

2.3 Derived Rules: Proved Sequents as New Rules

Section 2.1 closed an impossible case by hand, and Section 2.2 proved negations by hand, one box at a time. By now the same few patterns keep coming back: the impossible case of Example (An impossible case), and a box that turns a known implication round. Mathematicians give such patterns names (“by contraposition”, “since P fails, Q ”) and use them in one breath. This section proves three of them once, from the rules we have, and then allows each to be used as a single line. The one new thing is that permission: a **derived rule**.

2.3.1 A box that keeps coming back

Here are two short arguments from different corners of mathematics.

Let n be an integer whose square is not even. Suppose n is even. Then n^2 is even, which contradicts the hypothesis. Hence n is not even.

Let x be a real number with $x^2 < 1$. Suppose $x \geq 1$. Then $x^2 \geq x \geq 1$, which contradicts $x^2 < 1$. Hence $x < 1$.

The subjects differ; the steps are the same. Each has a known implication (“if n is even, then n^2 is even”; “if $x \geq 1$, then $x^2 \geq 1$ ”), and a fact saying that the implication’s conclusion fails. Each then opens a box on the implication’s hypothesis, fires the implication inside it by $\rightarrow E$, meets the clash with $\neg E$, and closes the box by $\neg I$ (Definition 2.2.1). (For reals, $x^2 < 1$ and $x < 1$ are the exact negations of $x^2 \geq 1$ and $x \geq 1$.) The same four lines appear whenever an implication is used backwards, from the failure of its conclusion to the failure of its hypothesis.

A mathematician does not write these four lines. She writes “since n^2 is not even, n is not even”, or “by contraposition”, and moves on: the lines are the same every time. But a derivation is checked line by line against the rules, and “by contraposition” is not one of the rules. What licenses the short form? First we derive the pattern once, as a sequent, with the rules we have. Then we say exactly when a sequent already derived may be used as a single line.

2.3.2 Modus tollens, from the rules we have

The pattern of the two arguments is: from an implication and the negation of its conclusion, infer the negation of its hypothesis.

Proposition 2.3.1. Modus Tollens

$$P \rightarrow Q, \neg Q \vdash \neg P.$$

Idea. Read the skeleton off the goal. The goal $\neg P$ is a negation, and Section 2.2’s move for a negated goal is a box opened on what is negated, here P , with goal $\perp$. Inside the box, look for a clash (Section 2.1’s move for the goal $\perp$). The premise $\neg Q$ will clash with Q , so Q is the subgoal, and the premise $P \rightarrow Q$ gives it from the box’s own assumption. In the pictures, the box on P stands with its goal $\perp$; then $\neg E$ writes $\perp$ from the subgoal Q , still unjustified.

1	$P \rightarrow Q$		
2	$\neg Q$		
3	$\begin{array}{ l} P \\ \vdots \\ \perp \end{array}$	asm, for $\neg I$	
5	$\perp$		
6	$\neg P$	$\neg I$ 3–5	

1	$P \rightarrow Q$		
2	$\neg Q$		
3	$\begin{array}{ l} P \\ \vdots \\ Q \\ \perp \end{array}$	asm, for $\neg I$	
4	Q		
5	$\perp$	$\neg E$ 4, 2	
6	$\neg P$	$\neg I$ 3–5	

Proof. The following is a derivation with premises $P \rightarrow Q$ and $\neg Q$, and last line $\neg P$.

1	$P \rightarrow Q$		
2	$\neg Q$		
3	$\begin{array}{ l} P \\ \vdots \\ Q \\ \perp \end{array}$	asm, for $\neg I$	
4	Q	$\rightarrow E$ 1, 3	
5	$\perp$	$\neg E$ 4, 2	
6	$\neg P$	$\neg I$ 3–5	

Line 5 cites the premise on line 2, which lies in no box and so is available everywhere below it. The box 3–5 ends in $\perp$ as a line of its own, so $\neg I$ closes it on line 6. This proves the proposition. ■

The name is Latin for “the mode that takes away”: denying the conclusion takes away the hypothesis. Its partner, from $P \rightarrow Q$ and P to Q , is $\rightarrow E$, traditionally *modus ponens*, “the mode that puts” (Definition 1.3.1). The derivation uses $\rightarrow E$, $\neg E$, and $\neg I$, and nothing else.

A second form of the same fact packs the two premises into one implication. It is the form in which mathematicians state it: an implication **implies** its contrapositive.

Proposition 2.3.2. Contrapositive

$$P \rightarrow Q \vdash \neg Q \rightarrow \neg P.$$

Idea. The goal is an implication, so Chapter 1’s first goal-directed move applies: open a box with its hypothesis $\neg Q$, and the new goal is $\neg P$. That goal is a negation, so open a second box, on P , inside the first. Inside both boxes we are exactly where the proof of [Proposition 2.3.1](#) was: P and $P \rightarrow Q$ give Q , which clashes with $\neg Q$.

Proof. The following is a derivation with premise $P \rightarrow Q$ and last line $\neg Q \rightarrow \neg P$.

1	$P \rightarrow Q$	
2	$\neg Q$	asm, for $\rightarrow I$
3	P	asm, for $\neg I$
4	Q	$\rightarrow E$ 1, 3
5	$\perp$	$\neg E$ 4, 2
6	$\neg P$	$\neg I$ 3–5
7	$\neg Q \rightarrow \neg P$	$\rightarrow I$ 2–6

Line 5 may cite line 2, because the only box containing line 2, the box 2–6, also contains line 5 (the scope rule of Definition 1.4.2). The inner box closes on line 6, a line of the outer box itself, and line 7 closes the outer box. This proves the proposition. ■

The statement $\neg Q \rightarrow \neg P$ is called the **contrapositive** of $P \rightarrow Q$. Like modus tollens, its derivation uses only the rules so far: $\rightarrow I$, $\rightarrow E$, $\neg I$, and $\neg E$. The passage back, from $\neg Q \rightarrow \neg P$ to $P \rightarrow Q$, is a different matter (Common errors, below).

Now compare the two derivations. Lines 3–6 of the derivation of [Proposition 2.3.1](#) are, line for line and citation for citation, lines 3–6 of the derivation of [Proposition 2.3.2](#): P , then Q by $\rightarrow E$ 1, 3, then $\perp$ by $\neg E$ 4, 2, then $\neg P$ by $\neg I$ 3–5. And they are the four lines of the two arguments that opened this section. Writing them out every time buries the argument in bookkeeping.

2.3.3 What a derived rule is

A sequent that has been derived may be used as a rule.

This is what a mathematician does when she writes “by Lemma 3”: the lemma was proved once, and each use of it is a single step. For derivations we must say exactly what that step may do.

Definition 2.3.1. Derived Rule

Let $\alpha_1, \dots, \alpha_n \vdash \beta$ be a sequent, written with statement letters, that has **already been derived** earlier in the book. In a later derivation, replace each letter in $\alpha_1, \dots, \alpha_n, \beta$ by a statement, the **same** statement for every occurrence of the same letter. If lines $i_1, \dots, i_n$, all **available** at line k , hold the resulting instances of $\alpha_1, \dots, \alpha_n$, we may write the resulting instance of β on line k . The justification names the result and cites $i_1, \dots, i_n$. A sequent used in this way is a **derived rule**. For example, [Proposition 2.3.1](#) becomes the rule MT:

i		$\varphi \rightarrow \psi$	
j		$\neg\psi$	
k		$\neg\varphi$	MT i, j

In words: a proved sequent is a new rule. Its premises become the cited lines, its conclusion the

line written, and its letters the metavariables of a schema (Definition 1.2.1). Read the definition clause by clause.

