

5.5 Proving “There Exists”: Exhibit a Witness

Sections 5.3 and 5.4 gave the two rules for “for every”: $\forall E$ uses a universal statement, and $\forall I$ proves one. This section starts on the other quantifier. It gives the rule that **proves** an existential statement, $\exists I$, and the habit that goes with it: when the goal is “there exists”, do not guess the object, but wait until a line of the derivation shows it. The sequent $\forall x P(x) \vdash \exists x P(x)$, which no rule so far can finish, is finished here in three lines.

5.5.1 Showing that something exists

How does a mathematician prove that there is a natural number N with $1/(N+1) < 1/100$? By naming one. “Take $N = 100$: then $1/(N+1) = 1/101$, and $1/101 < 1/100$.” Nobody asks for more, and nobody objects that $N = 1000$ would also have done. The proof exhibits a **witness**, checks that it has the property, and stops.

Look at what the proof does with the witness at the end. The statement proved, “there is an N with $1/(N+1) < 1/100$ ”, does not say which N ; the 100 still in it belongs to the bound $1/100$, not to N . The number was needed to establish the claim and is then forgotten: a reader of the conclusion learns that some N works, not which one.

Chapter 1 used the same pattern from its first page. It recalled that an integer n is **even** when $n = 2k$ for **some** integer k , and said that the word “some” has rules of its own, to come in Chapter 5. Here is the first of them. To show that 6 is even, take $k = 3$: then $6 = 2 \cdot 3$. The statement “6 is even” is $\exists k (6 = 2 \cdot k)$, and the proof passes from the instance $6 = 2 \cdot 3$ to it. The second rule for “some”, how to **use** “ $n = 2k$ for some k ”, is the subject of Section 5.6.

There is a helpful way to see the step, which Section 5.1’s reading of $\exists$ suggests. Over a domain with three elements named a, b, c , the sentence $\exists x P(x)$ says what the disjunction

$$P(a) \vee P(b) \vee P(c)$$

says (grouped to the right, as in Section 4.5): at least one of the three has P . An existential is a long “or”, with one disjunct for each object of the domain. Proving a disjunction from one of its sides is $\vee I$ (Definition 1.5.1), and proving an existential from one instance is the rule of this section. The analogy is only a guide (a domain such as $\mathbb{N}$ has infinitely many elements, and a formula cannot be infinitely long), but it predicts the rule’s behavior exactly: it throws information away, and it must never be run backwards.

5.5.2 The rule of existential introduction

To prove that something has a property, show that one particular thing has it.

Definition 5.5.1. Existential Introduction

$$\begin{array}{c|c} i & \varphi[t/x] \\ k & \exists x \varphi \quad \exists I \ i \end{array}$$

The rule given by this schema is called $\exists I$ (**existential introduction**). Here φ is **any**

formula, x any variable, and t **any** term, subject to one side condition: t is **free for x in φ** (Definition 5.2.6). Line i must be available at line k (Definition 1.4.2).

- **Schema:** the block above: one cited line, no box, no fresh name.
- **Reading:** from a line that says something about the term t , write “something has that property”: mark some occurrences of t with a variable x to get φ , and write $\exists x \varphi$.
- **Example:** from $6 = 2 \cdot 3$, marking the 3 gives $\exists k (6 = 2 \cdot k)$.

Which occurrences? Any you like, as the table below shows; the term t is the **witness**, and it may be a constant, a compound term or a variable: a variable used elsewhere in the derivation, a flag such as x_0 , or even the variable x itself. Check two things. First, $\varphi[t/x]$ must be **exactly** the cited line: choose a variable x that does not appear in the line and mark some occurrences of t with it, and this marking recipe guarantees it; with an x that does appear, check directly (from $R(x, c)$, marking c gives $R(x, x)$, and $R(x, x)[c/x]$ is $R(c, c)$, not the line). Second, t must be free for x in φ , the condition of Definition 5.2.6 that $\forall E$ also carries. With a bound, $\exists x \in A \varphi$, the witness needs the line $t \in A$ too; “A bounded witness” below shows the two steps.

