Y)\rightarrow(X\rightarrow W)))$

   and a λ-term to go with it.

Horn clauses

1. What is a horn clause? What is an intersection-closed property of relations?[10] Let $\phi(\vec{x})$ be a horn clause (in which 'R' appears and the $\vec{x}$ range over the

[10] A horn clause is a formula of the kind $\bigwedge_{i\in I}\psi_i\rightarrow\phi$ where ϕ and all the ψ_i are atomic. $F()$ is an intersection-closed property of relations if an intersection of any number of relations that have property F also has property F.

domain of R). Show that the property $\forall\vec{x}(\phi(\vec{x}))$ is intersection closed. (The converse is also true but do not attempt to prove it!)

2. Let I be an index set, and for each $i \in I$, P_i is a person, with an associated set of beliefs, B_i. We assume (unrealistically) that each B_i is deductively closed and consistent. Show that $\bigcap_{i\in I} B_i$ is deductively closed and consistent. What about the set of all propositions p such that p is believed by a majority of people? (You may assume I is finite in this case, otherwise it doesn't make sense). What about the set of things believed by all but finitely many of the P_i? (You may assume I is *in*finite in this case, otherwise it doesn't make sense).[11]

3. We are given a set $\mathcal{L}$ of literals. We are also given a subset $K_0 \subseteq \mathcal{L}$. ('$K$' for '$K$nown'.) Also a set C_0 ('C' for 'Conditionals) of formulaæ of the kind

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$$

If we are given two such sets, of literals and of conditionals, we can get a new set of Known literals by adding to K_0 any q that is the consequent of a conditional all of whose antecedents are in K_0. Of course we can then throw away that conditional.

   (a) Turn this into a precise algorithm that will tell us, given K_0, C_0 and a candidate literal q, whether or not q can be deduced from K_0 and C_0. By coding this algorithm in `ML`, or by otherwise concentrating the mind, determine how efficient it is.

   (b) What difference does it make to the implementation of your algorithm if the conditionals are of the form

$$p_1 \rightarrow (p_2 \rightarrow (p_3 \rightarrow \ldots q)\ldots)?$$

   (c) What happens to your algorithm if Conditionals are allowed to be of the (more complicated) form:

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow (q_1 \vee q_2)?$$

   Can anything be saved?

   (d) Define a quasi-order (remember what a quasi-order is?[12]) on $\mathcal{L}$ by setting $p\ R\ q$ if there is a conditional in C_0 which has q as its consequent and p as one of its antecedents, and letting $<$ be the transitive closure of R. Is $<$ reflexive? Irreflexive? Antisymmetrical? What happens if $p < p$? What happens if $(p < q) \wedge (q < p)$?

[11] What about the set of propositions believed by an even number of people?

[12] And don't lose sleep over the reflexivity condition: we can add lots of silly clauses like $p \rightarrow p$ at no cost!