1. **“Already derived.”** The sequent must have been derived **before** the line that uses it: earlier in the book, and never inside its own derivation. A derivation that used a sequent to derive that same sequent would prove nothing.
2. **“Replace each letter ... the same statement for every occurrence.”** The letters of a derived sequent stood for arbitrary statements all along (Definition 1.2.3), so they may be replaced by any statements, provided the replacement is **uniform**. From $(A \wedge B) \rightarrow C$ and $\neg C$, the rule MT gives $\neg(A \wedge B)$, with the letters P and Q of [Proposition 2.3.1](#) (written φ and ψ in the schema) replaced by $A \wedge B$ and C .
3. **“Available at line k .”** The scope rule of Definition 1.4.2 still governs every citation. A derived rule may not reach into a closed box, just as a primitive rule may not.
4. **“The resulting instance of β .”** The rule writes the conclusion, with the same replacement, and nothing else. The derived rule does not open or close any box of the derivation that uses it.

We give the derived rules of this section short tags: MT for [Proposition 2.3.1](#), CP for [Proposition 2.3.2](#), and, once it is proved below, DS for [Proposition 2.3.4](#). Every other derived sequent is a derived rule too, cited by its name: the four lines 2–5 of Example (An implication with an impossible hypothesis), for instance, are now one line citing Proposition 2.1.2.

Left: with the derived rule. Right: written out.

1	$P \rightarrow Q$		1	$P \rightarrow Q$	
2	$\neg Q$		2	$\neg Q$	
3	$\neg P$	MT 1, 2	3	P	asm, for $\neg$ I
			4	Q	$\rightarrow$ E 1, 3
			5	$\perp$	$\neg$ E 4, 2
			6	$\neg P$	$\neg$ I 3–5

Line 3 on the left stands for lines 3–6 on the right: the same premises, the same last line.

A derived rule is shorthand for lines we could always write out, so it lets us prove nothing that the primitive rules could not.

Quick check. In the figure, which lines does line 3 on the left cite, and which lines on the right use those same two premises?

Solution. Lines 1 and 2. On the right, line 4 cites line 1 and line 5 cites line 2.

🕒 **Second reading** · *Why a derived rule adds no power*

Convenience, not power. A derived-rule line abbreviates a stretch of derivation that we could write out in full. To expand it, repeat each cited line by (D3) of Definition 1.4.2, then copy the derivation of the sequent below the repetitions, with its letters replaced, its premises replaced

by the repetitions, and its line numbers shifted. Every citation inside the copy points inside the copy or to a repetition, all in the current box, so every citation is available. The copy's boxes close before its last line, which is the instance of β . If the copy itself uses derived rules, expand those lines in the same way; this stops, because each derivation cites only results proved before it. So whatever can be derived with derived rules can be derived with the primitive rules alone.

The degenerate case is a sequent with nothing done to its premise, $P \vdash P$, whose derivation is the single premise line (part (a) of Example (Derivations, simplest first)): as a derived rule it copies an available line, which repetition already does. The first use with content is modus tollens proved a second time, with CP as a rule. The premise $P \rightarrow Q$ invites CP, and its conclusion $\neg Q \rightarrow \neg P$ is an implication whose hypothesis is the other premise.

1		$P \rightarrow Q$	
2		$\neg Q$	
3		$\neg Q \rightarrow \neg P$	CP 1
4		$\neg P$	$\rightarrow E$ 3, 2

Line 3 is the instance of [Proposition 2.3.2](#) with P and Q replaced by themselves; line 4 is modus ponens on it. Written out in full, line 3 would become a repetition of line 1 followed by lines 2–7 of the derivation of [Proposition 2.3.2](#). This is honest because [Proposition 2.3.2](#) was derived from the primitive rules, not from [Proposition 2.3.1](#): the chain of derived rules ends in primitive rules, without a loop.

Warning. A derived rule must match its sequent exactly, under one uniform replacement of letters. From $P \rightarrow Q$ and $\neg R$, MT gives nothing: no single statement in place of ψ turns the pair into $\varphi \rightarrow \psi$ and $\neg\psi$. Equally, from $P \rightarrow \neg Q$ and Q , MT gives nothing yet: it needs the negation of the conclusion, $\neg\neg Q$, and Q is not that line. (Here $\neg I$ would give $\neg\neg Q$ first, as in Example (Two negations from one premise), and then MT applies.) Likewise DS, as stated below, refutes the **left** disjunct; applied blindly to $P \vee Q$ and $\neg Q$, it does not match.

In the Givens/Goal table, a derived rule adds its conclusion to the Givens in one row, as an elimination rule does.

2.3.4 Pasting whole derivations: weakening and cut

The figure expands one derived-rule line inside a derivation. Outside every box there is a cleaner statement, about whole derivations: two derivations can be joined end to end, and premises that are never used do no harm.

Lemma 2.3.3. Weakening and Cut

Let Γ and Δ be lists of statements, and let $\varphi, \psi, \alpha_1, \dots, \alpha_m$ ($m \geq 1$), and β be statements.

- (a) **Weakening.** If $\Gamma \vdash \psi$ and every member of Γ is a member of Δ , then $\Delta \vdash \psi$. In particular, $\Gamma \vdash \psi$ implies $\Gamma, \varphi \vdash \psi$.

- (b) **Cut.** If $\Gamma \vdash \varphi$ and $\Gamma, \varphi \vdash \psi$, then $\Gamma \vdash \psi$.
 (c) **Chaining.** If $\Gamma \vdash \alpha_i$ for **every** $i = 1, \dots, m$, and $\alpha_1, \dots, \alpha_m \vdash \beta$, then $\Gamma \vdash \beta$.

In words: (a) extra premises never hurt; (b) a statement that has been derived may be used as a premise; (c) a sequent already proved can be applied to statements already derived. Part (c) is Definition 2.3.1 for whole derivations, outside every box; inside a box, the expansion of the fold “Why a derived rule adds no power” does the same job.

Chaining and cut are the reason a derived-rule line outside every box is legitimate: the lines it cites lie in no box, so the derivation up to each of them derives it from Γ , and (c) then derives the instance of the sequent’s conclusion from Γ ; by (b), the rest of the derivation may use that instance.

◉ **Second reading** · *The proof: pasting derivations*

Idea. Part (a) is read off Definition 1.2.3, which asks only that the premises of the derivation **belong to** the list. For (b) and (c), write the derivations one after another and let the last one cite, instead of its premise α_i , the last line of the derivation of α_i . The only thing to check is the scope rule of Definition 1.4.2: the last line of a derivation lies in no box, so it stays available to everything written after it.

Proof. (a) A derivation witnessing $\Gamma \vdash \psi$ has premises that belong to Γ , hence to Δ , and its last line is ψ . By Definition 1.2.3 it witnesses $\Delta \vdash \psi$. The second sentence is the case where Δ is Γ, φ .

For (b) and (c) we prove one statement that contains both:

(*) If $\Gamma \vdash \alpha_i$ for every $i = 1, \dots, m$, and $\Gamma, \alpha_1, \dots, \alpha_m \vdash \beta$, then $\Gamma \vdash \beta$.

Part (b) is (*) with $m = 1$, $\alpha_1 = \varphi$ and $\beta = \psi$. Part (c) follows from (*), since $\alpha_1, \dots, \alpha_m \vdash \beta$ gives $\Gamma, \alpha_1, \dots, \alpha_m \vdash \beta$ by (a).