One line, several readings. Let line i be $R(c, c)$, with R a two-place predicate symbol and c a constant. The witness is c , and c occurs twice. Each occurrence may be marked with x or left alone, and each choice is a different φ :

φ	$\varphi[c/x]$ (the cited line)	the new line $\exists x \varphi$
$R(x, c)$	$R(c, c)$	$\exists x R(x, c)$
$R(c, x)$	$R(c, c)$	$\exists x R(c, x)$
$R(x, x)$	$R(c, c)$	$\exists x R(x, x)$

All three are legal steps. Read over $\mathbb{N}$ with $R(x, y)$ as “ $x \leq y$ ” and c as 5: the cited line says $5 \leq 5$, and the three useful conclusions say that something is at most 5, that 5 is at most something, and that something is at most itself. Each is a true and weaker statement.

⊙ **Second reading** · *A witness that is not marked*

A fourth row is legal too:

φ	$\varphi[c/x]$ (the cited line)	the new line $\exists x \varphi$
$R(c, c)$	$R(c, c)$	$\exists x R(c, c)$

The last row is the **degenerate** choice: φ has no free x , so $\varphi[c/x]$ is φ (Section 5.2) and the new line $\exists x R(c, c)$ quantifies over nothing. It is legal, and it says nothing that line i did not.

Why this rule. Under the reading of Section 5.1, $\exists x \varphi$ is true when at least one element of the domain, put in for x , makes φ true. If $\varphi[t/x]$ is true, then the object that t names is such an element, so $\exists x \varphi$ is true. The side condition is what makes “ $\varphi[t/x]$ says about t what φ says about x ” correct: that was the content of “free for” in Section 5.2.

$\exists I$ forgets the witness, and keeps the truth.

Quick check. Line 1 is $x_0 + 1 > x_0$. Give an $\exists$ I line with the witness x_0 , and one with the witness $x_0 + 1$.

Solution. Marking both occurrences of x_0 with y gives $\varphi = (y + 1 > y)$ and the line $\exists y (y + 1 > y)$; marking the term $x_0 + 1$ gives $\varphi = (y > x_0)$ and the line $\exists y (y > x_0)$. In both, y appears nowhere in line 1, and the formula has no quantifier, so the witness is free for y .

A nonexample: capture. Let line 1 be $\forall y R(y, y)$. With $\varphi = \forall y R(x, y)$ and $t = y$, the definition of substitution gives $\varphi[y/x] = \forall y R(y, y)$, which is line 1. So it is tempting to write $\exists x \forall y R(x, y)$ by $\exists$ I.

$$\begin{array}{l|l} 1 & \forall y R(y, y) \\ \hline 2 & \exists x \forall y R(x, y) \quad \exists\text{I } 1 \end{array}$$

Line 2 breaks the side condition: the free occurrence of x in φ lies in the scope of $\forall y$, and y is the variable of the term t , so y is **not** free for x in φ . The step would be wrong. Read over $\mathbb{Z}$ with $R(x, y)$ as “ $x \leq y$ ”: line 1 says that every integer is at most itself, which is true, and line 2 says that some integer is at most every integer, that is, that there is a least integer, which is false. The y put in for x was meant to name one object, and it was captured by $\forall y$ and made to range over all of them.

Warning. The witness must be **written on a line**. “There is an N with $1/(N+1) < 1/100$: take N large enough” is not an application of $\exists$ I, because “large enough” is not a term, and the rule asks for an instance $\varphi[t/x]$ on an available line. In a written proof, “large enough” is a promise to name the witness, and the promise is kept by a term such as $N = 100$, followed by the check that it works ($1/101 < 1/100$). Until then nothing has been proved.

Quick check. Let line 1 be $2 + 2 = 4$. Which of

$$\exists x (x + x = 4), \quad \exists x (x + 2 = 4), \quad \exists x (2 + 2 = x)$$

may line 2 be, justified by one application of $\exists$ I to line 1? For each that may, name φ and the witness t .

Solution. All three. For $\exists x (x + x = 4)$, take $\varphi = (x + x = 4)$ and $t = 2$: both 2’s of line 1 are marked. For $\exists x (x + 2 = 4)$, take $\varphi = (x + 2 = 4)$ and $t = 2$: only the first 2 is marked, and the second is written out in φ . For $\exists x (2 + 2 = x)$, take $\varphi = (2 + 2 = x)$ and $t = 4$: the witness is a different term. In each case $\varphi[t/x]$ is exactly line 1, and φ has no quantifier, so t is free for x .

