

5.6 Using “There Exists”: Name a Witness

Section 5.5 gave the rule that proves an existential statement: exhibit a witness, and forget it. This section gives the rule that **uses** one, $\exists E$. It is the last of the four quantifier rules, and the subtlest, because an existential says that a witness exists without saying which one it is. The rule handles this with a box and a fresh name, as $\forall I$ did, but the name now stands for an object that is **not** arbitrary, and the side condition keeps it from being treated as if it were. With the rule in hand, the section moves an $\exists$ past a $\forall$, and shows exactly where the reverse move breaks down.

5.6.1 Using a witness whose identity is unknown

Chapter 2 proved that if n^2 is even then n is even (Theorem 2.1.3). One of the facts it rested on, (E3), says that the square of an odd integer is odd, and it was shown by taking “an integer k with $n = 2k + 1$ ” and computing with it. Chapter 2 noted that naming the k of (E3) lay outside its derivation: it is a quantifier step, whose rule had to wait. Here is the simplest proof with the same step.

If n is even, then $n + 2$ is even. Since n is even, choose an integer k with $n = 2k$.
Then $n + 2 = 2k + 2 = 2(k + 1)$, so $n + 2$ is even.

The hypothesis is $\exists k (n = 2 \cdot k)$. The proof does not know which integer k is; it does not need to. It gives the unknown witness a name, uses the one fact it has about it, $n = 2k$, and reaches a conclusion, “ $n + 2$ is even”, in which the name no longer appears. The witness $k + 1$ of the last step is forgotten by $\exists I$, as in Section 5.5.

Why is this correct? Two tempting shortcuts show what the proof is careful **not** to do.

- It does not name the witness by a term that already means something. From “some integer is even” we may not conclude “3 is even”: the existential does not say that the witness is 3, and, as the warning “ $\exists I$ runs one way only” of Section 5.5 noted, it cannot be read back as a statement about a named object.
- It does not let the conclusion mention the name. If it did, the conclusion would be a statement about k , and outside the argument k refers to nothing; the existential promised only that **some** k works.

So the name must be new, the argument may use only what the existential says about it, and the conclusion must not mention it. Then the argument works for the witness, whichever integer it is, because it never used anything else about it.

5.6.2 The rule of existential elimination

To use “there exists”, give the witness a new name, assume only what the existential says about it, and conclude something that does not mention it.

Definition 5.6.1. Rules for the Existential Quantifier

h	$\exists x \varphi$		
i	x_0	$\varphi[x_0/x]$	asm, for $\exists E$
		$\vdots$	
j		χ	
k	χ		$\exists E \ h, i-j$

i	$\varphi[t/x]$	
k	$\exists x \varphi$	$\exists I \ i$

The rule on the left is $\exists E$ (**existential elimination**). It cites a line h holding $\exists x \varphi$ and a **flagged box** with the name x_0 , a variable, whose first line is the assumption $\varphi[x_0/x]$ and whose last line j , a line of that box itself, is χ ; line h and the box must be available at line k (Definition 1.4.2, with the flagged boxes of Section 5.4). The new line k repeats χ . Side condition, at line k : the name x_0 does **not appear**

- in χ ,
- in $\exists x \varphi$,
- in any premise, or
- in any assumption of a box **still open at line k** .

The rule on the right is $\exists I$, recalled from Definition 5.5.1: t is any term free for x in φ .

The box of $\exists E$ is the flagged box of Section 5.4 with one difference: it **opens with an assumption**, $\varphi[x_0/x]$, “ x_0 is a witness”. The flagged box of $\forall I$ had no assumption, because “let x_0 be arbitrary” assumes nothing about x_0 . The citation “ $\exists E \ h, i-j$ ” names the line of the existential and the box, as $\forall E$ names its disjunction and its boxes. “Appear” is the word of Section 5.2: written anywhere in the formula, after a quantifier symbol included. In a finished derivation the box’s assumption is printed “asm, for $\exists E$ ”; read it as “choose x_0 with ...”.

In practice, two habits make every clause of the side condition hold: name the witness with a brand-new letter, written nowhere in the derivation so far, and make sure the box’s last line does not mention it. Clauses 3–5 below, the side condition, are the official test, the one a checker runs.

This rule has conditions that matter; read each one.

1. **The assumption.** The box assumes $\varphi[x_0/x]$: the formula of the existential, with the new name in place of x . This is “choose x_0 with φ ”. It is the **only** thing the box knows about x_0 .
2. **The last line.** The box ends with χ , a line of the box itself, not of a box inside it, as for $\forall E$ and $\forall I$. It is “whatever the witness is, χ follows”. The new line k then asserts χ outside the box, where x_0 is no longer assumed to be anything.
3. **x_0 does not appear in χ .** The box shows that χ follows from “ x_0 is a witness”; if χ mentioned x_0 , line k would make a claim about a name that, outside the box, is tied to nothing. The subsection “Three ways to break the rule” below shows the damage.
4. **x_0 does not appear in a premise or in an assumption of an open box.** The name must be new to everything we know at line k . If a premise or an open assumption already said something about x_0 , the assumption $\varphi[x_0/x]$ would add to it a claim that x_0 **is** the witness, which the existential never made.
5. **x_0 does not appear in $\exists x \varphi$.** The existential must not itself mention the name chosen for its witness. This clause also makes x_0 free for x in φ (Section 5.2: a variable that does not appear in φ is free for every variable there), so the assumption $\varphi[x_0/x]$ says of x_0 exactly what φ says of x .
6. **“Still open at line k ”.** The box’s own assumption $\varphi[x_0/x]$ is closed at line k , so it is not

among the assumptions checked. This matters: read inside the box, “an open assumption” would include $\varphi[x_0/x]$, which contains x_0 whenever x is free in φ , and the rule could then never be applied in the cases that matter.

5.6.2.1 A first witness: $n + 2$ is even

Here is the proof above as a derivation, over $\mathbb{Z}$, with “ n is even” written $\exists k (n = 2 \cdot k)$ and the computation as one line justified “arith” (Section 5.3). The premise is an existential, so its box opens first, aimed at the goal (left); the goal is postponed until a line shows its witness (right).

1		$\exists k (n = 2 \cdot k)$	
2	k_0	$n = 2 \cdot k_0$	asm, for $\exists E$
		$\vdots$	
4		$\exists k (n + 2 = 2 \cdot k)$	?
5		$\exists k (n + 2 = 2 \cdot k)$	?
1		$\exists k (n = 2 \cdot k)$	
2	k_0	$n = 2 \cdot k_0$	asm, for $\exists E$
3		$n + 2 = 2 \cdot (k_0 + 1)$	arith 2
4		$\exists k (n + 2 = 2 \cdot k)$	?
5		$\exists k (n + 2 = 2 \cdot k)$	?
1		$\exists k (n = 2 \cdot k)$	
2	k_0	$n = 2 \cdot k_0$	asm, for $\exists E$
3		$n + 2 = 2 \cdot (k_0 + 1)$	arith 2
4		$\exists k (n + 2 = 2 \cdot k)$	$\exists I$ 3
5		$\exists k (n + 2 = 2 \cdot k)$	$\exists E$ 1, 2–4

At line 5, k_0 is not in line 4, not in the existential of line 1, which is also the only premise, and no box is open. The derivation and the proof match sentence for sentence:

Line	Sentence
1	“Since n is even, ...”
box $k_0, 2$	“... choose an integer k with $n = 2k$.”
3	“Then $n + 2 = 2k + 2 = 2(k + 1)$, ...” (arith)
4	“... so $n + 2$ is even.” ($\exists I$, the witness $k + 1$)
5	(unwritten: the conclusion does not mention k , so the box closes)

Quick check. Could line 5 have been $n + 2 = 2 \cdot (k_0 + 1)$, closing the box one line earlier?

Solution. No: that line mentions the witness k_0 , which breaks clause 3. Outside the box k_0 names nothing; $\exists I$ must forget it first, as line 4 does.

5.6.2.2 One box instead of many cases

The long “or” of Section 5.1 shows why the rule has this shape. Over a domain whose elements are named m and n , $\exists x P(x)$ says $P(m) \vee P(n)$, and $\forall E$ (Definition 1.6.1) would use it by proving the goal twice, once in each case. The cases look alike, so they can be done once, with a name that could be either.

1	$P(m) \vee P(n)$	
2	$\forall x (P(x) \rightarrow Q(f(x)))$	
3	$P(m)$	asm, for $\forall E$
4	$P(m) \rightarrow Q(f(m))$	$\forall E$ 2
5	$Q(f(m))$	$\rightarrow E$ 4, 3
6	$\exists y Q(y)$	$\exists I$ 5
7	$P(n)$	asm, for $\forall E$
8	$P(n) \rightarrow Q(f(n))$	$\forall E$ 2
9	$Q(f(n))$	$\rightarrow E$ 8, 7
10	$\exists y Q(y)$	$\exists I$ 9
11	$\exists y Q(y)$	$\forall E$ 1, 3–6, 7–10

1	$\exists x P(x)$	
2	$\forall x (P(x) \rightarrow Q(f(x)))$	
3	$x_0 \mid P(x_0)$	asm, for $\exists E$
4	$P(x_0) \rightarrow Q(f(x_0))$	$\forall E$ 2
5	$Q(f(x_0))$	$\rightarrow E$ 4, 3
6	$\exists y Q(y)$	$\exists I$ 5
7	$\exists y Q(y)$	$\exists E$ 1, 3–6

On the left, Section 1.6’s rule over the two named elements; on the right, the same argument by $\exists E$. Each case box on the left is the box on the right with m or n in place of x_0 . Because x_0 is fresh, one box serves for every element, named or not, and for domains that cannot be listed.

5.6.3 Using an existential: open the box early

When a resource is $\exists x \varphi$, the premise-directed step of the search method is to open its $\exists E$ box at once, with a fresh name x_0 , and to make the box’s last line the **current goal**. Inside the box, the assumption $\varphi[x_0/x]$ is a new resource, and the name x_0 is a new term for later steps to use.

Name the witness early: open the $\exists E$ box as soon as the existential is available, and aim it at the current goal.

Why early? Opening early keeps every resource, since every line available before the box is available inside it; and a box aimed at the current goal can always be closed once the goal is reached, since its name was chosen fresh. What the early box gives is the witness’s name, often exactly the term a postponed $\exists$ goal is waiting for.