To prove (*), let D_i be a derivation of α_i with premises in Γ , for each i , and let E be a derivation of β with premises in $\Gamma, \alpha_1, \dots, \alpha_m$. If the last line of E is one of its premises, then β is a member of Γ , and the one-line derivation whose only line is the premise β shows $\Gamma \vdash \beta$; or β is some α_i , and D_i shows $\Gamma \vdash \beta$. Otherwise, build a list of lines F as follows.

1. First, as premises, every premise of $D_1, \dots, D_m$, and every premise of E that is a member of Γ .
2. Then the lines of D_1 that are not premises, then those of D_2 , and so on up to D_m , each with its boxes.
3. Then the lines of E that are not premises, with its boxes.

Renumber the lines, and change each citation as follows. A citation of a premise that is in Γ now cites the premise line of step 1 carrying that statement. A citation in E of a premise α_i that is not in Γ now cites the last line of D_i ; that line is not a premise of D_i , because the premises of D_i are in Γ and α_i is not, so it was copied in step 2. Every other citation follows its line to its new number.

We check that F is a derivation (Definition 1.4.2). The premises come first and lie in no box.

The boxes are those of the D_i and of E , moved as blocks, so two boxes are still disjoint or nested, each still begins with its assumption, and each line lies in exactly the boxes it lay in before. Hence a line and a box that were available at a citing line are still available there, since the boxes containing each are unchanged. A premise line of step 1 lies in no box and comes first, so it is available at every later line. The last line of D_i lies in no box (it was the last line of a derivation) and comes before every line of E , so it is available at every line of E . Each line carries the same statement and the same justification as before, citing lines with the same statements, so it is an instance of the same rule. Finally, the last line of F is the last line of E , namely β , and it lies in no box. The premises of F are all in Γ . Therefore $\Gamma \vdash \beta$, which proves (*). ■

Quick check. Given Proposition 2.3.1, which part of Lemma 2.3.3 gives $P \rightarrow Q, \neg Q, R \vdash \neg P$ at once? Given also Proposition 2.1.2, which part gives $P \rightarrow Q, \neg Q \vdash P \rightarrow R$?

Solution. Part (a), weakening, with R as the extra premise. Part (c), chaining, with $m = 1$, $\alpha_1 = \neg P$ and $\beta = P \rightarrow R$: Proposition 2.3.1 gives $P \rightarrow Q, \neg Q \vdash \neg P$, and Proposition 2.1.2 with R in place of Q gives $\neg P \vdash P \rightarrow R$. (Part (a) and then part (b) do the same.)

2.3.5 Disjunctive syllogism: the impossible case, filed

The second pattern is the impossible case of Section 2.1. Every integer is even or odd; this one is not even; so it is odd. A disjunction, one side refuted, the other side left.

Proposition 2.3.4. Disjunctive Syllogism

$P \vee Q, \neg P \vdash Q$.

Idea. This is Example (An impossible case) with a simpler clash. There, the case P produced R by $\rightarrow E$, which clashed with $\neg R$. Here the case P clashes with the premise $\neg P$ at once. So: split the premise $P \vee Q$ by $\vee E$, both boxes ending in the current goal Q . The Q box is its own assumption. The P box cannot reach Q honestly, so it reaches a clash and closes by $\perp E$: an impossible case closes itself.

Proof. The following is a derivation with premises $P \vee Q$ and $\neg P$, and last line Q .

1		$P \vee Q$	
2		$\neg P$	
3			P asm, for $\vee E$
4			$\perp$ $\neg E$ 3, 2
5			Q $\perp E$ 4
6			Q asm, for $\vee E$
7		Q	$\vee E$ 1, 3–5, 6–6

The two boxes 3–5 and 6–6 are separate. The second consists of its assumption alone, which is already the statement Q that $\vee E$ needs. This proves the proposition. ■

Set the derivation beside that of Example (An impossible case). Both split $P \vee Q$ into the same two boxes, and in both the Q box is one line long. Inside the P box, two lines reached $\perp$ there (lines 5–6) and one line does here (line 4); then $\perp E$ closes the box in the same way. From now on this whole stretch is one line, tagged DS.

The rule as stated refutes the **left** disjunct. To refute the right one, first put the disjunction in the other order; that, too, is now one line, since Example (First derivations with “or”) derived $P \vee Q \vdash Q \vee P$. (Exercise B1 derives the mirror image directly.)

Example. Derived rules in use

- (a) Show that $P \rightarrow Q$, $Q \rightarrow R$, $\neg R \vdash \neg P$, and then write the derivation out with primitive rules only.
- (b) Show that $P \vee Q$, $\neg P$, $Q \rightarrow R \vdash R$.

Solution. Idea. A derived rule is a **premise-directed shortcut**: a line $\varphi \rightarrow \psi$ with a line $\neg\psi$ invites MT; a disjunction with one side refuted invites DS. This is the move this section adds to the search for derivations: before opening a box by hand, ask whether a derived rule takes the step at once.

- (a) Work backwards from the goal $\neg P$. The premise $P \rightarrow Q$ would give it by MT if $\neg Q$ were available. And $\neg Q$ comes by MT from $Q \rightarrow R$ and $\neg R$. So MT is used twice, the second time on the conclusion of the first.

1		$P \rightarrow Q$	1		$P \rightarrow Q$	
2		$Q \rightarrow R$	2		$Q \rightarrow R$	
3		$\neg R$	3		$\neg R$	
		$\vdots$			$\vdots$	
5		$\neg P$	4		$\neg Q$	
			5		$\neg P$	MT 1, 4

1	$P \rightarrow Q$	
2	$Q \rightarrow R$	
3	$\neg R$	
4	$\neg Q$	MT 2, 3
5	$\neg P$	MT 1, 4

Line 4 is the instance with φ replaced by Q and ψ by R ; line 5 the instance with P and Q . In primitive rules, each MT line becomes its four lines, as in lines 3–6 of the derivation of [Proposition 2.3.1](#): a box on the hypothesis, $\rightarrow E$, $\neg E$, $\neg I$. This natural expansion has eleven lines.

1	$P \rightarrow Q$	
2	$Q \rightarrow R$	
3	$\neg R$	
4	Q	asm, for $\neg I$
5	R	$\rightarrow E$ 2, 4
6	$\perp$	$\neg E$ 5, 3
7	$\neg Q$	$\neg I$ 4–6
8	P	asm, for $\neg I$
9	Q	$\rightarrow E$ 1, 8
10	$\perp$	$\neg E$ 9, 7
11	$\neg P$	$\neg I$ 8–10

The literal expansion of the fold “Why a derived rule adds no power” adds a repetition of each cited line and is longer; the natural one cites the available lines directly.

- (b) The disjunction $P \vee Q$ has its left side refuted by $\neg P$, so DS gives Q , and then $Q \rightarrow R$ fires.

1	$P \vee Q$	1	$P \vee Q$
2	$\neg P$	2	$\neg P$
3	$Q \rightarrow R$	3	$Q \rightarrow R$
	$\vdots$		$\vdots$
5	R	4	Q
		5	R
			$\rightarrow E$ 3, 4

1	$P \vee Q$	
2	$\neg P$	
3	$Q \rightarrow R$	
4	Q	DS 1, 2
5	R	$\rightarrow E$ 3, 4

Expanded, line 4 becomes lines 3–7 of the derivation of [Proposition 2.3.4](#) (five lines), with a case split on line 1 and the case P closed by $\perp E$.

