COMP0009 Logic — Problem Sheet 6: Model Theory

Part A — Truth and consequence

Alice, Bob and Mallory share a network of files that Charlie looks after. Alice keeps her coins in a vault, Bob keeps his notes, Mallory keeps a junk file of her own making, and Mallory would like to read what is not hers. Who may read what is decided by a *rulebook*, a few sentences of logic with names and quantifiers, and recorded in a *table*: who is a user, who is an administrator, who owns what, who may read what. Charlie can query the table, and anyone can send him a tree, a proof built bar by bar from the rulebook, to claim a right.

Two questions sound alike and are not: is this sentence true of *today's* table? And does it *follow* from the rulebook, so that it is true of every table the rulebook allows? In the four scenes below you will evaluate sentences in the table, build tables that obey the rulebook and break a claim, check trees line by line against the table, catching Mallory's forgeries as you go, and meet the law that the trees were missing.

Marks are in square brackets; the whole of Part A is worth 25.

A1. Truth in a structure.

The vocabulary, or *signature*, of the network has six names, alice, bob, $\mathsf{mallory}$, notes, junk, vault, and four relation symbols, $\mathsf{usr}(x)$ ("x is a user"), $\mathsf{adm}(x)$ ("x is an administrator"), $\mathsf{own}(x, y)$ ("x owns y") and $\mathsf{read}(x, y)$ ("x may read y"). A sentence is built from these with $\to$, $\wedge$, $\vee$, $\bot$, $\forall$ and $\exists$, and $\neg\varphi$ is short for $\varphi \to \bot$; $\wedge$ and $\vee$ take precedence over $\to$, and a quantifier covers as little as it can, so brackets are written round a longer scope. The rulebook has two lines, the *access policy*:

(pol1) $\forall x\, \forall y\, (\mathsf{adm}(x) \to \mathsf{read}(x, y))$ administrators may read anything;
(pol3) $\forall x\, \forall y\, (\mathsf{own}(x, y) \to \mathsf{read}(x, y))$ owners may read what they own.

(There was once a (pol2), "anyone who owns something is an administrator"; it comes back in A3.) Nothing here says what the words *mean*. A *structure* does that: it is a non-empty set $\mathbb{D}$ of things, the *domain*, together with an *interpretation* of the symbols: a thing $[\![c]\!]^{\mathfrak{M}}$ for each name c and a set $[\![R]\!]^{\mathfrak{M}}$ of rows for each relation symbol R, one row for each tuple of things of which R holds.

Today's table is the structure $\mathfrak{M}$ with six things, three users and three files:

$$\begin{aligned}
\mathbb{D} &= \{\text{Alice}, \text{Bob}, \text{Mallory}, \text{Notes}, \text{Junk}, \text{Vault}\},\\
[\![\mathsf{alice}]\!]^{\mathfrak{M}} &= \text{Alice}, \quad [\![\mathsf{bob}]\!]^{\mathfrak{M}} = \text{Bob}, \quad \text{and so on: each name names its thing},\\
[\![\mathsf{usr}]\!]^{\mathfrak{M}} &= \{\text{Alice}, \text{Bob}, \text{Mallory}\}, \qquad [\![\mathsf{adm}]\!]^{\mathfrak{M}} = \{\text{Alice}\},\\
[\![\mathsf{own}]\!]^{\mathfrak{M}} &= \{(\text{Alice}, \text{Vault}),\ (\text{Bob}, \text{Notes}),\ (\text{Mallory}, \text{Junk})\},\\
[\![\mathsf{read}]\!]^{\mathfrak{M}} &= \{(\text{Alice}, d) : d \in \mathbb{D}\} \cup \{(\text{Bob}, \text{Notes}),\ (\text{Mallory}, \text{Junk})\}.
\end{aligned}$$

Charlie filled the last table by running the policy: (pol1) says administrators may read *anything*, and the table takes it at its word, so Alice has six rows, the users' entries included; (pol3) gives each owner one row, so the table has eight rows in all.

One clause for each symbol decides whether a sentence is *true in* $\mathfrak{M}$. On the way the clauses meet formulas with free variables, such as $\mathsf{read}(x, y)$, so they carry an *assignment* s, a record of what each variable stands for; $s[d/x]$ is s with d for x.

Read $\mathfrak{M}, s \vDash \varphi$ as "φ is true in $\mathfrak{M}$ under s":

$\mathfrak{M}, s \vDash R(t_1, \dots, t_n)$	iff	the things named by $t_1, \dots, t_n$ form a row of $[\![R]\!]^{\mathfrak{M}}$
$\mathfrak{M}, s \nvDash \bot$		
$\mathfrak{M}, s \vDash \psi \wedge \chi$	iff	$\mathfrak{M}, s \vDash \psi$ and $\mathfrak{M}, s \vDash \chi$
$\mathfrak{M}, s \vDash \psi \vee \chi$	iff	$\mathfrak{M}, s \vDash \psi$ or $\mathfrak{M}, s \vDash \chi$
$\mathfrak{M}, s \vDash \psi \to \chi$	iff	$\mathfrak{M}, s \nvDash \psi$ or $\mathfrak{M}, s \vDash \chi$
$\mathfrak{M}, s \vDash \forall x\, \psi$	iff	$\mathfrak{M}, s[d/x] \vDash \psi$ for every $d \in \mathbb{D}$
$\mathfrak{M}, s \vDash \exists x\, \psi$	iff	$\mathfrak{M}, s[d/x] \vDash \psi$ for some $d \in \mathbb{D}$

The atomic clause looks up a table. The two quantifier clauses are loops over the domain: to decide $\forall x\, \psi$, try each of the six things as x and check ψ every time; to decide $\exists x\, \psi$, look for one that works. For a sentence the assignment s makes no difference, and we write $\mathfrak{M} \vDash \varphi$. Take care with the clause for $\to$: $\psi \to \chi$ fails only when ψ is true and χ false, so an implication whose antecedent is false is true at once.