🕒 **Second reading** · *Why opening early is safe*

And a box aimed at the current goal χ can always be closed once χ is reached: x_0 is chosen, when the box opens, to appear in no premise, in no open assumption, not in $\exists x \varphi$ and not in the current goal χ . The assumptions still open at the line that closes the box are the ones that were open when it opened, so every clause of the side condition holds there. (One caution: a $\forall I$ inside the box needs a flag that does not appear in the new assumption; a flag that is fresh at that point has this property.)

The first result is the derivation that this step writes almost by itself.

Proposition 5.6.1. Some Distributes Over And, One Way

$\exists x (P(x) \wedge Q(x)) \vdash \exists x P(x) \wedge \exists x Q(x)$.

Idea. The premise is an existential, so open its box first, with a fresh x_0 , and aim it at the goal. Inside, the assumption $P(x_0) \wedge Q(x_0)$ splits by $\wedge E$, and each half is an instance of one conjunct of the goal, with the witness x_0 . The goal does not mention x_0 , so the box closes.

1		$\exists x (P(x) \wedge Q(x))$	
2	x_0	$P(x_0) \wedge Q(x_0)$	asm, for $\exists E$
		$\vdots$	
7		$\exists x P(x) \wedge \exists x Q(x)$	?
8		$\exists x P(x) \wedge \exists x Q(x)$	?
1		$\exists x (P(x) \wedge Q(x))$	
2	x_0	$P(x_0) \wedge Q(x_0)$	asm, for $\exists E$
3		$P(x_0)$	$\wedge E$ 2
4		$\exists x P(x)$	?
5		$Q(x_0)$	$\wedge E$ 2
6		$\exists x Q(x)$	?
7		$\exists x P(x) \wedge \exists x Q(x)$	$\wedge I$ 4, 6
8		$\exists x P(x) \wedge \exists x Q(x)$	?

Proof. The following is a derivation.

1		$\exists x (P(x) \wedge Q(x))$	
2		x_0 $P(x_0) \wedge Q(x_0)$	asm, for $\exists E$
3		$P(x_0)$	$\wedge E$ 2
4		$\exists x P(x)$	$\exists I$ 3
5		$Q(x_0)$	$\wedge E$ 2
6		$\exists x Q(x)$	$\exists I$ 5
7		$\exists x P(x) \wedge \exists x Q(x)$	$\wedge I$ 4, 6
8		$\exists x P(x) \wedge \exists x Q(x)$	$\exists E$ 1, 2–7

Line 2 is the assumption $\varphi[x_0/x]$ for $\varphi = P(x) \wedge Q(x)$. Lines 4 and 6 are $\exists I$ with the witness x_0 . At line 8, x_0 does not appear in line 7, in line 1 (which is also the only premise), or in any assumption of an open box (none is open). So line 8 is a correct $\exists E$, and the derivation has 8 lines. ■

Notice where the witness went. It was used twice inside the box, as the witness of two different existentials, and then forgotten twice. The conclusion records that something has P and something has Q , and no longer that it is the same thing.

Quick check. Is $\exists x P(x) \wedge \exists x Q(x) \vdash \exists x (P(x) \wedge Q(x))$? Run the search, and say where it stalls.

Solution. The premise splits by $\wedge E$ into $\exists x P(x)$ and $\exists x Q(x)$. Opening both boxes early gives the assumptions $P(x_0)$ and, for the second box, a **different** name, $Q(y_0)$: the second box is opened while the first is open, so x_0 appears in an open assumption and may not be reused. The postponed goal $\exists x (P(x) \wedge Q(x))$ needs one term t with $P(t) \wedge Q(t)$, and the resources speak of two names, with nothing to say that they are equal. The search stalls there. It must: over $\mathbb{Z}$, with P as “even” and Q as “odd”, the premise is true and the conclusion, “some integer is both even and odd”, is false. That is a counter-reading (Section 5.3).

5.6.4 Three ways to break the rule

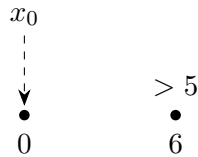
Each of clauses 3, 4 and 5 can be seen failing, and each failure leads from premises that are true, under the reading given, to a false line. Here is clause 3, beside a correct use of the same premise; the fold after it breaks clauses 4 and 5.

The conclusion clause (3). Over $\mathbb{N}$, “some number exceeds 5” is true. Let the $\exists E$ box end in the line $x_0 > 5$, which mentions its own witness:

1	$\exists x (x > 5)$			1	$\exists x (x > 5)$		
2	$x_0 \mid x_0 > 5$	asm, for $\exists E$		2	$x_0 \mid x_0 > 5$	asm, for $\exists E$	
3	$x_0 > 5$	$\exists E$ 1, 2–2		3	$x_0 + 1 > 6$	arith 2	
4	$x_0 \mid x_0 > 5$	R 3		4	$\exists x (x > 6)$	$\exists I$ 3	
5	$\forall x (x > 5)$	$\forall I$ 4–4		5	$\exists x (x > 6)$	$\exists E$ 1, 2–4	

Line 3 breaks clause 3. Every other line is legal: in particular line 5 is a correct $\forall I$, since x_0 appears in no premise and in no open assumption (there is none), and not in line 5. Over $\mathbb{N}$ the conclusion says that every number exceeds 5, which is false at 0. Once the name leaves its box, it can be generalized over as if it were arbitrary.

On the right, a correct use of the same premise: the box ends in $\exists x (x > 6)$, which forgets the witness before the box closes, and the conclusion is true over $\mathbb{N}$.



A small world in which the premise is true and the line that breaks clause 3 is false. The label “ > 5 ” is the one-place predicate $x > 5$ (5 is not a dot); the dashed arrow gives x_0 the value 0. The premise is true (at 6); line 3, $x_0 > 5$, is false; so is line 5 (at 0).

Quick check. In the clause-3 derivation, line 5 is a correct $\forall I$, yet it is false in the picture. Which line is to blame, and why does a correct step not save the derivation?

Solution. Line 3, which closes the $\exists E$ box with a line that mentions its witness. $\forall I$ is safe only when the last line of its box, here line 4, is true whatever x_0 names. Line 4 is copied from line 3, and both are false when x_0 names 0. So line 5 inherits the error from line 3; it is not a new one.

🕒 Second reading · Clauses 4 and 5, broken

The premise clause (4). Over $\mathbb{N}$, with P read as “even” and the variable x_0 read as 1, both premises below are true: some number is even, and 1 is not even.

1	$\exists x P(x)$		
2	$\neg P(x_0)$		
3	$x_0 \mid P(x_0)$	asm, for $\exists E$	
4	$\perp$	$\neg E$ 3, 2	
5	$\perp$	$\exists E$ 1, 3–4	

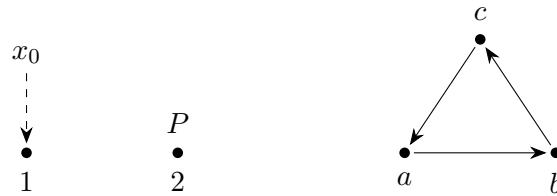
Line 5 breaks clause 4: x_0 appears in the premise on line 2. The box assumed that x_0 , which

the premise had already described as odd, is the even witness, and derived a contradiction from that assumption, not from the premises.

The existential clause (5). Over $\mathbb{Z}$, with $R(x, y)$ read as “ $x < y$ ”, the premise below says that every integer has a smaller one: true.

1	$\forall y \exists x R(x, y)$	
2	$\exists x R(x, x_0)$	$\forall E$ 1
3	x_0 $R(x_0, x_0)$	asm, for $\exists E$
4	$\exists z R(z, z)$	$\exists I$ 3
5	$\exists z R(z, z)$	$\exists E$ 2, 3–4

Line 2 is a legal $\forall E$ at the term x_0 . Line 5 breaks clause 5: the existential on line 2 is $\exists x \varphi$ with $\varphi = R(x, x_0)$, and x_0 appears in it. The assumption $\varphi[x_0/x]$ on line 3 is $R(x_0, x_0)$: the box has assumed that the witness smaller than x_0 is x_0 itself. The conclusion says that some integer is less than itself, which is false. The other clauses hold at line 5: x_0 is not in $\exists z R(z, z)$, not in the premise, and no box is open.



Two small worlds, one per clause: in each, the premises are true and the line that breaks the clause is false. Left, clause 4: the dots 1 and 2, with P (“even”) true at 2 only, and x_0 naming 1; both premises, $\exists x P(x)$ and $\neg P(x_0)$, are true, and the line $\perp$ is false, as always. Right, clause 5: three dots, an arrow from u to v meaning $R(u, v)$; the premise $\forall y \exists x R(x, y)$ is true, since every dot has an arrow into it, and the line $\exists z R(z, z)$ is false, since there is no loop.

A fourth illegal pattern, a second witness given a name that an open assumption already uses, is the error of the warning “Two witnesses, one name” below.

Warning. The witness is not arbitrary. The flagged boxes of $\forall I$ and $\exists E$ look alike: both introduce a fresh name. Their names mean opposite things. In a $\forall I$ box, x_0 is **any** object, and what is proved about it holds for all. In an $\exists E$ box, x_0 is **one particular** object, the witness, about which we know $\varphi[x_0/x]$ and nothing else; what is proved about it holds for it alone. From “some integer is even” nothing follows about every integer, and the rules agree:

1	$\exists x P(x)$	
2	x_0 $P(x_0)$	asm, for $\exists E$
3	x_0 $P(x_0)$	R 2
4	$\forall x P(x)$	$\forall I$ 3–3
5	$\forall x P(x)$	$\exists E$ 1, 2–4

Line 4 is blocked: x_0 appears in the assumption $P(x_0)$ of the $\exists E$ box, which is still open at line 4. That clause of $\forall I$ is what keeps a witness from being generalized over inside its box; clause 3 of $\exists E$, that x_0 not appear in χ , keeps it from leaving the box (the derivation for clause 3 above).

Here are three more derivations, each with an Idea saying why each rule was chosen: two for part (a), one for each direction, and one for part (b).

Example. Derivations with existential elimination

Show that:

- (a) $\exists x (P(x) \vee Q(x)) \dashv\vdash \exists x P(x) \vee \exists x Q(x)$;
- (b) $\exists x P(x), \forall x (P(x) \rightarrow \neg Q(x)) \vdash \neg \forall x Q(x)$.

Solution.

- (a) ($\vdash$) *Idea.* The premise is an existential: open its box first. Inside, the assumption $P(x_0) \vee Q(x_0)$ is a disjunction, and the premise-directed step for $\vee$ (Section 1.6) opens two cases, each ending in the current goal. In each case one side of the goal has an instance with the witness x_0 , so $\exists I$ and $\forall I$ finish it.