Quick check. Which derived rule of this section, if any, gives a new line in one step from each pair of available lines?

- (i) $P \rightarrow Q$ and $\neg Q$. (ii) $P \vee Q$ and $\neg P$. (iii) $P \vee Q$ and $Q \rightarrow R$. (iv) $P \rightarrow \neg Q$ and Q .

Solution.

- (i) MT gives $\neg P$. (ii) DS gives Q . (iii) None: nothing is known about the case P . (iv) None in one step: MT needs the negation of the conclusion $\neg Q$, which is $\neg\neg Q$, not Q . A $\neg I$ box gives $\neg\neg Q$ from Q first, as in Example (Two negations from one premise), and then MT gives $\neg P$.

2.3.6 Modus tollens on numbers, and the green card

In a mathematical proof, MT is the step “since the conclusion fails, the hypothesis fails”. Here it is with numbers.

Example. Modus tollens on numbers

Let x be a real number with $x^2 \leq 4$. Use the implication “if $x > 2$, then $x^2 > 4$ ” to show that $x \leq 2$, naming the derived rule.

Solution. Take P : “ $x > 2$ ” and Q : “ $x^2 > 4$ ”. The implication is $P \rightarrow Q$. (It holds because $x > 2 > 0$ gives $x^2 = x \cdot x > 2x > 4$.) The hypothesis $x^2 \leq 4$ is $\neg Q$, since for real numbers $x^2 \leq 4$ and $x^2 > 4$ are exact negations of each other. By MT ([Proposition 2.3.1](#)), $\neg P$, that is, $\neg(x > 2)$, which is $x \leq 2$.

The claim of Example (Four cards) (Section 1.3), for one card, is $E \rightarrow R$, with E : “this card’s number is even” and R : “its color side is red”.

The card shows	So we have	What a rule gives	Turn it?
6	E	$\rightarrow E$: R ; the back must be red	yes: a green back would break the claim
7	$\neg E$	nothing about R : no rule takes $E \rightarrow R$ and $\neg E$ to R or to $\neg R$	no

The card shows	So we have	What a rule gives	Turn it?
red	R	nothing about E : concluding E would be affirming the consequent	no
green	$\neg R$	MT: $\neg E$; the number must be odd	yes: an even number would break the claim

Turning the green card tests exactly the line MT wrote: an even number there gives E , and with $\neg R$ and $E \rightarrow R$, $\rightarrow E$ and $\neg E$ reach $\perp$. Modus tollens is the step people skip.

CP turns the claim into its contrapositive $\neg R \rightarrow \neg E$, “a card whose color is not red has an odd number”, which carries the claim’s content to the green card; Section 2.5 derives the passage back, so the two say the same. The converse $R \rightarrow E$, “a red card has an even number”, is a different claim, and the card rule never made it.

Quick check. Which card would MT settle if the claim were “if a card’s color side is red, then its number is even”?

Solution. The 7. The claim is $R \rightarrow E$, the 7 shows $\neg E$, and MT gives $\neg R$, so its back must not be red: turn it.

🕒 Second reading • Modus tollens and testing a claim

A claim about every integer of a kind makes one prediction per instance. “For every prime p , the number $2^p - 1$ is prime” predicts that 3, 7, 31 and 127 are prime, for $p = 2, 3, 5, 7$, and all four are. Write A for the claim and B for one prediction, so that $A \rightarrow B$. The form “from $A \rightarrow B$ and B , conclude A ” breaks (it is affirming the consequent, Section 1.3), so no number of confirming instances proves the claim. One failed instance refutes it, by MT on that instance: for $p = 11$, $2^{11} - 1 = 2047 = 23 \cdot 89$, so the prediction B fails, and from $A \rightarrow B$ and $\neg B$, MT gives $\neg A$. Scientists call a hypothesis that has survived many tests *corroborated*, not proved; a mathematician calls such a claim a conjecture.

2.3.7 How this rule looks in a mathematical proof

Theorem 2.1.3 (Section 2.1) says that for an integer n , if n^2 is even then n is even. Section 2.1 proved it by cases, with the odd case shown impossible and closed by $\perp E$. Here is the same theorem argued as mathematicians usually write it, with the derived rules doing the work. We use the facts (E1)–(E3) of Section 2.1: every integer is even or odd; no integer is both; the square of an odd integer is odd.

Written the way a mathematician would write it, the proof is four sentences: *Suppose n^2 is even. Then n^2 is not odd, since no integer is both. By the contrapositive of (E3), n is not odd.*

As every integer is even or odd, n is even. Each sentence after the first is one named step: $\neg$ I with (E2); CP with $\rightarrow$ E; DS, after exchanging the disjuncts of (E1), as line 11 of the derivation below does. The example below writes the same proof with every step tagged, and then as a derivation.

Example. Even square, even number, by contraposition

Let n be an integer. Prove that if n^2 is even, then n is even, using CP and DS, and label each step with its rule.

Solution. Idea. The hypothesis “ n^2 is even” hands us nothing to compute with, while “ n is odd” hands us $n = 2k + 1$. So we turn (E3) round by CP: a number whose square is not odd is not odd itself. Then (E1), with one side refuted, leaves “even” by DS.

Suppose n^2 is even [assumption for $\rightarrow$ I]. If n^2 were odd [assumption for $\neg$ I], it would be both even and odd [$\wedge$ I], contradicting (E2) [$\neg$ E]; hence n^2 is not odd [$\neg$ I]. By (E3), if n is odd then n^2 is odd, so by contraposition, if n^2 is not odd then n is not odd [CP]. Hence n is not odd [$\rightarrow$ E]. By (E1), n is even or odd, so n is odd or even [or commutes], by the exchange of disjuncts of Example (First derivations with “or”) used as a derived rule. Since n is not odd, n is even [DS]. This proves that if n^2 is even, then n is even [$\rightarrow$ I].

With E : “ n is even”, O : “ n is odd”, S : “ n^2 is even”, T : “ n^2 is odd”, and the three facts as premises, the skeleton is this derivation.

1	$E \vee O$	
2	$\neg(S \wedge T)$	
3	$O \rightarrow T$	
4	S	asm, for $\rightarrow$ I
5	T	asm, for $\neg$ I
6	$S \wedge T$	$\wedge$ I 4, 5
7	$\perp$	$\neg$ E 6, 2
8	$\neg T$	$\neg$ I 5–7
9	$\neg T \rightarrow \neg O$	CP 3
10	$\neg O$	$\rightarrow$ E 9, 8
11	$O \vee E$	or commutes 1
12	E	DS 11, 10
13	$S \rightarrow E$	$\rightarrow$ I 4–12

Line 11 is Example (First derivations with “or”) used as a derived rule, so that line 12 refutes the left disjunct, as DS requires.

🕒 **Second reading** · *The two derivations of Even Square, line for line*

Compare this with the twelve-line derivation after Theorem 2.1.3 in Section 2.1. There, line 11 split on (E1) at once, and the odd case, lines 6–10, got T from (E3), built $S \wedge T$, clashed with (E2), and closed by $\perp$ E. Here the same work is spread over named steps. The $\neg$ I box on lines 5–7 does the clash with (E2), which there was lines 8–9. Lines 9 and 10, CP and $\rightarrow$ E, abbreviate a box that assumes O , gets T by (E3), as line 7 did there, and clashes with line 8. Line 12, DS, abbreviates a case split on the disjunction with the case O closed by $\perp$ E, as lines 5–11 did there. The short version reads the way people talk.