Example. Is (pol3), $\forall x\, \forall y\, (\mathsf{own}(x, y) \to \mathsf{read}(x, y))$, true in $\mathfrak{M}$?

The clause for $\forall$, twice, asks for $\mathsf{own}(x, y) \to \mathsf{read}(x, y)$ to be true under $s[d/x][e/y]$ for each of the $6 \times 6 = 36$ pairs (d, e). The clause for $\to$ settles 33 of them at once: (d, e) is not a row of $[\![\mathsf{own}]\!]^{\mathfrak{M}}$, so the antecedent is false. Three pairs remain, (Alice, Vault), (Bob, Notes) and (Mallory, Junk), and the atomic clause finds each of them in $[\![\mathsf{read}]\!]^{\mathfrak{M}}$. So $\mathfrak{M} \vDash$ (pol3).

Charlie's query engine does the same: "select the rows of own that are not rows of read", and nothing comes back.

(a) Decide each by the clauses, in one line each: "true, because ..." or "false, because ...". [1]

(i) $\mathfrak{M} \vDash \mathsf{read}(\mathsf{mallory}, \mathsf{vault})$?

(ii) $\mathfrak{M} \vDash \mathsf{own}(\mathsf{alice}, \mathsf{vault}) \wedge \mathsf{adm}(\mathsf{alice})$?

(iii) $\mathfrak{M} \vDash \mathsf{adm}(\mathsf{bob}) \to \mathsf{read}(\mathsf{bob}, \mathsf{vault})$?

(iv) $\mathfrak{M} \vDash \neg\mathsf{adm}(\mathsf{mallory})$?

(b) Two more, with a loop each. [2]

(i) (pol1) is $\forall x\, \forall y\, (\mathsf{adm}(x) \to \mathsf{read}(x, y))$. Fill in the gaps: the outer loop runs over _____ things; for _____ of them the antecedent $\mathsf{adm}(x)$ is false, so the inner loop need not run; for _____ it runs over _____ things, and the row (_____, d) is in $[\![\mathsf{read}]\!]^{\mathfrak{M}}$ every time. So (pol1) is _____ in $\mathfrak{M}$.

(ii) Is there a user who is not an administrator and may read the vault, $\exists x\, (\mathsf{usr}(x) \wedge \neg\mathsf{adm}(x) \wedge \mathsf{read}(x, \mathsf{vault}))$? Run the loop: for each of the six things, say which conjunct fails, or that none does.

(c) The two sentences below use the same words in a different order. Evaluate each in $\mathfrak{M}$ by the clauses, loop by loop, and say each in plain English. [2]

(i) $\forall x\, (\mathsf{usr}(x) \to \exists y\, \mathsf{read}(x, y))$ (ii) $\exists y\, \forall x\, (\mathsf{usr}(x) \to \mathsf{read}(x, y))$

Hint: for (i), the outer loop needs a witness y for each user; for (ii), each of the six candidates for y is refuted by one user.

(d) Write a sentence that says "nobody but administrators and owners may read anything": whoever may read something is an administrator or owns it. Call it

(pol4). Is it true in $\mathfrak{M}$? Say which of the 36 pairs the loop must look at closely. [1]

A2. Consequence.

An auditor reads A1 and asks Charlie the better question: "Can that ever stop being true?" The table changes every day, as users join, files are made and rights are granted. The auditor wants to know not whether a sentence is true of today's table but whether the *rulebook* guarantees it, in every table the rulebook allows.

A structure in which every sentence of a set Γ is true is a *model* of Γ, or *satisfies* Γ. The set Γ *entails* a sentence φ, and φ *follows from* Γ, written $\Gamma \models \varphi$, if φ is true in every model of Γ. The symbol now does three jobs, and what stands on its left says which:

$\mathfrak{M}, s \models \varphi$	φ is true in $\mathfrak{M}$ under s	one structure and assignment, given
$\mathfrak{M} \models \varphi$	φ is true in $\mathfrak{M}$	one structure, given
$\Gamma \models \varphi$	φ is true in every model of Γ	all models of Γ

Written as a *theory*, a set of sentences, the rulebook is $\Theta = \{(\text{pol1}), (\text{pol3})\}$, and today's table satisfies it, as A1 checked. To show $\Theta \models \varphi$ takes an argument about *every* model of Θ, as in (a). To show that φ does *not* follow takes one model of Θ in which φ is false, a *counter-model*. Here is a recipe for finding one.