1		$\exists x (P(x) \vee Q(x))$	
2		x_0 $P(x_0) \vee Q(x_0)$	asm, for $\exists E$
		$\vdots$	
9		$\exists x P(x) \vee \exists x Q(x)$	?
10		$\exists x P(x) \vee \exists x Q(x)$	?
1		$\exists x (P(x) \vee Q(x))$	
2		x_0 $P(x_0) \vee Q(x_0)$	asm, for $\exists E$
3		$P(x_0)$	asm, for $\vee E$
		$\vdots$	
5		$\exists x P(x) \vee \exists x Q(x)$	?
6		$Q(x_0)$	asm, for $\vee E$
		$\vdots$	
8		$\exists x P(x) \vee \exists x Q(x)$	?
9		$\exists x P(x) \vee \exists x Q(x)$	$\vee E$ 2, 3–5, 6–8
10		$\exists x P(x) \vee \exists x Q(x)$	?

1	$\exists x (P(x) \vee Q(x))$	
2	$x_0 \mid P(x_0) \vee Q(x_0)$	asm, for $\exists E$
3	$\mid P(x_0)$	asm, for $\vee E$
4	$\mid \exists x P(x)$	$\exists I$ 3
5	$\mid \exists x P(x) \vee \exists x Q(x)$	$\vee I$ 4
6	$\mid Q(x_0)$	asm, for $\vee E$
7	$\mid \exists x Q(x)$	$\exists I$ 6
8	$\mid \exists x P(x) \vee \exists x Q(x)$	$\vee I$ 7
9	$\exists x P(x) \vee \exists x Q(x)$	$\vee E$ 2, 3–5, 6–8
10	$\exists x P(x) \vee \exists x Q(x)$	$\exists E$ 1, 2–9

Line 9 is $\vee E$ (Definition 1.6.1), and it is the last line of the $\exists E$ box itself. At line 10, x_0 is in neither line 9 nor line 1, and no box is open.

($\neg$) *Idea.* Now the premise is a disjunction: $\vee E$ first, with two cases, each ending in the goal. In each case the resource is an existential, so its box opens at once, and inside it $\vee I$ and $\exists I$ build the goal.

1	$\exists x P(x) \vee \exists x Q(x)$	
2	$\mid \exists x P(x)$	asm, for $\vee E$
	$\mid \vdots$	
6	$\mid \exists x (P(x) \vee Q(x))$	?
7	$\mid \exists x Q(x)$	asm, for $\vee E$
	$\mid \vdots$	
11	$\mid \exists x (P(x) \vee Q(x))$	?
12	$\exists x (P(x) \vee Q(x))$	$\vee E$ 1, 2–6, 7–11

1	$\exists x P(x) \vee \exists x Q(x)$	
2	$\exists x P(x)$	asm, for $\vee E$
3	$x_0 \mid P(x_0)$	asm, for $\exists E$
	$\vdots$	
5	$\exists x (P(x) \vee Q(x))$	?
6	$\exists x (P(x) \vee Q(x))$	$\exists E$ 2, 3–5
7	$\exists x Q(x)$	asm, for $\vee E$
8	$x_0 \mid Q(x_0)$	asm, for $\exists E$
	$\vdots$	
10	$\exists x (P(x) \vee Q(x))$	?
11	$\exists x (P(x) \vee Q(x))$	$\exists E$ 7, 8–10
12	$\exists x (P(x) \vee Q(x))$	$\vee E$ 1, 2–6, 7–11
1	$\exists x P(x) \vee \exists x Q(x)$	
2	$\exists x P(x)$	asm, for $\vee E$
3	$x_0 \mid P(x_0)$	asm, for $\exists E$
4	$P(x_0) \vee Q(x_0)$	$\vee I$ 3
5	$\exists x (P(x) \vee Q(x))$	$\exists I$ 4
6	$\exists x (P(x) \vee Q(x))$	$\exists E$ 2, 3–5
7	$\exists x Q(x)$	asm, for $\vee E$
8	$x_0 \mid Q(x_0)$	asm, for $\exists E$
9	$P(x_0) \vee Q(x_0)$	$\vee I$ 8
10	$\exists x (P(x) \vee Q(x))$	$\exists I$ 9
11	$\exists x (P(x) \vee Q(x))$	$\exists E$ 7, 8–10
12	$\exists x (P(x) \vee Q(x))$	$\vee E$ 1, 2–6, 7–11

At line 6, the open assumption is line 2, which does not contain x_0 ; at line 11 it is line 7, which does not either. The name x_0 is used in both cases. That is allowed: when the second box opens, the first has closed, and the side condition looks only at the premises, the boxes still open, the existential and the conclusion. Lines 6 and 11 are lines of the two case boxes themselves, as $\vee E$ requires.

The two derivations mirror each other: $\exists E$ outside and $\vee E$ inside in one, the other way round in the other. Over a domain, both sides say that some element has P or Q . Contrast [Proposition 5.6.1](#), where only one direction holds: $\exists$ passes through $\vee$ in both directions and through $\wedge$ in one.

- (b) *Idea.* The goal is a negation, so the goal-directed step of Section 2.2 opens a $\neg I$ box on $\forall x Q(x)$ (Definition 2.2.1), with the goal $\perp$. Then the premise $\exists x P(x)$ opens its box, aimed at $\perp$. Inside, the witness x_0 is the term at which to instantiate both universal statements: the premise gives $\neg Q(x_0)$, and the assumption gives $Q(x_0)$, a clash.

1		$\exists x P(x)$	
2		$\forall x (P(x) \rightarrow \neg Q(x))$	
3		$\forall x Q(x)$	asm, for $\neg I$
		$\vdots$	
9		$\perp$	?
10		$\neg \forall x Q(x)$	$\neg I$ 3–9
1		$\exists x P(x)$	
2		$\forall x (P(x) \rightarrow \neg Q(x))$	
3		$\forall x Q(x)$	asm, for $\neg I$
4		x_0 $P(x_0)$	asm, for $\exists E$
		$\vdots$	
8		$\perp$	?
9		$\perp$	$\exists E$ 1, 4–8
10		$\neg \forall x Q(x)$	$\neg I$ 3–9
1		$\exists x P(x)$	
2		$\forall x (P(x) \rightarrow \neg Q(x))$	
3		$\forall x Q(x)$	asm, for $\neg I$
4		x_0 $P(x_0)$	asm, for $\exists E$
5		$P(x_0) \rightarrow \neg Q(x_0)$	$\forall E$ 2
6		$\neg Q(x_0)$	$\rightarrow E$ 5, 4
7		$Q(x_0)$	$\forall E$ 3
8		$\perp$	$\neg E$ 7, 6
9		$\perp$	$\exists E$ 1, 4–8
10		$\neg \forall x Q(x)$	$\neg I$ 3–9

At line 9, the box of line 3 is still open, so its assumption $\forall x Q(x)$ is checked: x_0 does not appear in it. Nor is x_0 in $\perp$, in line 1, or in line 2. Read over $\mathbb{Z}$ with P as “odd” and Q as “divisible by 4”: some integer is odd, no odd integer is divisible by 4, so not every integer is divisible by 4. The witness, whichever odd integer it is, is a counterexample to “every integer is divisible by 4”, and the derivation never needs to know which.

5.6.5 Moving one quantifier past another

Section 5.1 read $\exists y \forall x \varphi$ and $\forall x \exists y \varphi$ as games, and observed that the first gives the second: if one y works for every x , then for every x some y works, namely the same one. Here is that observation as a derivation, with the letters of a two-place predicate. It shows, written out in full, a pattern that later derivations of the chapter use again and again and that later exercises

leave more and more of to the reader.

Proposition 5.6.2. Some-All Gives All-Some

$$\exists x \forall y R(x, y) \vdash \forall y \exists x R(x, y).$$

Idea. Three moves, read off the goal and the premise.

① **Fix.** The goal is $\forall y$: open a flagged box with a fresh y_0 (Section 5.4); the new goal is $\exists x R(x, y_0)$.

② **Obtain.** That goal is an existential: postpone it. The premise is an existential: open its box early, with a fresh x_0 , assuming $\forall y R(x_0, y)$, and aim it at the current goal $\exists x R(x, y_0)$. Instantiate the assumption at the term the goal mentions, y_0 : this gives $R(x_0, y_0)$.

③ **Choose.** That line is an instance of the postponed goal, with the witness x_0 : $\exists I$.

In the Givens/Goal table:

Givens			Goal		
$\exists x \forall y R(x, y)$			$\forall y \exists x R(x, y)$		
+ the fresh name y_0 (fix: $\forall I$ opens a box)			$\exists x R(x, y_0)$: postponed		
+ the witness x_0 and $\forall y R(x_0, y)$ (obtain: $\exists E$ opens a box)			$\exists x R(x, y_0)$		
+ $R(x_0, y_0)$ ($\forall E$ at y_0)			$\exists x R(x, y_0) \checkmark$ by $\exists I$, the witness x_0 (choose)		

1	$\exists x \forall y R(x, y)$		2	$\exists x \forall y R(x, y)$		
	y_0	$\vdots$		y_0	x_0	$\forall y R(x_0, y)$ asm, for $\exists E$
5	$\exists x R(x, y_0)$	?	4	$\exists x R(x, y_0)$	?	
6	$\forall y \exists x R(x, y)$	?	5	$\exists x R(x, y_0)$		$\exists E$ 1, 2–4
			6	$\forall y \exists x R(x, y)$	?	

Before reading on: at the line that closes the $\exists E$ box, check each clause of its side condition. Where could x_0 still appear?

Proof. The following is a derivation.

1	$\exists x \forall y R(x, y)$			
2	y_0	x_0	$\forall y R(x_0, y)$	asm, for $\exists E$
3			$R(x_0, y_0)$	$\forall E$ 2
4			$\exists x R(x, y_0)$	$\exists I$ 3
5		$\exists x R(x, y_0)$		$\exists E$ 1, 2–4
6	$\forall y \exists x R(x, y)$			$\forall I$ 2–5

Line 2 is the assumption $\varphi[x_0/x]$ for $\varphi = \forall y R(x, y)$. Line 3 is $\forall E$ at y_0 . Line 4 is $\exists I$ with $\varphi = R(x, y_0)$ and the witness x_0 , which is free for x since $R(x, y_0)$ has no quantifier.

Line 5 closes the $\exists E$ box, whose last line, line 4, is a line of the box itself. Its side condition holds: x_0 does not appear in $\chi = \exists x R(x, y_0)$, nor in the existential $\exists x \forall y R(x, y)$ of line 1, which is also the only premise; and the one box still open at line 5, the flagged box of y_0 , has no assumption.