2.3.8 Common errors

Warning. A derived rule may be used only **after** its sequent has been derived, and never inside its own derivation. A “derivation” of Proposition 2.3.2 that justifies one of its lines by CP proves nothing: it assumes what it sets out to show. Exercise C2 is an example.

Warning. The converse of the contrapositive is a different sequent. CP passes from $P \rightarrow Q$ to $\neg Q \rightarrow \neg P$; it does not pass from $\neg Q \rightarrow \neg P$ back to $P \rightarrow Q$. Try it: in a box on P the goal is Q , a letter with no negation, and the natural box, on $\neg Q$, reaches $\perp$ and so closes to $\neg\neg Q$, not Q . Section 2.5 derives the passage back with a new rule.

2.3.9 The rule card

Example. Instances of MT, CP and DS

A sequent is proved once, for letters, and used for every statement put in their place. So it pays to prove a lemma with the fewest premises and the most general letters it allows: one derivation, written once, serves every row of its rule below.

Rule	Letters replaced	Cited lines	New line
MT	$\varphi := P \vee Q,$ $\psi := R \wedge S$	$(P \vee Q) \rightarrow (R \wedge S),$ $\neg(R \wedge S)$	$\neg(P \vee Q)$
CP	$\varphi := \neg P,$ $\psi := Q \rightarrow R$	$\neg P \rightarrow (Q \rightarrow R)$	$\neg(Q \rightarrow R) \rightarrow \neg\neg P$
DS	$\varphi := P \rightarrow Q,$ $\psi := \neg R \vee S$	$(P \rightarrow Q) \vee (\neg R \vee S),$ $\neg(P \rightarrow Q)$	$\neg R \vee S$

Not an instance. From $(P \rightarrow Q) \vee R$ and $\neg P$, DS gives nothing: the refuted line must be the negation of the whole left disjunct, $\neg(P \rightarrow Q)$, and $\neg P$ is not that line.

Chapter 1’s seven rules are on the card at the end of Section 1.6; here are this chapter’s so far.

Rule	Shape	You write	Lean
$\neg E$	$\varphi, \neg\varphi \implies \perp$	“..., which contradicts ...”	<code>exact hn hp</code> (goal <code>False</code>)
$\perp E$	$\perp \implies \text{any } \varphi$	“This case cannot occur.” “So there is nothing to prove.”	<code>exfalso</code>
$\neg I$	$\text{box } \varphi \dots \perp \implies \neg\varphi$	“Suppose P This is a contradiction. Hence not P .”	<code>intro hp</code> (goal <code>False</code>)
MT	(derived) $\varphi \rightarrow \psi, \neg\psi \implies \neg\varphi$	“Since Q fails, so does P .”	<code>mt h hnq</code>
CP	(derived) $\varphi \rightarrow \psi \implies \neg\psi \rightarrow \neg\varphi$	“We prove the contrapositive: suppose not Q ; ... so not P .”	<code>mt</code>
DS	(derived) $\varphi \vee \psi, \neg\varphi \implies \psi$	“ P is impossible, so Q .”	<code>h.resolve_left hnp Q</code>

Warning (Not allowed: derived rules). Each step breaks the clause of the reading of [Definition 2.3.1](#) shown.

- “CP on a line of the derivation of [Proposition 2.3.2](#)”: the sequent is not yet derived where it is used (clause 1; Exercise C2).
- “ $\neg P$ by MT from $(P \wedge Q) \rightarrow R$ and $\neg R$ ”: MT writes the negation of the whole hypothesis, $\neg(P \wedge Q)$ (clause 4).
- “MT citing a line inside a closed box”: the scope rule still governs every citation (clause 3).
- “ $\neg P$ in one line from $P \rightarrow Q, Q \rightarrow R, \neg R$ ”: one instance per line; [Example \(Derived rules in use\)](#) (a) takes two MT lines (clause 4).
- “ P by $\neg\neg E$ from $\neg\neg P$, here”: $\neg\neg E$ is derived only in Section 2.5 (clause 1).

Remark (Looking ahead). Chapter 4 makes exact the replacement of letters that a derived rule allows, under the name substitution.

2.3.10 Exercises

2.3.10.1 A. Check your understanding

Exercise. A1

- State [Definition 2.3.1](#) in your own words, including what “already derived” and “the same statement” require.
- Here is a derivation that uses MT. Rewrite it with primitive rules only.

1		$R \rightarrow P$	
2		$\neg P$	
3		$\neg R$	MT 1, 2
4		$\neg R \vee S$	$\vee I$ 3

- (c) True or false, with a reason: “ $\neg Q \rightarrow \neg P$ follows from $P \rightarrow Q$ by CP, so $P \rightarrow Q$ follows from $\neg Q \rightarrow \neg P$ by CP.”

Solution.

- (a) If a sequent has been derived earlier (not inside the derivation that uses it), then in a later derivation we may replace its letters by statements, each letter by one statement everywhere it occurs, and, when available lines hold the resulting instances of its premises, write the resulting instance of its conclusion on one line, citing the sequent and those lines.

- (b) Line 3 becomes a box on R , then $\rightarrow E$, $\neg E$, and $\neg I$:

1		$R \rightarrow P$	
2		$\neg P$	
3			asm, for $\neg I$
4			
5			
6		$\neg R$	$\neg I$ 3–5
7		$\neg R \vee S$	$\vee I$ 6

- (c) False. CP is the sequent $P \rightarrow Q \vdash \neg Q \rightarrow \neg P$. Applied to $\neg Q \rightarrow \neg P$, with P replaced by $\neg Q$ and Q by $\neg P$, it gives $\neg\neg P \rightarrow \neg\neg Q$, not $P \rightarrow Q$. The passage from $\neg Q \rightarrow \neg P$ to $P \rightarrow Q$ is the converse, a different sequent; Section 2.5 derives it with a new rule.

Exercise. A2: Drill

Each part takes a line or two. The parts run from single steps, through a missing line and a justification column, to whole derivations. Let x be a real number.

- Lines 1 $(A \wedge B) \rightarrow C$, 2 $\neg C$. What does “MT 1, 2” write?
- Lines 1 $\neg P \vee Q$, 2 $\neg\neg P$. What does “DS 1, 2” write?
- What does CP write from $(x > 0) \rightarrow (x^2 > 0)$?
- Line 3 is $\neg(P \vee Q)$ and line 5 is $\neg R \rightarrow (P \vee Q)$. What does “MT 5, 3” write?
- Written out with primitive rules, citing available lines directly, how many lines does one MT line become?
- Line 8 is $\neg(R \wedge S)$, justified “MT 2, 6”, and line 6 is $\neg T$. What is line 2?
- Line 9 is $R \rightarrow S$, justified “DS 4, 7”, and line 7 is $\neg(P \wedge Q)$. What is line 4?
- Lines 1–4 are the premises $P \vee (Q \rightarrow R)$, $\neg P$, $S \rightarrow Q$, $\neg R$. Justify 5 $Q \rightarrow R$; 6 $\neg Q$; 7 $\neg S$.

- (i) Lines 1 $P \rightarrow \neg Q$, 2 Q . Does MT apply?
- (j) Lines 1 $P \vee Q$, 2 $\neg Q$. Does DS, as stated, apply?
- (k) May a derivation of [Proposition 2.3.2](#) use CP on one of its lines?
- (l) Find the illegal line: 1 $P \rightarrow Q$; 2 $\neg P$; 3 $\neg Q$, MT 1, 2.
- (m) Derive $P \rightarrow (Q \wedge R)$, $\neg R \vdash \neg P$.
- (n) Derive $P \vee Q$, $\neg P$, $\neg Q \vdash R$.
- (o) Derive $\neg P \rightarrow Q$, $\neg Q \vdash \neg\neg P$ in one line.