1. Write down what the structure must do: make every sentence of Γ true and φ false.
2. Build it as lazily as possible: as few things as you can, starting with one; every relation as small as the demands allow, empty if nothing forces a row into it; names sharing a thing where nothing forbids it.
3. Check the result against the clauses. When a choice breaks a demand, the demand says what to change.

Example. Today there is an administrator: $\mathfrak{M} \models \exists x\, \mathsf{adm}(x)$. Does the rulebook guarantee one, $\Theta \models \exists x\, \mathsf{adm}(x)$?

Demands: (pol1) and (pol3) true, $\exists x\, \mathsf{adm}(x)$ false. Laziness: one thing, a, named by all six names, and every table empty. Check: (pol1) runs over the one pair (a, a), where $\mathsf{adm}(x)$ is false, so it is true; (pol3) likewise; and $\exists x\, \mathsf{adm}(x)$ is false, since nobody is an administrator. The rulebook allows a table with no administrator at all, so the answer is no: true today, not guaranteed.

(a) Alice is an administrator today, and the auditor grants that fact. Does it follow that she may read the vault, (pol1), $\mathsf{adm}(\mathsf{alice}) \models \mathsf{read}(\mathsf{alice}, \mathsf{vault})$? Fill in the gaps of Charlie's argument. [1]

Let $\mathfrak{M}$ be any structure in which (pol1) and $\mathsf{adm}(\mathsf{alice})$ are true, and write a for $[\![\mathsf{alice}]\!]^{\mathfrak{M}}$ and v for $[\![\mathsf{vault}]\!]^{\mathfrak{M}}$. By the clause for _____, twice, with a for x and v for y, the formula _____ is true under $s[a/x][v/y]$. Its antecedent is true, because _____, so by the clause for _____ its consequent is. That is $\mathsf{read}(\mathsf{alice}, \mathsf{vault})$, and $\mathfrak{M}$ was any structure that satisfies the two hypotheses.

(b) Alice may read the notes today. The auditor grants only that she owns the vault. Does (pol1), (pol3), $\mathsf{own}(\mathsf{alice}, \mathsf{vault}) \models \mathsf{read}(\mathsf{alice}, \mathsf{notes})$? Follow the recipe. Start with one thing and show that it fails; say which demand fails and

what it tells you to change; then give the counter-model and check it against the three sentences and the conclusion. [2]

Hint: with one thing, alice, vault *and* notes *all name it.*

(c) Mallory may not read the vault today: $\mathfrak{M} \models \neg\mathsf{read}(\mathsf{mallory}, \mathsf{vault})$. Can that stop being true while the rulebook is obeyed, that is, does $\Theta \models \neg\mathsf{read}(\mathsf{mallory}, \mathsf{vault})$ fail? Give a counter-model that is as close to today's table as you can. What have you learnt about the rulebook? [1]

(d) Charlie adds (pol4) of A1(d) to the rulebook. Show that (pol1), (pol3), (pol4) still do not entail $\neg\mathsf{read}(\mathsf{mallory}, \mathsf{vault})$: build the laziest counter-model. Then say which two facts about Mallory the auditor must be granted, and argue that with those two facts added the sentence does follow. [2]

A3. Soundness.

A claim on the network comes with a certificate: a tree, or derivation, of NJ, built bar by bar from the rules for $\to$, $\wedge$, $\vee$, $\bot$, $\forall$ and $\exists$, with the hypotheses at its leaves and the claim at its root. A tree with open hypotheses in Γ and φ at the bottom shows $\Gamma \vdash_{\mathrm{NJ}} \varphi$, and what ties trees to tables is the *soundness* of NJ: if $\Gamma \vdash_{\mathrm{NJ}} \varphi$ then $\Gamma \models \varphi$. In words: whatever a tree derives from some hypotheses is true in every structure, under every assignment, that makes the hypotheses true.

Watch soundness at work on one tree. List its formulas in an order in which each comes after those it is inferred from; beside each, record its rule, its open hypotheses (by line number) and its truth value in $\mathfrak{M}$ under some assignment s. Soundness does not promise that every line is true. It promises that *a line can be false only if one of its open hypotheses is false.* That makes the table a checking tool: in a forged tree, the bad bar sits at the first line that is false while all its open hypotheses are true.

Example. This tree shows (pol3) $\vdash_{\mathrm{NJ}} \forall x\,(\mathsf{own}(x, \mathsf{vault}) \to \mathsf{read}(x, \mathsf{vault}))$: whoever owns the vault may read it.