Line 6 closes the flagged box of y_0 by $\forall I$ (Definition 5.4.1). That box immediately contains the $\exists E$ box, so its range starts at line 2 (the convention of Section 5.4), and its last line, line 5, is a line of the box itself, the instance $(\exists x R(x, y))[y_0/y]$. The name y_0 appears neither in the premise nor in line 6, and at line 6 no box is open. This proves the proposition. ■

The two names played opposite parts. The name y_0 is arbitrary: nothing was assumed about it, and line 6 generalizes over it. The name x_0 is the witness: line 2 assumed everything the premise says about it, and line 5 forgets it. The witness x_0 works for y_0 because it works for every y , which line 2 says. This is the shape of a great many proofs in analysis, and it has a name.

Fix, obtain, choose: fix the arbitrary objects of the goal ($\forall I$); obtain witnesses from the hypotheses ($\forall E$ and $\exists E$); choose the goal's witness from what is now available ($\exists I$).

Nothing in the proof used that the formula is $R(x, y)$: the same six lines derive $\exists x \forall y \varphi \vdash \forall y \exists x \varphi$ for any formula φ , which is the derivation promised in Section 5.1; the fold checks the substitutions.

🔄 **Second reading** · *The swap for any formula*

For any formula φ and different variables x and y , with different names x_0 and y_0 , other than x and y , that do not appear in φ , the same six lines derive $\exists x \forall y \varphi \vdash \forall y \exists x \varphi$. Line 2 is $\forall y (\varphi[x_0/x])$. Line 3 is $(\varphi[x_0/x])[y_0/y]$, which equals $(\varphi[y_0/y])[x_0/x]$, since the two substitutions put fresh names in for two different variables and so do not interfere; so line 4 is $\exists I$ with the formula $\varphi[y_0/y]$ and the witness x_0 . The fresh names are free for their variables, since neither appears in φ , and the side conditions are checked as before. With the letters x and y exchanged, this is the derivation of $\exists y \forall x \varphi$ to $\forall x \exists y \varphi$ promised in Section 5.1.

🕒 **Second reading** · *Either nesting works*

Either nesting works. The derivation opened the flagged box of y_0 first and the $\exists E$ box inside it. The other order is just as good.

1		$\exists x \forall y R(x, y)$	
2	x_0	$\forall y R(x_0, y)$	asm, for $\exists E$
3		y_0 $R(x_0, y_0)$	$\forall E$ 2
4		$\exists x R(x, y_0)$	$\exists I$ 3
5		$\forall y \exists x R(x, y)$	$\forall I$ 3–4
6		$\forall y \exists x R(x, y)$	$\exists E$ 1, 2–5

At line 5, y_0 appears neither in the premise, nor in the open assumption $\forall y R(x_0, y)$ (its y is a bound variable, not y_0), nor in line 5. At line 6, x_0 is not in line 5, not in line 1, and no box is open. In this order the $\exists E$ box is aimed at the whole goal; in the first, at the goal left inside the flagged box. Both are the search method’s “open the box early”: early relative to the goal that the box must reach.

The converse search stalls at a side condition. Try $\forall y \exists x R(x, y) \vdash \exists x \forall y R(x, y)$. The goal is an existential: postpone it; it will need a witness x_0 and a line $\forall y R(x_0, y)$. The premise is a universal, and to get an existential out of it we must instantiate it at some term. The natural routes then meet a side condition. Here are two of them.

First route: obtain the witness, then try to generalize. Instantiate at a name y_0 , open the $\exists E$ box on the result, and try to prove $\forall y R(x_0, y)$ inside it by $\forall I$:

1		$\forall y \exists x R(x, y)$	
2		$\exists x R(x, y_0)$	$\forall E$ 1
3	x_0	$R(x_0, y_0)$	asm, for $\exists E$
4		y_0 $R(x_0, y_0)$	R 3
5		$\forall y R(x_0, y)$	$\forall I$ 4–4
6		$\exists x \forall y R(x, y)$	$\exists I$ 5
7		$\exists x \forall y R(x, y)$	$\exists E$ 2, 3–6

Line 5 is blocked: y_0 appears in the assumption $R(x_0, y_0)$ of the $\exists E$ box, which is still open. The witness x_0 was obtained **for** y_0 , and the assumption says so. Choosing a different flag, say z_0 , does not help: the goal inside its box would be $R(x_0, z_0)$, and nothing gives it.

Second route: fix first, obtain inside, and carry the witness out. Open the flagged box of y_0 first, obtain x_0 inside it, and try to close the $\exists E$ box with a line about x_0 , so that $\forall I$ can then generalize over y_0 :

1		$\forall y \exists x R(x, y)$	
2		y_0 $\exists x R(x, y_0)$	$\forall E$ 1
3		x_0 $R(x_0, y_0)$	asm, for $\exists E$
4		$R(x_0, y_0)$	$\exists E$ 2, 3–3
5		$\forall y R(x_0, y)$	$\forall I$ 2–4
6		$\exists x \forall y R(x, y)$	$\exists I$ 5

Line 4 is blocked: x_0 appears in $\chi = R(x_0, y_0)$. Lines 5 and 6 would be legal on their own; the derivation fails only because the witness escaped its box at line 4.

The two blocked lines are the two halves of one fact. The witness x_0 is obtained after y_0 is fixed, so it may depend on y_0 ; the conclusion asks for an x_0 chosen before any y , which may not. This is the dependence that Section 5.1 read off the order of the quantifiers, now visible as the order of the boxes. A stalled search is not a proof that no derivation exists. A counter-reading breaks the claim: two dots 0 and 1, with $R(x, y)$ read as “ x differs from y ”. Each dot has a dot that differs from it, so the premise is true; no dot differs from both dots, itself included, so the conclusion is false.

🕒 **Second reading** · *Renaming the bound variable of an existential*

Renaming the bound variable of an existential. Section 5.2 promised that a bound variable at the front of a formula may be renamed, and Section 5.4 derived the renaming for $\forall$ (the fold after Example (Flagged boxes at work)). Here is the derivation for $\exists$. Let φ be a formula and y, z variables, with z not appearing in φ . Then

$$\exists y \varphi \dashv\vdash \exists z \varphi[z/y].$$

Take a fresh name z_0 , a variable different from y and z that does not appear in φ , as in Section 5.4. Both directions use one fact about substitution: since z does not appear in φ , each free z of $\varphi[z/y]$ stands where φ had a free y , and nowhere else, so putting a term t in for those z ’s gives $\varphi[t/y]$; that is, $(\varphi[z/y])[t/z] = \varphi[t/y]$. (It is a structural induction of the kind in Section 5.2, one clause at a time.)

1		$\exists y \varphi$		1		$\exists z \varphi[z/y]$	
2		z_0 $\varphi[z_0/y]$	asm, for $\exists E$	2		z_0 $\varphi[z_0/y]$	asm, for $\exists E$
3		$\exists z \varphi[z/y]$	$\exists I$ 2	3		$\exists y \varphi$	$\exists I$ 2
4		$\exists z \varphi[z/y]$	$\exists E$ 1, 2–3	4		$\exists y \varphi$	$\exists E$ 1, 2–3

In the left derivation, line 3 is $\exists I$ with the formula $\varphi[z/y]$, the variable z and the witness z_0 : by the fact, $(\varphi[z/y])[z_0/z]$ is line 2. The witness is free for z , because the quantifiers of $\varphi[z/y]$ are those of φ , and none of them is on z_0 . In the right derivation, line 2 is the assumption of the box for the existential $\exists z \varphi[z/y]$, which is $(\varphi[z/y])[z_0/z]$, that is $\varphi[z_0/y]$ by the fact, and line 3 is $\exists I$ with φ, y and the witness z_0 , which is free for y since it does not appear in φ . In both, line 4 is a correct $\exists E$: z_0 does not appear in φ , so it is in neither line 1 nor line 3, and no box is open.

So $\exists y (y \neq x)$ and $\exists z (z \neq x)$ can each be derived from the other, as the recipe of Section 5.2

assumed.

5.6.6 Two witnesses

A proof often obtains several witnesses, one from each existential hypothesis. Each needs its own box and its own name.

Example. The sum of two even integers is even

Over $\mathbb{Z}$, with “ n is even” written $\exists k (n = 2 \cdot k)$, derive

$$\exists k (n = 2 \cdot k), \exists k (m = 2 \cdot k) \vdash \exists k (n + m = 2 \cdot k).$$

Solution. Idea. Both premises are existentials: open both boxes early, the second inside the first, with **different** names k_0 and l_0 . The goal is an existential: postpone it. Inside both boxes the resources are $n = 2 \cdot k_0$ and $m = 2 \cdot l_0$, and arithmetic gives $n + m = 2 \cdot (k_0 + l_0)$, which shows the witness: the compound term $k_0 + l_0$.

1		$\exists k (n = 2 \cdot k)$	
2		$\exists k (m = 2 \cdot k)$	
3		k_0 $n = 2 \cdot k_0$	asm, for $\exists E$
		$\vdots$	
7		$\exists k (n + m = 2 \cdot k)$	?
8		$\exists k (n + m = 2 \cdot k)$	?
1		$\exists k (n = 2 \cdot k)$	
2		$\exists k (m = 2 \cdot k)$	
3		k_0 $n = 2 \cdot k_0$	asm, for $\exists E$
4		l_0 $m = 2 \cdot l_0$	asm, for $\exists E$
		$\vdots$	
6		$\exists k (n + m = 2 \cdot k)$	?
7		$\exists k (n + m = 2 \cdot k)$	$\exists E$ 2, 4–6
8		$\exists k (n + m = 2 \cdot k)$	?

1		$\exists k (n = 2 \cdot k)$	
2		$\exists k (m = 2 \cdot k)$	
3		k_0 $n = 2 \cdot k_0$	asm, for $\exists E$
4		l_0 $m = 2 \cdot l_0$	asm, for $\exists E$
5		$n + m = 2 \cdot (k_0 + l_0)$	arith 3, 4
6		$\exists k (n + m = 2 \cdot k)$	$\exists I$ 5
7		$\exists k (n + m = 2 \cdot k)$	$\exists E$ 2, 4–6
8		$\exists k (n + m = 2 \cdot k)$	$\exists E$ 1, 3–7

Line 5 is one line of arithmetic: from $n = 2k_0$ and $m = 2l_0$, substituting and factoring gives $n + m = 2k_0 + 2l_0 = 2(k_0 + l_0)$. The substitutions are steps of the rule $=E$, which arrives only in Section 5.7, so here the whole calculation is one line justified “arith”, citing the two lines it uses. Line 6 is $\exists I$ with $\varphi = (n + m = 2 \cdot k)$ and the witness $k_0 + l_0$.