Solution.

- (a) $\neg(A \wedge B)$.
- (b) Q (the letter P of DS replaced by $\neg P$).
- (c) $\neg(x^2 > 0) \rightarrow \neg(x > 0)$, that is, $(x^2 \leq 0) \rightarrow (x \leq 0)$.
- (d) $\neg\neg R$, with $\varphi := \neg R$ and $\psi := P \vee Q$.
- (e) Four: an assumption, $\rightarrow E$, $\neg E$, $\neg I$ (the figure).
- (f) $(R \wedge S) \rightarrow T$.
- (g) $(P \wedge Q) \vee (R \rightarrow S)$.
- (h) 5 DS 1, 2; 6 MT 5, 4; 7 MT 3, 6.
- (i) Not yet: MT needs $\neg\neg Q$. Write it from Q by a $\neg I$ box first; then MT gives $\neg P$.
- (j) No: DS refutes the left disjunct. Use the other form (Exercise B1 (a)) or exchange the disjuncts first.
- (k) No: a derived rule may be used only after its sequent has been derived.
- (l) Line 3: MT needs the negation of the conclusion, $\neg Q$, and gives $\neg P$; line 3 runs it backwards, from $\neg P$ to $\neg Q$. The form breaks at P false, Q true.
- (m) 3 P , assumption; 4 $Q \wedge R$, $\rightarrow E$ 1, 3; 5 R , $\wedge E$ 4; 6 $\perp$, $\neg E$ 5, 2; 7 $\neg P$, $\neg I$ 3–6. (MT does not match: $\neg(Q \wedge R)$ is not available.)
- (n) 4 Q , DS 1, 2; 5 $\perp$, $\neg E$ 4, 3; 6 R , $\perp E$ 5.
- (o) 3 $\neg\neg P$, MT 1, 2.

2.3.10.2 B. Practice

Exercise. B1: The other disjunctive syllogism, used later

- (a) Show that $P \vee Q$, $\neg Q \vdash P$ by a derivation from the primitive rules.
- (b) Let x be a real number with $x^2 = 1$ and $x > 0$. You may use that $x^2 = 1$ implies $x = 1$ or $x = -1$. Deduce that $x = 1$, naming the result you use.

Solution.

- (a) As in [Proposition 2.3.4](#), with the roles of the boxes exchanged: now the case Q is the impossible one.

1	$P \vee Q$	
2	$\neg Q$	
3	P	asm, for $\vee E$
4	Q	asm, for $\vee E$
5	$\perp$	$\neg E$ 4, 2
6	P	$\perp E$ 5
7	P	$\vee E$ 1, 3–3, 4–6

- (b) Since $x^2 = 1$, we have $x = 1$ or $x = -1$. Since $x > 0$ and $-1 < 0$, we have $x \neq -1$. By part (a), with P : “ $x = 1$ ” and Q : “ $x = -1$ ”, used as a derived rule ([Definition 2.3.1](#)), we conclude $x = 1$.

Exercise. B2: Putting a derivation in order

Here are nine lines, each a statement with its justification. Seven of them, in the right order and with the right boxes, form a derivation of $P \rightarrow Q \vdash \neg Q \rightarrow \neg P$ from the primitive rules. Give the order, and say where each box opens and closes. Then say why each of the other two lines cannot be used.

- (i) $\neg Q \rightarrow \neg P$, by $\rightarrow I$ on the box from $\neg Q$ to $\neg P$.
- (ii) Q , by $\rightarrow E$ from $P \rightarrow Q$ and P .
- (iii) $P \rightarrow Q$, premise.
- (iv) $\neg P$, by $\neg I$ on the box from P to $\perp$.
- (v) $\neg Q$, assumption.
- (vi) $\perp$, by $\neg E$ from Q and $\neg Q$.
- (vii) P , assumption.
- (viii) $\neg P$, assumption, opening the box for the $\neg I$ that proves $\neg P$.
- (ix) Q , by $\rightarrow E$ from $P \rightarrow Q$ and the assumption P of (vii), written directly below (iv).

Solution. The order is (iii), (v), (vii), (ii), (vi), (iv), (i), with one box opened by (v) and closed after (iv), and a second box inside it, opened by (vii) and closed after (vi). This is the derivation of [Proposition 2.3.2](#). It is the only admissible order. The premise comes first. (i) needs a box from $\neg Q$ to $\neg P$, so (v) opens a box whose last line is (iv). (iv) needs a box from P to $\perp$ inside it, so (vii) opens a box whose last line is (vi). Inside that box, (ii) needs (vii), and (vi) needs (ii) and (v).

- (viii) cannot be used. $\neg I$ proves $\neg P$ from a box opened by P , the statement being negated ([Definition 2.2.1](#)). A box opened by $\neg P$ and ending in $\perp$ would give $\neg\neg P$. (ix) cannot be used where it is placed. Directly below (iv), the box opened by (vii) has closed, so the assumption P is not available ([Definition 1.4.2](#)). Placed inside that box, the same line is (ii).

Exercise. B3: Two refutations

A search for $(P \vee Q) \rightarrow R$, $\neg R \vdash \neg P \wedge \neg Q$ has reached the stage below. You may use the derived rules of this section. *Name the move, then complete it.*

1		$(P \vee Q) \rightarrow R$	
2		$\neg R$	
3		$\neg(P \vee Q)$	MT 1, 2
		$\vdots$	
12		$\neg P \wedge \neg Q$	

Solution. The premises are an implication and the negation of its conclusion, which invites MT: it gives $\neg(P \vee Q)$. The goal is a conjunction, so we need $\neg P$ and $\neg Q$, each a negation, each by a $\neg$ I box. In the box of P , the clash is manufactured: $\vee$ I gives $P \vee Q$, which clashes with line 3. The box of Q is the same.

1		$(P \vee Q) \rightarrow R$	
2		$\neg R$	
3		$\neg(P \vee Q)$	MT 1, 2
4		P	asm, for $\neg$ I
5		$P \vee Q$	$\vee$ I 4
6		$\perp$	$\neg$ E 5, 3
7		$\neg P$	$\neg$ I 4–6
8		Q	asm, for $\neg$ I
9		$P \vee Q$	$\vee$ I 8
10		$\perp$	$\neg$ E 9, 3
11		$\neg Q$	$\neg$ I 8–10
12		$\neg P \wedge \neg Q$	$\wedge$ I 7, 11

Line 3 is MT with φ replaced by $P \vee Q$ and ψ by R .

Exercise. B4: Dilemmas as derived rules, used later

- Section 1.6 derived the constructive dilemma, Example (Constructive dilemma). Use it as a derived rule, tagged CD, together with Example (First derivations with “or”), to derive $(P \rightarrow R) \wedge (Q \rightarrow R)$, $P \vee Q \vdash R$ in four lines.
- Derive the destructive dilemma $(P \rightarrow R) \wedge (Q \rightarrow S)$, $\neg R \vee \neg S \vdash \neg P \vee \neg Q$, using MT.
- Derive $\neg(P \wedge Q) \vdash P \rightarrow \neg Q$: “ P rules out Q ”, the form in which the traditional *modus ponendo tollens* is used. Then break “from $\neg(P \wedge Q)$ and $\neg P$, conclude Q ”.