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x\,\forall y\,(\mathsf{own}(x,y) \to \mathsf{read}(x,y))}{\forall y\,(\mathsf{own}(x,y) \to \mathsf{read}(x,y))}\,\forall\mathrm{E}}{\mathsf{own}(x,\mathsf{vault}) \to \mathsf{read}(x,\mathsf{vault})}\,\forall\mathrm{E} \qquad [\mathsf{own}(x,\mathsf{vault})]^1}{\mathsf{read}(x,\mathsf{vault})}\,\to\mathrm{E}}{\mathsf{own}(x,\mathsf{vault}) \to \mathsf{read}(x,\mathsf{vault})}\,\to\mathrm{I},1}{\forall x\,(\mathsf{own}(x,\mathsf{vault}) \to \mathsf{read}(x,\mathsf{vault}))}\,\forall\mathrm{I}$$

Its lines, evaluated in $\mathfrak{M}$ with x sent to Bob:

	Formula	**Rule**	**Open**	**Bob**
1	(pol3)	hyp	1	T
2	$\forall y\,(\mathsf{own}(x,y) \to \mathsf{read}(x,y))$	$\forall$E 1	1	T
3	$\mathsf{own}(x,\mathsf{vault}) \to \mathsf{read}(x,\mathsf{vault})$	$\forall$E 2	1	T
4	$\mathsf{own}(x,\mathsf{vault})$	hyp	4	**F**
5	$\mathsf{read}(x,\mathsf{vault})$	$\to$E 3, 4	1, 4	**F**
6	$\mathsf{own}(x,\mathsf{vault}) \to \mathsf{read}(x,\mathsf{vault})$	$\to$I 5	1	T
7	$\forall x\,(\mathsf{own}(x,\mathsf{vault}) \to \mathsf{read}(x,\mathsf{vault}))$	$\forall$I 6	1	T

Lines 4 and 5 are false, and each has the false line 4 among its open hypotheses. Line 6 discharges that hypothesis, and from there on every open hypothesis is true, and so is every line.

(a) The rulebook once had a line (pol2), $\forall x\,\forall y\,(\mathsf{own}(x,\,y) \to \mathsf{adm}(x))$, "anyone who owns something is an administrator". Here is a tree Mallory sent under that old policy, with its table: she owns her junk file, so she is an administrator. Fill in the truth column, in today's $\mathfrak{M}$. Four lines are false. Say why soundness is not contradicted, and why Charlie struck (pol2) out of the rulebook. [1]

$$\dfrac{\dfrac{\dfrac{\forall x\,\forall y\,(\mathsf{own}(x,\,y) \to \mathsf{adm}(x))}{\forall y\,(\mathsf{own}(\mathsf{mallory},\,y) \to \mathsf{adm}(\mathsf{mallory}))}\,\forall\mathrm{E}}{\mathsf{own}(\mathsf{mallory},\,\mathsf{junk}) \to \mathsf{adm}(\mathsf{mallory})}\,\forall\mathrm{E} \qquad \mathsf{own}(\mathsf{mallory},\,\mathsf{junk})}{\mathsf{adm}(\mathsf{mallory})}\,\to\mathrm{E}$$

	Formula	**Rule**	**Open**	$\mathfrak{M}$
1	(pol2): $\forall x\,\forall y\,(\mathsf{own}(x,\,y) \to \mathsf{adm}(x))$	hyp	1	___
2	$\forall y\,(\mathsf{own}(\mathsf{mallory},\,y) \to \mathsf{adm}(\mathsf{mallory}))$	$\forall$E 1	1	___
3	$\mathsf{own}(\mathsf{mallory},\,\mathsf{junk}) \to \mathsf{adm}(\mathsf{mallory})$	$\forall$E 2	1	___
4	$\mathsf{own}(\mathsf{mallory},\,\mathsf{junk})$	hyp	4	___
5	$\mathsf{adm}(\mathsf{mallory})$	$\to$E 3, 4	1, 4	___

(b) Under the new policy Mallory sends Charlie a tree. It shows, she says, that owning junk lets her read Bob's notes, and she attaches a claim: "every open hypothesis is true in today's table, so by soundness the conclusion is".

$$\dfrac{\dfrac{\dfrac{\forall x\,\forall y\,(\mathsf{own}(x,\,y) \to \mathsf{read}(x,\,y))}{\forall y\,(\mathsf{own}(\mathsf{mallory},\,y) \to \mathsf{read}(\mathsf{mallory},\,y))}\,\forall\mathrm{E}}{\mathsf{own}(\mathsf{mallory},\,\mathsf{junk}) \to \mathsf{read}(\mathsf{mallory},\,\mathsf{notes})}\,\forall\mathrm{E} \qquad \mathsf{own}(\mathsf{mallory},\,\mathsf{junk})}{\mathsf{read}(\mathsf{mallory},\,\mathsf{notes})}\,\to\mathrm{E}$$

Her premiss is right, and her conclusion is false in $\mathfrak{M}$. Make the table of its five lines, as in the example, and find the bad bar without looking at the rules: the first line that is false while all its open hypotheses are true. Then say what a correct bar there would have concluded. [2]

(c) A second forgery claims that owning *anything* lets Mallory read *everything*, from (pol3) alone:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall x\,\forall y\,(\mathsf{own}(x,\,y) \to \mathsf{read}(x,\,y))}{\forall y\,(\mathsf{own}(\mathsf{mallory},\,y) \to \mathsf{read}(\mathsf{mallory},\,y))}\,\forall\mathrm{E}}{\mathsf{own}(\mathsf{mallory},\,y) \to \mathsf{read}(\mathsf{mallory},\,y)}\,\forall\mathrm{E} \qquad [\mathsf{own}(\mathsf{mallory},\,y)]^1}{\mathsf{read}(\mathsf{mallory},\,y)}\,\to\mathrm{E}}{\forall y\,\mathsf{read}(\mathsf{mallory},\,y)}\,\forall\mathrm{I}}{\mathsf{own}(\mathsf{mallory},\,y) \to \forall y\,\mathsf{read}(\mathsf{mallory},\,y)}\,\to\mathrm{I},\,1}{\forall x\,(\mathsf{own}(\mathsf{mallory},\,x) \to \forall y\,\mathsf{read}(\mathsf{mallory},\,y))}\,\forall\mathrm{I}$$