At line 7 the only box still open is the outer one, whose assumption is line 3; l_0 appears neither in it, nor in the premises on lines 1 and 2 (line 2 is also the existential cited), nor in line 6. At line 8, k_0 appears neither in line 7, nor in the premises (line 1 is the existential cited), and no box is open. The derivation has 8 lines. The written proof is three sentences: *Choose k with $n = 2k$, and l with $m = 2l$. Then $n + m = 2(k + l)$. So $n + m$ is even.*

Quick check. Why must the second witness in [Example \(The sum of two even integers is even\)](#) be called l_0 , and not k_0 again? Name the line and the clause of the side condition that a second k_0 would break.

Solution. The inner box would then be flagged k_0 with the assumption $m = 2 \cdot k_0$, and line 7 would close it by $\exists E$. At line 7 the outer box is still open, and its assumption $n = 2 \cdot k_0$ (line 3) contains k_0 . That breaks the clause “ x_0 does not appear in any assumption of a box still open at line k ”. In words: the second witness would be assumed to be the same integer as the first, so n and m would be forced equal, which the premises never said.

5.6.7 A contradiction trapped in a box

An $\exists E$ box may end in $\perp$. The contradiction is found inside the box, about the witness, and leaves it as $\perp$, which mentions no name. The best-known instance is a theorem of pure logic.

Theorem 5.6.3. The Barber

For every two-place predicate symbol R ,

$$\vdash \neg \exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x)).$$

Try it first (five minutes): the goal is a negation.

Idea. The goal is a negation: open a $\neg$ I box on the existential, aimed at $\perp$. Its assumption is an existential: name the witness early, y_0 , aiming the $\exists$ E box at the same $\perp$. Inside, an attempt that instantiates the universal at some other term t gets $R(t, y_0) \leftrightarrow \neg R(t, t)$, and nothing clashes with it; the one term that makes both sides speak of the same thing is y_0 itself. The instance says that $R(y_0, y_0)$ holds exactly when it does not, and a statement equivalent to its own negation is contradictory (Lemma 2.4.2).

1		$\exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x))$	asm, for $\neg$ I
		$\vdots$	
10		$\perp$	?
11		$\neg \exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x))$	?
1		$\exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x))$	asm, for $\neg$ I
2		y_0 $\forall x (R(x, y_0) \leftrightarrow \neg R(x, x))$	asm, for $\exists$ E
		$\vdots$	
9		$\perp$	?
10		$\perp$	$\exists$ E 1, 2–9
11		$\neg \exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x))$	?

Proof. The following is a derivation with no premises.

1		$\exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x))$	asm, for $\neg$ I
2		y_0 $\forall x (R(x, y_0) \leftrightarrow \neg R(x, x))$	asm, for $\exists$ E
3		$R(y_0, y_0) \leftrightarrow \neg R(y_0, y_0)$	$\forall$ E 2
4		$R(y_0, y_0)$	asm, for $\neg$ I
5		$\neg R(y_0, y_0)$	$\leftrightarrow$ E 3, 4
6		$\perp$	$\neg$ E 4, 5
7		$\neg R(y_0, y_0)$	$\neg$ I 4–6
8		$R(y_0, y_0)$	$\leftrightarrow$ E 3, 7
9		$\perp$	$\neg$ E 8, 7
10		$\perp$	$\exists$ E 1, 2–9
11		$\neg \exists y \forall x (R(x, y) \leftrightarrow \neg R(x, x))$	$\neg$ I 1–10

Lines 4–9 are lines 2–7 of the derivation of Lemma 2.4.2 at the statement $R(y_0, y_0)$, with line 3 in place of its assumption. At line 10, y_0 is not in $\perp$, not in the existential of line 1 (its y is bound), and there is no premise; the only open assumption, line 1, does not contain y_0 . This proves the theorem. ■

Read $R(x, y)$ as “ y shaves x ”: nobody shaves exactly those who do not shave themselves. The old puzzle of the barber who does is answered by this theorem: there is no such barber. Read the domain as consisting of sets and $R(x, y)$ as $x \in y$: no set has as its elements exactly the sets that are not elements of themselves. For sets this is Russell’s theorem, which *Sets, Relations, and Cardinality*, Section 1.1 proves as a theorem about sets. Neither reading was used in the proof, which holds for every R ; the “paradox” is eleven lines of logic, and its conclusion is that something does not exist.

Quick check. In the proof of [Theorem 5.6.3](#), lines 3–9 are all about y_0 . Why may line 10 close the $\exists E$ box?

Solution. Its last line, $\perp$, does not mention y_0 (clause 3); y_0 appears in no premise and in no open assumption (line 1’s y is bound), and not in the existential of line 1 (clauses 4 and 5).

5.6.8 How this rule looks in a mathematical proof

In a written proof, the $\exists E$ box is announced by “choose”, “let x_0 be such a point”, “say $n = 2k$ ”, “fix such a k ”. The assumption of the box is the property in the sentence, and the rest of the paragraph is the inside of the box. The claim the paragraph ends on, usually the clause after the final “so”, must not mention the chosen name, though the computation leading up to it may. If that claim still mentions the name, the paragraph has not finished: a later step must reach a claim without the name before the box can close, often an $\exists I$ that forgets it (as in the example below), or a contradiction $\perp$ (as in [Example \(Derivations with existential elimination\)](#) (b)).

🕒 **Second reading** · *A bounded sequence, rule by rule*

Here is an instance from analysis. A sequence (a_n) is **bounded** if there is an M with $|a_n| \leq M$ for every $n \in \mathbb{N}$. A proof says:

Since (a_n) is bounded, choose M with $|a_n| \leq M$ for all $n \in \mathbb{N}$. Then $|2a_n| = 2|a_n| \leq 2M$ for all $n \in \mathbb{N}$, so $(2a_n)$ is bounded.

With the domain $\mathbb{R}$, the sequence as a function symbol a , and the bound on n written out by Definition 5.1.1, the proof is this derivation.

1		$\exists M \forall n (n \in \mathbb{N} \rightarrow a_n \leq M)$	
2	M_0	$\forall n (n \in \mathbb{N} \rightarrow a_n \leq M_0)$	asm, for $\exists E$
3	n_0	$n_0 \in \mathbb{N}$	asm, for $\rightarrow I$
4		$n_0 \in \mathbb{N} \rightarrow a_{n_0} \leq M_0$	$\forall E$ 2
5		$ a_{n_0} \leq M_0$	$\rightarrow E$ 4, 3
6		$ 2 \cdot a_{n_0} \leq 2 \cdot M_0$	arith 5
7		$n_0 \in \mathbb{N} \rightarrow 2 \cdot a_{n_0} \leq 2 \cdot M_0$	$\rightarrow I$ 3–6
8		$\forall n (n \in \mathbb{N} \rightarrow 2 \cdot a_n \leq 2 \cdot M_0)$	$\forall I$ 3–7
9		$\exists M \forall n (n \in \mathbb{N} \rightarrow 2 \cdot a_n \leq M)$	$\exists I$ 8
10		$\exists M \forall n (n \in \mathbb{N} \rightarrow 2 \cdot a_n \leq M)$	$\exists E$ 1, 2–9

The sentences match the boxes. “Choose M ” opens the $\exists E$ box (line 2). “For all $n \in \mathbb{N}$ ” in the second sentence is the flagged box of n_0 with its $\rightarrow I$ box (lines 3–7, closed by line 8); the arithmetic $|2a_n| = 2|a_n| \leq 2M$ is line 6. “So $(2a_n)$ is bounded” is two steps: $\exists I$ with the witness $2 \cdot M_0$ (line 9), which forgets the bound $2M$, and the close of the box (line 10). The conclusion mentions neither M_0 nor $2 \cdot M_0$, as the side condition requires.

Warning. Two witnesses, one name. “Let n and m be even, say $n = 2k$ and $m = 2k$ ” is a common error in parity proofs. It gives two unknown witnesses the same name, and the rest of the proof then uses an equation the premises never gave. For instance it “proves” that the sum of two even integers is divisible by 4:

1		$\exists k (n = 2 \cdot k)$	
2		$\exists k (m = 2 \cdot k)$	
3	k_0	$n = 2 \cdot k_0$	asm, for $\exists E$
4	k_0	$m = 2 \cdot k_0$	asm, for $\exists E$
5		$n + m = 4 \cdot k_0$	arith 3, 4
6		$\exists k (n + m = 4 \cdot k)$	$\exists I$ 5
7		$\exists k (n + m = 4 \cdot k)$	$\exists E$ 2, 4–6
8		$\exists k (n + m = 4 \cdot k)$	$\exists E$ 1, 3–7

Line 7 is blocked: k_0 appears in the assumption $n = 2 \cdot k_0$ of the outer box, still open at line 7. With $n = 2$ and $m = 4$, both premises are true and $n + m = 6$ is not divisible by 4.

5.6.9 The four quantifier rules on one card

Example. Instances of $\exists E$

The existential	The box’s assumption (name)	The box’s last line	The new line
$\exists k (m = 2 \cdot k + 1)$	$m = 2 \cdot k_0 + 1 \ (k_0)$	$\exists j (m + 1 = 2 \cdot j)$	$\exists j (m + 1 = 2 \cdot j)$
$\exists y (R(f(c), y) \wedge \forall z R(y, z))$	$R(f(c), u_0) \wedge \forall z R(u_0, z) \ (u_0)$	$\exists y R(y, y)$	$\exists y R(y, y)$
$\exists \delta (\delta > 0 \wedge \delta < \varepsilon)$	$\delta_0 > 0 \wedge \delta_0 < \varepsilon \ (\delta_0)$	$\varepsilon > 0$	$\varepsilon > 0$

Inside each box the last line is reached from the assumption (in the first by arith, $m + 1 = 2 \cdot (k_0 + 1)$, and $\exists I$; in the second by $\wedge E$, $\forall E$ at u_0 and $\exists I$; in the third by arith from $0 < \delta_0 < \varepsilon$), and none mentions its name.

Not an instance. From $\exists x R(x, c)$, a box that opens with $R(c, x_0)$: the assumption must be $\varphi[x_0/x] = R(x_0, c)$; $R(c, x_0)$ assumes the witness stands on the other side of c , which the existential never said.

Chapters 1 and 2’s thirteen rules are on the card at the end of Section 3.1. Here are the four quantifier rules, with their side conditions. Section 5.7 collects the whole table, and nothing later depends on the last column.