- (d) Let n be an integer. Use (b) to show: if n is odd or n is not a multiple of 3, then n is not a multiple of 4 or not a multiple of 9. Take as premises that a multiple of 4 is even and a multiple of 9 is a multiple of 3, and read “odd” as “not even”.

Solution.

- (a) Line 3 is Example (Constructive dilemma), $(P \rightarrow R) \wedge (Q \rightarrow R)$, $P \vee Q \vdash R \vee R$, with S replaced by R . Line 4 is the second sequent of Example (First derivations with “or”), $P \vee P \vdash P$, with P replaced by R .

1		$(P \rightarrow R) \wedge (Q \rightarrow R)$	
2		$P \vee Q$	
3		$R \vee R$	CD 1, 2
4		R	or merges 3

- (b) Split the premise $\neg R \vee \neg S$; in each case MT refutes one hypothesis, and $\vee I$ builds the goal.

1		$(P \rightarrow R) \wedge (Q \rightarrow S)$	
2		$\neg R \vee \neg S$	
3		$P \rightarrow R$	$\wedge E$ 1
4		$Q \rightarrow S$	$\wedge E$ 1
5		$\neg R$	asm, for $\vee E$
6		$\neg P$	MT 3, 5
7		$\neg P \vee \neg Q$	$\vee I$ 6
8		$\neg S$	asm, for $\vee E$
9		$\neg Q$	MT 4, 8
10		$\neg P \vee \neg Q$	$\vee I$ 9
11		$\neg P \vee \neg Q$	$\vee E$ 2, 5–7, 8–10

- (c) The goal is an implication, so open a box on P ; its goal $\neg Q$ is a negation, so open a $\neg I$ box on Q inside it.

1		$\neg(P \wedge Q)$	
2		P	asm, for $\rightarrow I$
3		Q	asm, for $\neg I$
4		$P \wedge Q$	$\wedge I$ 2, 3
5		$\perp$	$\neg E$ 4, 1
6		$\neg Q$	$\neg I$ 3–5
7		$P \rightarrow \neg Q$	$\rightarrow I$ 2–6

The look-alike breaks with P : “ $x > 5$ ” and Q : “ $x > 3$ ”, at $x = 0$: $\neg(P \wedge Q)$ and $\neg P$ are true and Q is false, so the counterexample set $\neg(P \wedge Q)$, $\neg P$, $\neg Q$ is true. *Modus ponendo tollens* uses a negated conjunction and **affirms** one conjunct; DS uses

a disjunction and **refutes** one disjunct; mixing the two is the error of the look-alike.

- (d) Write F : “ n is a multiple of 4”, E : “ n is even”, N : “ n is a multiple of 9”, T : “ n is a multiple of 3”. The premises are $(F \rightarrow E) \wedge (N \rightarrow T)$ (since $4k = 2(2k)$ and $9k = 3(3k)$), and the hypothesis is $\neg E \vee \neg T$. Open a box on the hypothesis; inside it, (b) as a derived rule, with P, Q, R, S replaced by F, N, E, T , gives $\neg F \vee \neg N$; then $\rightarrow I$ closes the box on $(\neg E \vee \neg T) \rightarrow (\neg F \vee \neg N)$. For instance $n = 7$ is odd, and not a multiple of 4.

Marking scheme. (10 points)

- 2: (a), CD with the replacement $S := R$ named, then $P \vee P \vdash P$.
- 3: (b), MT in each case box, both boxes ending in $\neg P \vee \neg Q$.
- 3: (c), the nested $\neg I$ box inside the $\rightarrow I$ box (2), and a correct break of the look-alike (1).
- 2: (d), the letters, the premises, and the use of (b) inside a $\rightarrow I$ box.

Fatal error (0 for (b)): a case box citing a line of the other case box.

Exercise. B5: Derive or break

For each claim, derive it with the rules so far, including MT, CP, DS and the sequents derived in this book so far, or break it by statements about a real number x that make its counterexample set true at one value of x .

- (a) $P \vee Q, Q \vdash \neg P$.
- (b) $(P \vee R) \rightarrow \neg Q, Q \vdash \neg R$.
- (c) $\neg P \rightarrow Q \vdash \neg Q \rightarrow \neg P$.
- (d) $P \vee (Q \wedge R), \neg P \vdash R$.
- (e) $(P \wedge Q) \rightarrow R, \neg R, P \vdash \neg Q$.
- (f) $P \rightarrow (Q \vee R), \neg Q \vdash P \rightarrow R$.
- (g) $P \rightarrow (Q \vee R), \neg Q \vdash R$.
- (h) $(P \rightarrow Q) \wedge (R \rightarrow S), \neg Q \vee \neg S \vdash \neg P \wedge \neg R$.

Solution.

- (a) Break. Take P : “ $x > 0$ ” and Q : “ $x > 1$ ”. At $x = 2$, $P \vee Q$ and Q are true and P is true, so the counterexample set (Definition 1.1.3) $P \vee Q, Q, \neg \neg P$ is true. This is affirming a disjunct (Section 1.6).
- (b) Derive. The goal is a negation: open a box on R , and manufacture the premise’s hypothesis by $\vee I$.

1		$(P \vee R) \rightarrow \neg Q$	
2		Q	
3			
4			
5			
6			
7			

(c) Break. Take P : “ $x > 0$ ” and Q : “ $x > 5$ ”. At $x = 1$, $\neg P \rightarrow Q$ is true (its hypothesis fails), $\neg Q$ is true and $\neg P$ is false, so the counterexample set $\neg P \rightarrow Q$, $\neg(\neg Q \rightarrow \neg P)$ is true. (CP on $\neg P \rightarrow Q$ gives $\neg Q \rightarrow \neg\neg P$, not this.)

(d) Derive.

1		$P \vee (Q \wedge R)$	
2		$\neg P$	
3			
4			

(e) Derive. MT refutes the conjunction; then a $\neg I$ box on Q rebuilds it from the premise P .

1		$(P \wedge Q) \rightarrow R$	
2		$\neg R$	
3		P	
4			
5			
6			
7			
8			

(f) Derive.

1		$P \rightarrow (Q \vee R)$	
2		$\neg Q$	
3			
4			
5			
6			

(g) Break. Take P : “ $x > 5$ ”, Q : “ $x > 3$ ”, R : “ $x > 4$ ”. The premise $P \rightarrow (Q \vee R)$ is true for every x . At $x = 0$, $\neg Q$ is true and R is false, so the counterexample set $P \rightarrow (Q \vee R)$, $\neg Q$, $\neg R$ is true.

(h) Break. Take P : “ $x > 5$ ”, Q : “ $x > 9$ ”, R : “ $x > 0$ ”, S : “ $x > -1$ ”. At $x = 1$, $P \rightarrow Q$ is

true (its hypothesis fails) and $R \rightarrow S$ is true (for every x), $\neg Q \vee \neg S$ is true since $\neg Q$ is, and $\neg P \wedge \neg R$ is false, since R is true. So the counterexample set $(P \rightarrow Q) \wedge (R \rightarrow S)$, $\neg Q \vee \neg S$, $\neg(\neg P \wedge \neg R)$ is true.

- (i) and (c) are the look-alikes of DS and of CP; (g) drops the hypothesis that (f) keeps in its box; (h) is the destructive dilemma of Exercise B4 (b) with the $\vee$ of its conclusion made $\wedge$.