(i) Its eight lines are listed below. Fill in the two truth columns, with y sent to Junk and with y sent to Vault. Under Junk, which line is the first that is false with all its open hypotheses true, and which side condition does its bar break? [1]

(ii) Under Vault the first such line is a different one, and its bar is legal. Explain, and say which value of y a checker should try. [1]

	Formula	Rule	Open	Junk	Vault
1	(pol3)	hyp	1	___	___
2	$\forall y\,(\mathsf{own}(\mathsf{mallory}, y) \to \mathsf{read}(\mathsf{mallory}, y))$	$\forall$E 1	1	___	___
3	$\mathsf{own}(\mathsf{mallory}, y) \to \mathsf{read}(\mathsf{mallory}, y)$	$\forall$E 2	1	___	___
4	$\mathsf{own}(\mathsf{mallory}, y)$	hyp	4	___	___
5	$\mathsf{read}(\mathsf{mallory}, y)$	$\to$E 3, 4	1, 4	___	___
6	$\forall y\,\mathsf{read}(\mathsf{mallory}, y)$	$\forall$I 5	1, 4	___	___
7	$\mathsf{own}(\mathsf{mallory}, y) \to \forall y\,\mathsf{read}(\mathsf{mallory}, y)$	$\to$I 6	1	___	___
8	$\forall x\,(\mathsf{own}(\mathsf{mallory}, x) \to \forall y\,\mathsf{read}(\mathsf{mallory}, y))$	$\forall$I 7	1	___	___

(d) Mallory announces a tree for $\bot$ whose open hypotheses are (pol1) and (pol3), and offers to sell it. Charlie declines without reading it. Why is he right? Would he also be right if she claimed a tree for $\bot$ with no open hypotheses at all? [1]

A4. Excluded middle.

Write $P(x)$ for $\mathsf{read}(x, \mathsf{vault})$ throughout this scene. The auditor is told "it is not the case that nobody may read the vault", $\neg\forall x\,\neg P(x)$, and asks "so who may?", $\exists x\,P(x)$. No tree of NJ takes that step, and the reason is a fact about NJ, its *existence property*, that the notes state, with a sketch of why. Every tree can be rewritten into one with no *detours*, where no formula is introduced by one bar and taken apart by the next. A tree of NJ with no detours and no open hypotheses for "there is an x such that φ" ends with ($\exists$I), so it names a term t with $\varphi[t/x]$ above it. A proof of "there is" names the thing, and "it is not the case that nobody" names nobody.

Yet $\neg\forall x\,\neg P(x) \to \exists x\,P(x)$ is true in *every* structure, as (a) asks you to check from the clauses. So the rules of NJ miss a sentence that follows from nothing at all. The whole of the gap is one law, two thousand years old, the *law of the excluded middle* (LEM): of a claim and its denial, one holds. The system NK is NJ with it added as a bar with nothing above it:

$$\frac{}{\varphi \vee \neg\varphi}\ \text{LEM}$$

For any formula φ. The bar has no premisses and discharges nothing; the leaf it makes is an open hypothesis of nobody.

A tree built with it shows $\Gamma \vdash_{\mathrm{NK}} \varphi$. Its soundness is one line: in every structure one of φ and $\neg\varphi$ is true, by the clause for $\neg$, so $\varphi \vee \neg\varphi$ is.

Example. For every formula φ, $\vdash_{\mathrm{NK}} \neg\neg\varphi \to \varphi$. Split on φ: if φ, there is nothing to do; if $\neg\varphi$, it meets $\neg\neg\varphi$ in $\bot$, and $\bot$ gives anything.

$$\dfrac{\dfrac{}{\varphi \vee \neg\varphi}\ \text{LEM} \qquad [\varphi]^2 \qquad \dfrac{\dfrac{[\neg\neg\varphi]^1 \qquad [\neg\varphi]^2}{\bot}\ \to\text{E}}{\varphi}\ \bot\text{E}}{\varphi}\ \vee\text{E}, 2}{\neg\neg\varphi \to \varphi}\ \to\text{I}, 1$$

From now on one bar, labelled (DN), stands for this tree followed by ($\to$E): from $\neg\neg\varphi$, conclude φ.

From here on you draw the trees yourself. The method: first try NJ, working up from the goal with introductions and down from the hypotheses with eliminations. If that sticks, look at where it sticks. If you have reached $\neg\neg\varphi$ and want φ, one

(DN) finishes. If the argument you would give aloud says "either ... or not", find the formula it splits on, write its instance of (LEM), and prove the goal in each case separately; then ($\vee$E).