Rule	Shape	Side condition	You write	Lean
$\forall E$	$\forall x \varphi \implies \varphi[t/x]$	t free for x in φ	“In particular, for $x = t, \dots$ ”; “applying the hypothesis to $t, \dots$ ”	h t (or specialize h t)
$\forall I$	box $[x_0] \dots$ $\varphi[x_0/x] \implies \forall x \varphi$	x_0 in no premise, in no open assumption, not in $\forall x \varphi$	“Let x be arbitrary. ... Since x was arbitrary, ...”	intro x
$\exists I$	$\varphi[t/x] \implies \exists x \varphi$	t free for x in φ	“Take $x = t$. Then ...”; “ $2k + 1$ will do.”	use t (or Exists.intro t h)
$\exists E$	$\exists x \varphi$, box $[x_0]$ $\varphi[x_0/x] \dots \chi$ $\implies \chi$	x_0 not in χ , not in $\exists x \varphi$, in no premise, in no open assumption	“Choose k with $n = 2k$. Then ...”; “let x_0 be such a point.”	obtain (or Exists.elim h)

🕒 Second reading · Choosing a name

The phrase “choose” is apt and slightly misleading. We do not choose the witness, since we cannot see it; we choose a **name** for it. A written proof that says “choose k ” promises the reader that nothing more about k will be used than the property stated, and that k will be gone by the end of the argument.

Warning (Not allowed: $\exists E$).

- “Close the box on a line that mentions its witness”: clause 3 (the pair in “Three ways to break the rule”).
- “Name the witness with a letter that a premise or an open assumption mentions”: clause 4 (the fold “Clauses 4 and 5, broken”; the warning “Two witnesses, one name”).
- “Name the witness with a letter that the existential mentions”: clause 5 (the fold “Clauses 4 and 5, broken”).
- “Open the box with an assumption other than $\varphi[x_0/x]$ ”: clause 1 (“Not an instance” in [Example \(Instances of \$\exists E\$ \)](#)).

The decision chart grows by two rows:

Main symbol	As the goal (goal-directed)	As an available line (premise-directed)
$\forall x \varphi$	open a flagged box with a brand-new name x_0 ; its last line is $\varphi[x_0/x]$; close with $\forall I$	instantiate at the term the goal, or another line, names ($\forall E$)
$\exists x \varphi$	postpone; use $\exists I$ once a line shows an instance $\varphi[t/x]$	open the $\exists E$ box at once, with a brand-new witness name, aimed at the current goal

The connective rows are the table of moves in Section 3.1.

The search method: one more step. With this rule, each of the four quantifier rules has added a step.

- **Premise $\exists x \varphi$.** Open the $\exists E$ box early, as soon as the existential is available, with a fresh name x_0 and the assumption $\varphi[x_0/x]$; make its last line the current goal, which must not mention x_0 . Give every new witness a new name.

In the Givens/Goal table, $\exists E$ puts a witness among the Givens, its name and its assumption $\varphi[x_0/x]$, and leaves the goal as it was.

Remark (Looking ahead). A derivation with n existential premises opens n boxes and names n witnesses, one choice per box. *Sets, Relations, and Cardinality*, Chapter 3 asks when infinitely many witnesses may be chosen at once, and answers with the axiom of choice.

5.6.10 Exercises

5.6.10.1 A. Check your understanding

Exercise. A1

These parts are about the proof of [Proposition 5.6.2](#).

- State $\exists E$ as a schema, with every clause of its side condition.
- The proof opened the flagged box of y_0 first and the $\exists E$ box of x_0 inside it. Could they

be opened in the other order? If so, does every side condition still hold?

- (c) Answer the *Before reading on* prompt of the proof: at line 5, where could x_0 still appear, and does it?
- (d) In the two attempts at the converse, $\forall y \exists x R(x, y) \vdash \exists x \forall y R(x, y)$, which line is blocked in each, and by which clause of which rule?
- (e) Give the idea of the proof in two sentences.

Solution. (a) From $\exists x \varphi$ on line h and a flagged box with name x_0 , from the assumption $\varphi[x_0/x]$ on line i to χ on line j , a line of the box itself, write χ on line k , justified “ $\exists E$ h , i – j ”. Side condition at line k : x_0 does not appear in χ , in $\exists x \varphi$, in any premise, or in any assumption of a box still open at line k .

(b) Yes, either order works. In the other order (the fold “Either nesting works” after the proof), the $\exists E$ box encloses the flagged box. At the $\forall I$ line, y_0 appears in no premise, not in the open assumption $\forall y R(x_0, y)$, and not in the conclusion; at the $\exists E$ line, x_0 is not in $\forall y \exists x R(x, y)$, not in the premise, and no box is open.

(c) At line 5, the clauses list four places: χ , which is line 4, $\exists x R(x, y_0)$; the existential of line 1, $\exists x \forall y R(x, y)$; the premise, which is line 1 again; and the assumptions of boxes open at line 5. The only box open at line 5 is the flagged box of y_0 , which has no assumption. The name x_0 appears in none of these, so line 5 is correct. It does appear in lines 2–4, inside the box, which the side condition allows.

(d) In the first attempt, line 5 ($\forall I$ over y_0) is blocked by the clause “ y_0 appears in no assumption of a box still open”, since the $\exists E$ box’s assumption $R(x_0, y_0)$ contains y_0 . In the second, line 4 ($\exists E$) is blocked by the clause “ x_0 does not appear in χ ”, since $\chi = R(x_0, y_0)$.

(e) Fix an arbitrary y_0 and obtain the witness x_0 of the premise, for which $R(x_0, y)$ holds for every y , in particular for y_0 . So x_0 is a witness for $\exists x R(x, y_0)$, and since y_0 was arbitrary, $\forall y \exists x R(x, y)$ follows.

Exercise. A2: Drill

Each part takes a line or two. The parts run from a single step, through a missing line, a justification column and steps to judge, to short derivations. “Clause” means a clause of the reading of [Definition 5.6.1](#).

- (a) A line h is $\exists x P(x)$. Write the first line of its $\exists E$ box, with the name u_0 .
- (b) Line 9 is $\exists y Q(y)$, justified “ $\exists E$ 3, 4–8”, and line 4 is the assumption $P(u_0) \wedge R(u_0, c)$. What is line 3?
- (c) Justify each line: 1 $\exists x (P(x) \wedge Q(x))$, premise; 2 $\forall x (Q(x) \rightarrow R(x))$, premise; in a box flagged x_0 : 3 $P(x_0) \wedge Q(x_0)$; 4 $Q(x_0)$; 5 $Q(x_0) \rightarrow R(x_0)$; 6 $R(x_0)$; 7 $P(x_0)$; 8 $P(x_0) \wedge R(x_0)$; 9 $\exists x (P(x) \wedge R(x))$; then, outside the box, 10 $\exists x (P(x) \wedge R(x))$.
- (d) An $\exists E$ box for $\exists k (m = 2 \cdot k)$, named k_0 , ends in $m^2 = 4 \cdot k_0^2$. May it close with that line?
- (e) The premise is $Q(x_0)$. May the box of $\exists x P(x)$ be named x_0 ?
- (f) Premises $\exists x P(x)$, $\exists x Q(x)$. May both boxes be named x_0 if one is inside the other?
- (g) May two boxes share a name if the first has closed before the second opens?

- (h) Inside an $\exists E$ box with assumption $P(x_0)$, may $\forall I$ generalize over x_0 ?
- (i) Find the illegal line: 1 $\exists x P(x)$, premise; in a box flagged x_0 : 2 $P(x_0)$, assumption; then 3 $P(x_0)$, $\exists E$ 1, 2–2; 4 $\exists y P(y)$, $\exists I$ 3.
- (j) Derive $\exists x (P(x) \wedge Q(x)) \vdash \exists x Q(x)$.
- (k) Derive $\exists x P(x), \forall x (P(x) \rightarrow Q(x)) \vdash \exists x Q(x)$.
- (l) Derive $\exists x \exists y R(x, y) \vdash \exists y \exists x R(x, y)$.

Solution.

- (a) The box flagged u_0 , opening with the assumption $P(u_0)$.
- (b) $\exists x (P(x) \wedge R(x, c))$, with any bound letter in place of x (one that does not clash with c or u_0).
- (c) 3 assumption, for $\exists E$; 4 $\wedge E$ 3; 5 $\forall E$ 2 (at x_0); 6 $\rightarrow E$ 5, 4; 7 $\wedge E$ 3; 8 $\wedge I$ 7, 6; 9 $\exists I$ 8; 10 $\exists E$ 1, 3–9.
- (d) No, clause 3: the last line mentions k_0 .
- (e) No, clause 4: x_0 appears in a premise.
- (f) No, clause 4: the inner box’s name appears in the open assumption $P(x_0)$ of the outer one.
- (g) Yes, as in [Example \(Derivations with existential elimination\)](#) (a), ($\neg$).
- (h) No: x_0 is in an open assumption, which the second clause of $\forall I$ forbids; the witness is not arbitrary.
- (i) Line 3, clause 3: its box’s last line mentions x_0 . (Line 4 would be legal; the conclusion is even derivable, with the $\exists I$ inside the box, but this derivation does not derive it.)
- (j) In a box flagged x_0 : 2 $P(x_0) \wedge Q(x_0)$, assumption; 3 $Q(x_0)$, $\wedge E$ 2; 4 $\exists x Q(x)$, $\exists I$ 3; then 5 $\exists x Q(x)$, $\exists E$ 1, 2–4.
- (k) In a box flagged x_0 : 3 $P(x_0)$, assumption; 4 $P(x_0) \rightarrow Q(x_0)$, $\forall E$ 2; 5 $Q(x_0)$, $\rightarrow E$ 4, 3; 6 $\exists x Q(x)$, $\exists I$ 5; then 7 $\exists x Q(x)$, $\exists E$ 1, 3–6.
- (l) In a box flagged x_0 : 2 $\exists y R(x_0, y)$, assumption; inside it, in a box flagged y_0 : 3 $R(x_0, y_0)$, assumption; 4 $\exists x R(x, y_0)$, $\exists I$ 3; 5 $\exists y \exists x R(x, y)$, $\exists I$ 4; then 6 $\exists y \exists x R(x, y)$, $\exists E$ 2, 3–5; and 7, the same line, $\exists E$ 1, 2–6.

5.6.10.2 B. Practice

Exercise. B1

Derive $\forall x \neg(P(x) \wedge Q(x)), \exists x P(x) \vdash \exists x \neg Q(x)$. Read the sequent over $\mathbb{Z}$ with P as “positive” and Q as “negative”.