Marking scheme. (16 points) For each claim: 1 for the verdict; 1 for a derivation every line of which checks, or for a choice of statements and one value of x at which **every** member of the counterexample set is true. Fatal errors (0 for the claim): a “break” at which a premise fails; RAA or $\neg\neg$ E in a derivation.

2.3.10.3 C. Going deeper

Exercise. C1: Two premises that cannot both fail, used later

- (a) Show that $P \rightarrow Q$, $\neg P \rightarrow R$, $\neg Q$, $\neg R \vdash \perp$, using MT twice.
 (b) Hence show that $P \rightarrow Q$, $\neg P \rightarrow R \vdash \neg(\neg Q \wedge \neg R)$ with the rules so far.
 (c) In words, the conclusion of (b) says that Q and R do not both fail. Explain why a derivation with the rules so far naturally ends at $\neg(\neg Q \wedge \neg R)$ rather than at $Q \vee R$.

Solution.

- (a) The first MT has $\varphi = P$, $\psi = Q$. The second has $\varphi = \neg P$, $\psi = R$, so it gives the negation of $\neg P$, which is $\neg\neg P$. Lines 5 and 6 then clash.

1	$P \rightarrow Q$	
2	$\neg P \rightarrow R$	
3	$\neg Q$	
4	$\neg R$	
5	$\neg P$	MT 1, 3
6	$\neg\neg P$	MT 2, 4
7	$\perp$	$\neg$ E 5, 6

Line 7 cites $\neg P$ and then $\neg\neg P$: the unnegated line first, with φ of $\neg$ E replaced by $\neg P$.

- (b) The goal is a negation, so open a box on $\neg Q \wedge \neg R$ and aim at $\perp$. Inside, $\wedge$ E supplies the two negated premises of (a), and the rest is (a).

1	$P \rightarrow Q$	
2	$\neg P \rightarrow R$	
3	$\neg Q \wedge \neg R$	asm, for $\neg I$
4	$\neg Q$	$\wedge E$ 3
5	$\neg R$	$\wedge E$ 3
6	$\neg P$	MT 1, 4
7	$\neg \neg P$	MT 2, 5
8	$\perp$	$\neg E$ 6, 7
9	$\neg(\neg Q \wedge \neg R)$	$\neg I$ 3–8

- (c) To reach $Q \vee R$ by $\vee I$ we would need Q or R on its own. The premises give Q once P is known and R once $\neg P$ is known, and nothing available says which of P , $\neg P$ holds. What the rules so far can do is refute the opposite, $\neg Q \wedge \neg R$, by a $\neg I$ box, and that gives the negation in (b). The step from (b) to $Q \vee R$ uses the rule of Section 2.5.

Exercise. C2: A circular derivation

A student offers this derivation of $P \rightarrow Q \vdash \neg Q \rightarrow \neg P$.

1	$P \rightarrow Q$	
2	$\neg Q$	asm, for $\rightarrow I$
3	$\neg Q \rightarrow \neg P$	CP 1
4	$\neg P$	$\rightarrow E$ 3, 2
5	$\neg Q \rightarrow \neg P$	$\rightarrow I$ 2–4

- (a) Every line is an instance of the rule it names. What is wrong?
 (b) Give a correct derivation. May lines 3 and 4 be replaced by the one line “ $\neg P$, MT 1, 2”?

Solution.

- (a) Line 3 uses CP, the derived rule whose sequent, $P \rightarrow Q \vdash \neg Q \rightarrow \neg P$, is the very one being derived. [Definition 2.3.1](#) allows a sequent to be used only when it has **already been derived**; here it has not, so line 3 has no justification. (The whole derivation is also pointless: line 3 alone is already the goal.)
 (b) The derivation of [Proposition 2.3.2](#), from the primitive rules:

1		$P \rightarrow Q$	
2			asm, for $\rightarrow$ I
3			
4			
5			
6			
7			

Yes: lines 3–4 become the one line “ $\neg P$, MT 1, 2” inside the box of $\neg Q$, and line 5 becomes $\neg Q \rightarrow \neg P$, $\rightarrow$ I 2–3. This is legitimate, because [Proposition 2.3.1](#) was derived from the primitive rules, without CP. What matters is that the chain of derived rules ends in primitive rules, without a loop.

Exercise. C3: Exit check: labeling a proof

Here is a proof that for an integer n , if n^2 is odd, then n is odd.

Suppose n^2 is odd. If n were even, $n = 2k$, then $n^2 = 2(2k^2)$ would be even; so, by contraposition, since n^2 is not even (it is odd, and no integer is both), n is not even. As every integer is even or odd, n is odd.

Label each sentence, or part of a sentence, with the rule or rules it uses, primitive or derived. Take as premises the facts (E1) and (E2) of Section 2.1 and the school computation “if n is even, then n^2 is even”.

Solution. Write E : “ n is even”, O : “ n is odd”, S : “ n^2 is even”, T : “ n^2 is odd”.

- “Suppose n^2 is odd”: the assumption T of the box for $\rightarrow$ I, whose goal is O .
- “If n were even, $n = 2k$, then $n^2 = 2(2k^2)$ would be even”: the implication $E \rightarrow S$, a premise (the school computation). Reading the sentence as a $\rightarrow$ I box that proves $E \rightarrow S$, assuming E and computing, is equally correct.
- “ n^2 is not even (it is odd, and no integer is both)”: $\neg S$, by $\neg$ I: a box on S builds $S \wedge T$ by $\wedge$ I and clashes with (E2), $\neg(S \wedge T)$, by $\neg$ E.
- “by contraposition ... n is not even”: CP on $E \rightarrow S$ gives $\neg S \rightarrow \neg E$, and $\rightarrow$ E with $\neg S$ gives $\neg E$. (One MT line does both.)
- “As every integer is even or odd, n is odd”: DS on (E1), $E \vee O$, with the left side E refuted, gives O .
- The frame as a whole: $\rightarrow$ I, closing the box of T on O , gives $T \rightarrow O$.

As a derivation:

1	$E \vee O$	
2	$E \rightarrow S$	
3	$\neg(S \wedge T)$	
4	T	asm, for $\rightarrow$ I
5	S	asm, for $\neg$ I
6	$S \wedge T$	$\wedge$ I 5, 4
7	$\perp$	$\neg$ E 6, 3
8	$\neg S$	$\neg$ I 5–7
9	$\neg S \rightarrow \neg E$	CP 2
10	$\neg E$	$\rightarrow$ E 9, 8
11	O	DS 1, 10
12	$T \rightarrow O$	$\rightarrow$ I 4–11

The computation is right: $(2k)^2 = 4k^2 = 2(2k^2)$, and $2k^2$ is an integer.

Marking scheme. (10 points)

- 2: identifies the frame as $\rightarrow$ I, with the box opened on the hypothesis “ n^2 is odd”.
- 2: identifies “ n^2 is not even” as $\neg$ I, naming the clash (with “no integer is both”, by $\neg$ E).
- 3: identifies CP (then $\rightarrow$ E), or MT, applied to “if n is even, then n^2 is even”, with that antecedent and consequent. Reading the “if n were even” sentence as a premise or as a $\rightarrow$ I box that proves the implication earns these points equally.
- 2: identifies DS on “every integer is even or odd”, naming “even” as the refuted side.
- 1: names the closing $\rightarrow$ I.

Fatal errors (0 for the step): naming anything but $\neg$ I for the “not even” step (it concludes a negation from a box on the unnegated statement); applying CP to the converse, “if n^2 is even, then n is even”.