(a) Let $\mathfrak{M}$ be any structure. Either some thing d of its domain has $P(d)$ true, or none does. Finish each case in one sentence, by the clauses, to show that $\neg\forall x\,\neg P(x) \to \exists x\,P(x)$ is true in $\mathfrak{M}$. [1]

(b) Draw a tree of NK, with no open hypotheses, for $\neg\forall x\,\neg P(x) \to \exists x\,P(x)$. [2]
Hint: suppose $[\neg\forall x\,\neg P(x)]^1$ *and split on* $\exists x\,P(x)$*. One case is immediate. In the other, build* $\forall x\,\neg P(x)$ *from* $[\neg\exists x\,P(x)]^2$*: suppose* $[P(u)]^3$*, reach* $\bot$*, discharge, generalise; then* $\bot$ *with the hypothesis, and* ($\bot$E)*.*

(c) "There is someone such that, if they may read the vault, everyone may": $\exists x\,(P(x) \to \forall y\,P(y))$, the *drinker principle*. Write δ for it. It sounds like a claim about a remarkable person, and it is true in every structure: either someone may not read the vault, and they are the one, or everyone may, and anyone is. Here is the NK tree, in three pieces with four gaps. Fill the gaps, and check the side condition at the ($\exists$E) bar of $\mathcal{F}_1$ and at the ($\forall$I) bar of $\mathcal{F}_2$. [2]

The piece $\mathcal{F}_1$, for the case in which someone may not:

$$\dfrac{[\exists y\,\neg P(y)]^1 \qquad \dfrac{\dfrac{\dfrac{[\neg P(z)]^2 \qquad [P(z)]^3}{\bot}\,{\to}\mathrm{E}}{\boxed{}}\,\bot\mathrm{E}}{P(z) \to \forall y\,P(y)}\,{\to}\mathrm{I},3 \qquad \boxed{}}{\delta}\,\exists\mathrm{E},2$$

The piece $\mathcal{F}_2$, for the case in which nobody may not, so everyone may:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg\exists y\,\neg P(y)]^1 \qquad \dfrac{[\neg P(y)]^4}{\exists y\,\neg P(y)}\,\exists\mathrm{I}}{\bot}\,{\to}\mathrm{E}}{\neg\neg P(y)}\,{\to}\mathrm{I},4}{\boxed{}}\,\mathrm{DN} \qquad \boxed{}}{\forall y\,P(y)}}{P(x) \to \forall y\,P(y)}\,{\to}\mathrm{I}}{\delta}\,\exists\mathrm{I}$$

The join:

$$\dfrac{\dfrac{}{\exists y\,\neg P(y) \vee \neg\exists y\,\neg P(y)}\,\mathrm{LEM} \qquad \begin{matrix}[\exists y\,\neg P(y)]^1\\ \mathcal{F}_1\\ \delta\end{matrix} \qquad \begin{matrix}[\neg\exists y\,\neg P(y)]^1\\ \mathcal{F}_2\\ \delta\end{matrix}}{\delta}\,\vee\mathrm{E},1$$

(d) Two short questions to end the sheet. [2]

(i) In a tree of NJ an ($\exists$I) bar names a term: a proof of "there is" says who. In the tree of (c), who is the witness? Say what the tree tells the auditor about who may read the vault, and what it does not.

(ii) Take on trust the *completeness* of NK: if $\Gamma \vDash \varphi$ then $\Gamma \vdash_{\mathrm{NK}} \varphi$. With soundness, "no tree" and "some counter-model" are the same fact. Charlie

has spent a week looking for a tree of NK for $\exists x\, P(x)$ from the rulebook Θ of A2. What should he have done instead, and what is the answer?

Charlie's table is real. A relational database is a finite structure, one table per relation symbol, by design: Codd built his relational model of data (1970), on which SQL rests, so that a query is a formula of first-order logic. A `WHERE` clause with `AND` and `OR` is the clauses for $\wedge$ and $\vee$; `EXISTS (SELECT ...)` is the clause for $\exists$, a loop over the rows; and "for every" is written as the absence of a counterexample, `NOT EXISTS` with the condition negated, which is $\forall$ as $\neg\exists\neg$. The query engine evaluates a sentence in today's table, exactly as A1 did, and in no other table. Other tools answer the auditor's question, "in every table the rulebook allows?". Alloy (Daniel Jackson, MIT) takes a set of sentences and looks for a structure that obeys them and breaks a claim, trying every structure up to a size you choose: the counter-model search of A2, run by machine. Amazon's Zelkova (Backes and others, FMCAD 2018) does the same for the access policies of Amazon Web Services, and when it reports that no structure breaks a claim, that report is, by completeness, as good as a tree.

Part B — Practice

Practice, for when you want more of the same; nothing here is marked. The drills go from reading a structure, through counter-models and truth along a tree, to trees of NK and questions with no scaffolding. The last two, B13 and B14, go beyond this week: try them only if you are curious. In the drills, P, Q and R are relation symbols, c is a name, f is a one-place function symbol, and x, y, z, u, v, w are variables. What you need:

Structures. A structure $\mathfrak{M}$ is a non-empty domain $\mathbb{D}$, a thing $[\![c]\!]^{\mathfrak{M}} \in \mathbb{D}$ for each name, a function $[\![f]\!]^{\mathfrak{M}} : \mathbb{D} \to \mathbb{D}$ for each one-place function symbol, and a set $[\![R]\!]^{\mathfrak{M}}$ of rows for each relation symbol. The term $f(f(c))$ names $[\![f]\!]^{\mathfrak{M}}([\![f]\!]^{\mathfrak{M}}([\![c]\!]^{\mathfrak{M}}))$. Where $=$ is used, it is a relation symbol interpreted as identity, as in a *normal* structure.