Solution. Idea. The premise $\exists x P(x)$ opens its box first, with a witness x_0 , aimed at the goal. The goal $\exists x \neg Q(x)$ is postponed; the witness x_0 is the natural candidate, so the new goal inside is $\neg Q(x_0)$, a negation: a $\neg I$ box on $Q(x_0)$. Inside, $P(x_0) \wedge Q(x_0)$ clashes with the first premise at x_0 .

1		$\forall x \neg(P(x) \wedge Q(x))$	
2		$\exists x P(x)$	
3		x_0 $P(x_0)$	asm, for $\exists E$
4		$Q(x_0)$	asm, for $\neg I$
5		$P(x_0) \wedge Q(x_0)$	$\wedge I$ 3, 4
6		$\neg(P(x_0) \wedge Q(x_0))$	$\forall E$ 1
7		$\perp$	$\neg E$ 5, 6
8		$\neg Q(x_0)$	$\neg I$ 4–7
9		$\exists x \neg Q(x)$	$\exists I$ 8
10		$\exists x \neg Q(x)$	$\exists E$ 2, 3–9

At line 10, x_0 is not in line 9, not in line 2, not in either premise, and no box is open. Over $\mathbb{Z}$: no integer is both positive and negative, and some integer is positive, so some integer is not negative. The witness of the conclusion is the positive witness of the premise.

Exercise. B2: Fix, obtain, choose, faded

Here is a derivation of

$$\forall x \exists y R(x, y), \forall x \forall y (R(x, y) \rightarrow Q(y)) \vdash \forall x \exists y (R(x, y) \wedge Q(y))$$

with its last line missing.

1		$\forall x \exists y R(x, y)$	
2		$\forall x \forall y (R(x, y) \rightarrow Q(y))$	
3		x_0 $\exists y R(x_0, y)$	$\forall E$ 1
4		y_0 $R(x_0, y_0)$	asm, for $\exists E$
5		$\forall y (R(x_0, y) \rightarrow Q(y))$	$\forall E$ 2
6		$R(x_0, y_0) \rightarrow Q(y_0)$	$\forall E$ 5
7		$Q(y_0)$	$\rightarrow E$ 6, 4
8		$R(x_0, y_0) \wedge Q(y_0)$	$\wedge I$ 4, 7
9		$\exists y (R(x_0, y) \wedge Q(y))$	$\exists I$ 8
10		$\exists y (R(x_0, y) \wedge Q(y))$	$\exists E$ 3, 4–9

Name the move, then complete it. Then mark which lines are the “fix”, which the “obtain”, and which the “choose”.

Solution. The missing line closes the flagged box of x_0 by $\forall I$; the move is the “fix” of fix, obtain, choose, completed: “since x_0 was arbitrary”.

1		$\forall x \exists y R(x, y)$	
2		$\forall x \forall y (R(x, y) \rightarrow Q(y))$	
3	x_0	$\exists y R(x_0, y)$	$\forall E$ 1
4		y_0 $R(x_0, y_0)$	asm, for $\exists E$
5		$\forall y (R(x_0, y) \rightarrow Q(y))$	$\forall E$ 2
6		$R(x_0, y_0) \rightarrow Q(y_0)$	$\forall E$ 5
7		$Q(y_0)$	$\rightarrow E$ 6, 4
8		$R(x_0, y_0) \wedge Q(y_0)$	$\wedge I$ 4, 7
9		$\exists y (R(x_0, y) \wedge Q(y))$	$\exists I$ 8
10		$\exists y (R(x_0, y) \wedge Q(y))$	$\exists E$ 3, 4–9
11		$\forall x \exists y (R(x, y) \wedge Q(y))$	$\forall I$ 3–10

Line 11 cites the flagged box 3–10; its last line, line 10, is a line of that box itself and is the instance $\psi[x_0/x]$ for $\psi = \exists y (R(x, y) \wedge Q(y))$. The name x_0 appears in neither premise and not in line 11, and at line 11 no box is open. (At line 10, y_0 is not in line 9, not in line 3, not in the premises, and the only open box, that of x_0 , has no assumption.)

The moves: **fix** is the flagged box of x_0 (opened before line 3, closed at line 11); **obtain** is line 3 ($\forall E$ at x_0) and the $\exists E$ box of y_0 (lines 4–10), with lines 5–7 using the second premise on the witness; **choose** is line 9, $\exists I$ with the witness y_0 .

Exercise. B3

An integer n is **odd** when $n = 2k + 1$ for some integer k . Over $\mathbb{Z}$, derive

$$\exists k (m = 2 \cdot k + 1), \exists k (n = 2 \cdot k + 1) \vdash \exists k (m \cdot n = 2 \cdot k + 1),$$

with one line justified “arith”. Then write the proof as three sentences of prose.

Solution. Idea. As in [Example \(The sum of two even integers is even\)](#): open both boxes early, with different names, and postpone the goal until the arithmetic shows the witness.

1		$\exists k (m = 2 \cdot k + 1)$	
2		$\exists k (n = 2 \cdot k + 1)$	
3		k_0 $m = 2 \cdot k_0 + 1$	asm, for $\exists E$
4		l_0 $n = 2 \cdot l_0 + 1$	asm, for $\exists E$
5		$m \cdot n = 2 \cdot (2 \cdot k_0 \cdot l_0 + k_0 + l_0) + 1$	arith 3, 4
6		$\exists k (m \cdot n = 2 \cdot k + 1)$	$\exists I$ 5
7		$\exists k (m \cdot n = 2 \cdot k + 1)$	$\exists E$ 2, 4–6
8		$\exists k (m \cdot n = 2 \cdot k + 1)$	$\exists E$ 1, 3–7

Line 5: $(2k_0 + 1)(2l_0 + 1) = 4k_0l_0 + 2k_0 + 2l_0 + 1 = 2(2k_0l_0 + k_0 + l_0) + 1$. Line 6 is $\exists I$ with $\varphi = (m \cdot n = 2 \cdot k + 1)$ and the witness $2 \cdot k_0 \cdot l_0 + k_0 + l_0$. At line 7, l_0 is in none of line 6, line 2, the premises, and the open assumption on line 3; at line 8, k_0 is in none of line 7, line 1, the premises, and no box is open.

In prose: Choose integers k and l with $m = 2k + 1$ and $n = 2l + 1$. Then $mn = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$. Since $2kl + k + l$ is an integer, mn is odd.

Exercise. B4: Derive or break

For each claim, derive it with the rules so far, or break it with a counter-reading.

- (a) $\exists x \forall y R(x, y) \vdash \exists x R(x, x)$.
- (b) $\forall x \exists y R(x, y) \vdash \exists x R(x, x)$.
- (c) $\forall x (P(x) \rightarrow Q(x)), \exists x \neg Q(x) \vdash \exists x \neg P(x)$.
- (d) $\forall x (P(x) \rightarrow Q(x)), \exists x \neg P(x) \vdash \exists x \neg Q(x)$.
- (e) $\exists x P(f(x)) \vdash \exists y P(y)$.
- (f) $\exists y P(y) \vdash \exists x P(f(x))$.
- (g) $\forall x (P(x) \rightarrow \exists y R(x, y)), \exists x P(x) \vdash \exists y \exists x R(x, y)$.

Solution.

- (a) Derive. Obtain the witness, and instantiate its universal at the witness itself.

1		$\exists x \forall y R(x, y)$	
2		x_0 $\forall y R(x_0, y)$	asm, for $\exists E$
3		$R(x_0, x_0)$	$\forall E$ 2
4		$\exists x R(x, x)$	$\exists I$ 3
5		$\exists x R(x, x)$	$\exists E$ 1, 2–4

- (b) Break. The domain $\{0, 1\}$, with R true of the pairs $(0, 1)$ and $(1, 0)$ only. Each element is related to something, and no element to itself.
- (c) Derive. The $\exists E$ box opens first, aimed at the goal; inside it, a $\neg I$ box.

1	$\forall x (P(x) \rightarrow Q(x))$	
2	$\exists x \neg Q(x)$	
3	$x_0 \mid \neg Q(x_0)$	asm, for $\exists E$
4	$P(x_0) \rightarrow Q(x_0)$	$\forall E$ 1
5	$\mid P(x_0)$	asm, for $\neg I$
6	$\mid Q(x_0)$	$\rightarrow E$ 4, 5
7	$\mid \perp$	$\neg E$ 6, 3
8	$\neg P(x_0)$	$\neg I$ 5–7
9	$\exists x \neg P(x)$	$\exists I$ 8
10	$\exists x \neg P(x)$	$\exists E$ 2, 3–9

(d) Break. The domain $\{0, 1\}$, with P true of nothing and Q true of both elements. The first premise holds (no hypothesis $P(x)$ is true), the second holds since $\neg P(0)$, and no element lacks Q .

(e) Derive. The witness of the conclusion is the compound term $f(x_0)$.

1	$\exists x P(f(x))$	
2	$x_0 \mid P(f(x_0))$	asm, for $\exists E$
3	$\exists y P(y)$	$\exists I$ 2
4	$\exists y P(y)$	$\exists E$ 1, 2–3

(f) Break. The domain $\{0, 1\}$, with f sending both elements to 0, and P true of 1 only. Some element has P , and no value of f does.

(g) Derive. Two boxes with different names, the second inside the first.

1	$\forall x (P(x) \rightarrow \exists y R(x, y))$	
2	$\exists x P(x)$	
3	$x_0 \mid P(x_0)$	asm, for $\exists E$
4	$P(x_0) \rightarrow \exists y R(x_0, y)$	$\forall E$ 1
5	$\exists y R(x_0, y)$	$\rightarrow E$ 4, 3
6	$y_0 \mid R(x_0, y_0)$	asm, for $\exists E$
7	$\exists x R(x, y_0)$	$\exists I$ 6
8	$\exists y \exists x R(x, y)$	$\exists I$ 7
9	$\exists y \exists x R(x, y)$	$\exists E$ 5, 6–8
10	$\exists y \exists x R(x, y)$	$\exists E$ 2, 3–9

At line 9 the open assumption $P(x_0)$ does not contain y_0 ; at line 10 no box is open.

The pairs: (c) and (d) are the contrapositive and its look-alike (denying the antecedent); (e) and (f) are converses; (a) and (b) differ in the order of the quantifiers. Worked examples of these types: [Proposition 5.6.1](#) and its Quick check (a counter-reading); [Example \(Derivations](#)

with existential elimination) (b); [Example \(The sum of two even integers is even\)](#); the two-dot counter-reading of the converse of [Proposition 5.6.2](#).