Truth. $\mathfrak{M}, s \vDash \varphi$ by the clauses of A1: the atomic clause looks up a row, $\bot$ is never true, $\wedge$, $\vee$, $\to$ as in truth tables ($\psi \to \chi$ fails only when ψ is true and χ false), $\forall x\, \psi$ loops over the domain and needs ψ every time, $\exists x\, \psi$ needs ψ once. $\neg\varphi$ is $\varphi \to \bot$, so $\neg\varphi$ is true exactly when φ is false.

Entails. $\Gamma \vDash \varphi$ (Γ entails φ; φ follows from Γ): φ is true in every model of Γ (every structure that makes all of Γ true). φ is *valid* if it is true in every structure, *satisfiable* if in some. A counter-model to $\Gamma \vDash \varphi$ is a model of Γ in which φ is false; find one by the recipe of A2: as few things, as few rows, as possible, then check.

Trees. The bars of NJ are the introduction and elimination rules for $\to$, $\wedge$, $\vee$, $\forall$, $\exists$ and ($\bot$E). Soundness: a line of a tree can be false in a structure under an assignment only if one of its open hypotheses is. NK adds

$$\frac{}{\varphi \vee \neg\varphi}\ \text{LEM} \qquad \text{and the derived bar} \qquad \frac{\neg\neg\varphi}{\varphi}\ \text{DN}.$$

Soundness and completeness of NK: $\Gamma \vDash \varphi$ if and only if $\Gamma \vdash_{\text{NK}} \varphi$.

B1. Reading a structure. Let $\mathfrak{M}_1$ have domain $\{1,2,3\}$, $[\![c]\!]^{\mathfrak{M}} = 1$, $[\![P]\!]^{\mathfrak{M}} = \{1,2\}$, $[\![Q]\!]^{\mathfrak{M}} = \{2,3\}$ and $[\![R]\!]^{\mathfrak{M}} = \{(1,2),(2,3),(3,3)\}$. For each sentence say whether it is true in $\mathfrak{M}_1$, giving the witness or the counterexample.

(i) $P(c)$
(ii) $\forall x\, P(x)$
(iii) $\exists x\, R(x,x)$
(iv) $\forall x \exists y\, R(x,y)$
(v) $\exists y \forall x\, R(x,y)$
(vi) $\forall x\, (\neg P(x) \to R(x,x))$
(vii) $\exists x\, (P(x) \wedge R(x,c))$
(viii) $\forall x\, (Q(x) \to \exists y\, R(y,x))$

B2. Loop by loop. Write out the evaluation in $\mathfrak{M}_1$ of each sentence as A1 did, one line per value of the outer variable, with the witness or the reason each inner question is settled.

(i) $\forall x\,(P(x) \to \exists y\,R(x,y))$ (ii) $\exists x\,\forall y\,(R(x,y) \to P(y))$

B3. Terms. Let $\mathfrak{M}_2$ have domain $\{0,1,2\}$, $[\![c]\!]^{\mathfrak{M}} = 0$, $[\![f]\!]^{\mathfrak{M}}$ the function $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 0$, and $[\![R]\!]^{\mathfrak{M}} = \{(0,1),(1,2),(0,2)\}$, that is, $R(x,y)$ means $x < y$.

(i) What do the terms $f(f(c))$ and, with x sent to 2, $f(f(f(x)))$ name?
(ii) Decide each, and say it in English:

$$\forall x\,R(x,f(x)), \qquad \exists x\,R(f(x),x), \qquad \forall x\,\exists y\,R(x,y),$$
$$\exists x\,\forall y\,\neg R(y,x), \qquad \forall x\,(f(f(f(x))) = x).$$

B4. Counter-models by the recipe. For each, show that the entailment fails: start with one thing, and where that is a dead end say which demand fails and move to two. Check your structure against every sentence.

(i) $\forall x\,(P(x) \to Q(x)),\ Q(c) \vDash P(c)$
(ii) $\forall x\,\exists y\,R(x,y) \vDash \exists y\,\forall x\,R(x,y)$
(iii) $\exists x\,(P(x) \to Q(x)),\ P(c) \vDash Q(c)$

B5. Entailments by argument. (i) is started for you; write (ii) in the same shape.

(i) $\forall x\,(P(x) \to Q(x)),\ \exists x\,P(x) \vDash \exists x\,Q(x)$. *Let $\mathfrak{M}$ be any structure that satisfies the two hypotheses. By the clause for $\exists$, some d has* _____ *true. By the clause for $\forall$ at d,* _____ *is true, so by the clause for $\to$,* _____. *Hence* _____ *by the clause for $\exists$.*
(ii) $\forall x\,\neg P(x) \vDash \neg\exists x\,P(x)$.

B6. Valid, satisfiable or neither. For each sentence, say whether it is valid (true in every structure), satisfiable but not valid (true in some, false in some), or unsatisfiable, and give the structures or the argument that show it.