Marking scheme. (10 points)

- 1 each: (a), (b), (d), (e), (f), with the derivation or the counter-reading in full.
- 2: (c), with the $\exists E$ box opened first and aimed at the goal, and $\neg P(x_0)$ obtained inside it (by a $\neg I$ box or by MT).
- 2: (g), with two boxes, different names, closed in the right order.
- 1: the closing pairing.

Fatal errors (0 for the claim): an $\exists E$ box closed on a line that mentions its witness; a counter-reading in which a premise is false.

5.6.10.3 C. Going deeper

Exercise. C1

Derive

$$\exists x \forall y R(x, y), \forall x \forall y (R(x, y) \rightarrow R(y, x)) \vdash \forall y \exists x R(y, x),$$

and check the side condition of every $\exists E$ and $\forall I$ line. Then give a reading over $\mathbb{Z}$ in which both premises are true, and say which integer the derivation’s witness is.

Solution (Hint 1). The shape is the one of [Proposition 5.6.2](#): fix, obtain, choose. Which line does symmetry have to turn round?

Solution (Hint 2). Open a flagged box for y_0 , and inside it the $\exists E$ box of the first premise, with the assumption $\forall y R(x_0, y)$.

Solution. Idea. The goal is $\forall y$: fix y_0 . The new goal $\exists x R(y_0, x)$ is postponed. The first premise is an existential: obtain x_0 with $\forall y R(x_0, y)$, and instantiate it at the term the goal mentions, y_0 : $R(x_0, y_0)$. The goal needs $R(y_0, t)$, with y_0 first, so the second premise turns the line round, instantiated at x_0 and y_0 in that order (read off the line to be turned). Then choose the witness x_0 .

1		$\exists x \forall y R(x, y)$	
2		$\forall x \forall y (R(x, y) \rightarrow R(y, x))$	
3	y_0 x_0	$\forall y R(x_0, y)$	asm, for $\exists E$
4		$R(x_0, y_0)$	$\forall E$ 3
5		$\forall y (R(x_0, y) \rightarrow R(y, x_0))$	$\forall E$ 2
6		$R(x_0, y_0) \rightarrow R(y_0, x_0)$	$\forall E$ 5
7		$R(y_0, x_0)$	$\rightarrow E$ 6, 4
8		$\exists x R(y_0, x)$	$\exists I$ 7
9		$\exists x R(y_0, x)$	$\exists E$ 1, 3–8
10		$\forall y \exists x R(y, x)$	$\forall I$ 3–9

Line 9 ($\exists E$): x_0 does not appear in $\chi = \exists x R(y_0, x)$, nor in the existential of line 1, nor in either premise; the only box open at line 9 is the flagged box of y_0 , which has no assumption. Line 8 is a line of the $\exists E$ box itself.

Line 10 ($\forall I$): the flagged box immediately contains the $\exists E$ box, so its range starts at line 3. Its last line, line 9, is a line of the box itself and is $(\exists x R(y, x))[y_0/y]$. The name y_0 appears in neither premise and not in line 10, and no box is open.

A reading. Over $\mathbb{Z}$, let $R(x, y)$ mean “ $x \cdot y = 0$ ”. The second premise holds since $x \cdot y = y \cdot x$. The first holds with the witness 0, and only with it: for $x \neq 0$, the instance $y = 1$ gives $x \cdot 1 = x \neq 0$. The conclusion says that every integer has a partner with product 0, which is true. The derivation’s x_0 names the witness of the first premise, so under this reading it can only be 0, and the derivation gives every y the partner 0; the derivation itself never uses which integer it is.

Marking scheme. (10 points) - 2: opens a flagged box for the goal’s $\forall y$ with a fresh name, and postpones the existential. - 2: opens the $\exists E$ box of the first premise with a **fresh** witness, aimed at the current goal. - 2: instantiates the assumption at y_0 and the symmetry premise at x_0, y_0 in that order, and fires it. - 2: $\exists I$ with the witness x_0 , inside the $\exists E$ box. - 1: checks the side conditions of the $\exists E$ and $\forall I$ lines clause by clause. - 1: a reading over $\mathbb{Z}$ in which both premises hold, with the witness identified (or, if the reading does not determine it, correctly described as whichever witness the first premise has). Fatal errors (0 for the step): an $\exists E$ box closed on a line containing its witness; $\forall I$ over a name in an open assumption; the symmetry premise instantiated in the wrong order and then used as if it fired.

Exercise. C2: Find the error, used later

Here is a “derivation” of $\exists x (P(x) \wedge Q(x)) \vdash \exists x P(x)$.

1		$\exists x (P(x) \wedge Q(x))$	
2		x_0 $P(x_0) \wedge Q(x_0)$	asm, for $\exists E$
3		$P(x_0)$	$\wedge E$ 2
4		$P(x_0)$	$\exists E$ 1, 2–3
5		$\exists x P(x)$	$\exists I$ 4

- (a) Is the conclusion derivable from the premise? Justify your answer.
- (b) Does this derivation prove it? If not, name the exact line that fails, the rule, and the clause of its side condition that is broken.
- (c) Show that the illegal step itself is unsound: use the same step to “derive”, from a premise true over $\mathbb{Z}$, a sentence false over $\mathbb{Z}$.

Solution (Hint 1). For (a), the conclusion is half of the conclusion of a result proved in this section.

Solution (Hint 2). For (c), drop Q : start from the premise $\exists x P(x)$ and take the same illegal step as line 4.

Solution. (a) Yes, the conclusion is derivable: by [Proposition 5.6.1](#) the premise gives $\exists x P(x) \wedge \exists x Q(x)$, and $\wedge E$ gives $\exists x P(x)$. Directly, moving the $\exists I$ inside the box repairs the derivation:

1		$\exists x (P(x) \wedge Q(x))$	
2		x_0 $P(x_0) \wedge Q(x_0)$	asm, for $\exists E$
3		$P(x_0)$	$\wedge E$ 2
4		$\exists x P(x)$	$\exists I$ 3
5		$\exists x P(x)$	$\exists E$ 1, 2–4

At line 5, x_0 is not in line 4, not in line 1, and no box is open.

(b) No. Line 4 fails: it is $\exists E$ with $\chi = P(x_0)$, and x_0 appears in χ , which breaks the clause “ x_0 does not appear in χ ” of [Definition 5.6.1](#). The witness has escaped its box. Lines 1–3 are correct, and line 5 would be a correct $\exists I$ if line 4 were a legitimate line. A true conclusion does not make the argument correct: the conclusion is derivable, but not by this derivation.

(c) The same step, from $\exists x P(x)$ alone:

1	$\exists x P(x)$	
2	$x_0 \mid P(x_0)$	asm, for $\exists E$
3	$P(x_0)$	$\exists E$ 1, 2–2
4	$x_0 \mid P(x_0)$	R 3
5	$\forall x P(x)$	$\forall I$ 4–4

Line 3 is the illegal step of line 4 above. Line 4 repeats line 3 into a flagged box, and line 5 is a correct $\forall I$: x_0 appears in no premise, in no open assumption, and not in line 5. Over $\mathbb{Z}$ with P as “even”, the premise “some integer is even” is true and the conclusion “every integer is even” is false. So the step from $\exists x P(x)$ to $P(x_0)$ can lead from truth to falsehood; it is a counterexample to the **step**, while the conclusion of the original sequent has no counterexample at all. (This is the same failure as the derivation after [Definition 5.6.1](#) that “proves” every natural number exceeds 5.)

Marking scheme. (10 points) - 2: (a) says the conclusion is derivable and gives a correct derivation or cites [Proposition 5.6.1](#) with $\wedge E$. - 3: (b) names line 4, the rule $\exists E$, and the clause “ x_0 not in χ ”. - 1: (b) says that the other lines are correct, so the error is in that one line. - 4: (c) gives a derivation that uses the same illegal step and is otherwise legal, with a reading in which the premise is true and the conclusion false. Fatal errors (0 for the step): answering (a) “no” because the derivation is wrong; giving a counterexample to the conclusion of the original sequent (there is none); blaming line 5.

Exercise. C3: The diagonal of a list

Let $A_0, A_1, A_2, \dots$ be sets of natural numbers, one for each $n \in \mathbb{N}$, and let $D = \{n \in \mathbb{N} : n \notin A_n\}$.

- Over the domain $\mathbb{N}$, read $R(x, y)$ as “ $x \in A_y$ ”. Follow the proof of [Theorem 5.6.3](#) in this reading to show that D is none of the sets A_m .
- Compute D for the list $A_n = \{k \in \mathbb{N} : k > n\}$, and for the list $A_n = \{k \in \mathbb{N} : k \text{ is a multiple of } n+1\}$. In each case, find a number at which D differs from A_0 , from A_1 and from A_2 .

Solution (Hint). In (a), the existential of line 1 is “some m has $D = A_m$ ”. What does the definition of D say about every n , when $D = A_m$?

Solution. (a) Suppose $D = A_m$ for some m : this is the existential of line 1, with its witness named m (line 2). By the definition of D , for every n : $n \in A_m$ exactly when $n \notin A_n$; that is $\forall x (R(x, m) \leftrightarrow \neg R(x, x))$. At $n = m$ (line 3): $m \in A_m$ exactly when $m \notin A_m$, which is impossible (lines 4–9). So no m has $D = A_m$.

(b) First list: $n > n$ is false, so $n \notin A_n$ for every n , and $D = \mathbb{N}$. D differs from A_m at m : $m \in D$ and $m \notin A_m$ ($0 \notin A_0$, $1 \notin A_1$, $2 \notin A_2$).

Second list: n is a multiple of $n+1$ only for $n = 0$ ($0 = 0 \cdot 1$; for $n \geq 1$, $0 < n < n+1$), so $D = \{1, 2, 3, \dots\}$. $A_0 = \mathbb{N}$ contains $0 \notin D$; $A_1 = \{0, 2, 4, \dots\}$ lacks $1 \in D$; $A_2 = \{0, 3, 6, \dots\}$

lacks $2 \in D$.

In both, D and A_m differ at the number m itself, as the proof says they must.

Marking scheme. (10 points)

- 2: the assumption $D = A_m$ set up as the witness of an existential.
- 2: the universal $\forall x (R(x, m) \leftrightarrow \neg R(x, x))$ read off the definition of D .
- 2: the instance at m and the contradiction.
- 2: the first list's D , with the three differences.
- 2: the second list's D (the case $n = 0$ justified), with the three differences.

Fatal error (0 for (a)): instantiating at some number other than m .