(i) $\exists x\,(P(x) \to P(c))$
(ii) $P(c) \to \forall x\,P(x)$
(iii) $(\exists x\,P(x)) \wedge \forall x\,\neg P(x)$
(iv) $(\forall x\,\exists y\,R(x,y)) \to \exists x\,R(x,x)$
(v) $(\exists x\,\forall y\,R(x,y)) \to \forall y\,\exists x\,R(x,y)$

B7. Truth along a tree. Here is a tree with open hypotheses $\forall x\,(P(x) \to Q(x))$ and $P(c)$:

$$\dfrac{\dfrac{\dfrac{\forall x\,(P(x) \to Q(x))}{P(c) \to Q(c)}\ \forall\mathrm{E} \qquad P(c)}{Q(c)}\ \to\mathrm{E}}{\exists x\,Q(x)}\ \exists\mathrm{I}$$

List its five lines with rule, open hypotheses and truth value in $\mathfrak{M}_1$ of B1. Which lines are false? Does any of them have all its open hypotheses true? What does the table say about the tree?

B8. Finding the bad bar by the table. Each tree has one wrong bar. Let $\mathfrak{M}_3$ have domain $\{a, b\}$, $[\![c]\!]^{\mathfrak{M}} = a$, $[\![P]\!]^{\mathfrak{M}} = \emptyset$, $[\![Q]\!]^{\mathfrak{M}} = \{a\}$ and $[\![R]\!]^{\mathfrak{M}} = \{(a, b), (b, a)\}$. List the lines of each tree with their truth values in $\mathfrak{M}_3$, find the first false line whose open hypotheses are all true, and say what is wrong with its bar.

(i) $$\dfrac{\forall x\, \exists y\, R(x, y)}{\exists y\, R(y, y)}\ \forall\mathrm{E}$$

(ii) $$\dfrac{\dfrac{P(c) \vee Q(c)}{P(c)}\ \wedge\mathrm{E}}{\exists x\, P(x)}\ \exists\mathrm{I}$$

B9. Trees of NK. Draw a tree with no open hypotheses for each, saying which formula you split on.

(i) $(\neg P(c) \to P(c)) \to P(c)$
(ii) $(P(c) \to Q(c)) \vee (Q(c) \to P(c))$
(iii) $\forall x\, (P(x) \vee \neg P(x))$

Hint: in (ii), split on $P(c)$: in each case one of the two implications is true for a cheap reason.

B10. Two sentences that look alike:

(i) $\exists x\, (\forall y\, P(y) \to P(x))$ (ii) $\exists x\, (P(x) \to \forall y\, P(y))$.

Both are valid. One has a tree of NJ with no open hypotheses; draw it. For the other, which A4 proved in NK, say what a tree of NJ would have to do, and why it cannot.

B11. Decide and justify. For each, say whether the entailment holds. If it does, give a tree (of NJ if you can, of NK if you must); if not, a counter-model.

(i) $\forall x\, (P(x) \to Q(x)),\ \neg Q(c) \vDash \neg P(c)$
(ii) $\forall x\, (P(x) \to Q(x)),\ \neg P(c) \vDash \neg Q(c)$
(iii) $\neg\exists x\, (P(x) \wedge Q(x)),\ P(c) \vDash \neg Q(c)$
(iv) $\forall x\, \forall y\, (R(x, y) \to R(y, x)),\ \exists x\, \exists y\, R(x, y) \vDash \exists x\, R(x, x)$

B12. Build it. Write (ser) for $\forall x\, \exists y\, R(x, y)$, (irr) for $\forall x\, \neg R(x, x)$ and (asy) for $\forall x\, \forall y\, (R(x, y) \to \neg R(y, x))$.

(i) Find a structure in which (ser) and (irr) are true, with as few things as possible, and say why no smaller one will do.
(ii) Do the same for (ser), (irr) and (asy) together.

B13. *(For the curious.)* Add to the three sentences of B12 the sentence (tra): $\forall x\, \forall y\, \forall z\, (R(x, y) \wedge R(y, z) \to R(x, z))$.

(i) Show that no structure with finitely many things makes all four true.
(ii) Find a structure that does.
(iii) Does $\{(\text{ser}), (\text{irr}), (\text{asy}), (\text{tra})\} \vDash \bot$ hold? Why can the recipe of A2, run by hand or by machine, never find this out?

B14. *(For the curious.)* A structure made of words, the *term structure*. Let Γ be $\{P(c),\ \forall x\, (P(x) \to P(f(x)))\}$. Take as the domain the closed terms themselves, $\mathbb{D} = \{c, f(c), f(f(c)), ...\}$, let $[\![c]\!]^{\mathfrak{M}}$ be the string c, and let $[\![f]\!]^{\mathfrak{M}}$ send a string t to the string $f(t)$.

(i) Which $[\![P]\!]^{\mathfrak{M}}$ makes this structure satisfy Γ? Show that $[\![P]\!]^{\mathfrak{M}} = \{c\}$ does not.
(ii) Nothing forbids a domain of strings. What is it about Γ that lets the sentences themselves say which rows $[\![P]\!]^{\mathfrak{M}}$ must have?