5.5.3 From “for every” to “there exists”

The sequent $\forall x P(x) \vdash \exists x P(x)$ looks like the easiest in the chapter, and it has a small puzzle in it. To use $\exists\text{I}$, the goal needs an instance $P(t)$ on a line. The premise gives an instance for every term, by $\forall\text{E}$. But the sequent mentions no constant, so which term?

Proposition 5.5.1. Every Implies Some

$\forall x P(x) \vdash \exists x P(x)$.

Proof. The following is a derivation.

1	$\forall x P(x)$	
2	$P(x)$	$\forall\text{E } 1$
3	$\exists x P(x)$	$\exists\text{I } 2$

Line 2 is $\forall\text{E}$ at the term x : with $\varphi = P(x)$, the instance $\varphi[x/x]$ is $P(x)$, and the variable x is free for x in every formula (Section 5.2). Line 3 is $\exists\text{I}$ with the same φ and the witness x . This proves the proposition. ■

The puzzle is answered by the paragraph “Which occurrences?” after [Definition 5.5.1](#): the witness may be a variable, the variable x itself included, so no constant is needed. The line $P(x)$ has x free; it says that P holds of whatever x names. Nothing in the derivation says what that is, and nothing needs to. The same three lines prove $\forall x \varphi \vdash \exists x \varphi$ for every formula φ , since $\varphi[x/x] = \varphi$ (Section 5.2).

Remark. The rules accept this derivation in any case; it leads from a true premise to a true conclusion only because every domain has **at least one** element, the convention of Section 5.1. Over an empty domain, $\forall x P(x)$ would be true with nothing to check and $\exists x P(x)$ false with no witness; the convention enters at line 2, where $P(x)$ treats x as naming an object, and there must be one to name.

🔄 **Second reading** · *The empty set, again*

This does not clash with the empty set of Section 5.1, where $\forall x \in \emptyset \varphi$ is true and $\exists x \in \emptyset \varphi$ is false. A bounded quantifier is an abbreviation (Definition 5.1.1): $\forall x \in \emptyset \varphi$ is $\forall x (x \in \emptyset \rightarrow \varphi)$, and $\exists x \in \emptyset \varphi$ is $\exists x (x \in \emptyset \wedge \varphi)$. The domain is still non-empty; it is the set $\emptyset$ that has no elements. Running the three lines on the bounded premise gives $\forall\text{E}$ at x , the line $x \in \emptyset \rightarrow \varphi$, and then $\exists\text{I}$ gives only $\exists x (x \in \emptyset \rightarrow \varphi)$, an existential with $\rightarrow$ inside. No line $x \in \emptyset$ is available to fire the implication, so the bounded “every implies some” is not derived, and it should not be.

5.5.4 An existential goal: postpone the witness

The search method of Section 3.1 asks two questions at each gap: what is the goal, and what are the resources? Sections 5.3 and 5.4 added a step for each side of $\forall$. Now $\exists$ can be a goal.

If the goal is $\exists x \varphi$, its last line can be $\exists I$, and then the new goal is $\varphi[t/x]$ for a term t **of our choosing**. That is the same situation as a goal $\varphi \vee \psi$, where $\vee I$ left us to choose a side, and the danger is the same. A wrong t can leave a goal that does not follow from the resources, although the existential does. Section 3.1 met the danger for $\vee$ and answered it by postponing; the answer here is the same.

Postpone the witness: choose the term t of a goal $\exists x \varphi$ only when an available line shows an instance $\varphi[t/x]$.

Quick check. Premises: $\forall x (P(x) \rightarrow Q(x+1))$ and $P(2)$. The goal is $\exists y Q(y)$. Which witness will the search find, and after which steps?

Solution. The term $2+1$: $\forall E$ at 2 gives $P(2) \rightarrow Q(2+1)$, $\rightarrow E$ gives $Q(2+1)$, and only then does $\exists I$ have an instance to cite. (Writing the witness as 3 instead needs the line $2+1=3$ and the equality rule of Section 5.7.)

Until then, work on the premises and on the other goals, and watch what terms appear. Often the witness is a term that only appears late, built by $\forall E$ or $\rightarrow E$ from the premises. Here are four derivations, in order of difficulty, each with an Idea that says why each rule was chosen.

Example. Derivations with existential introduction

Show that:

- (a) $P(c) \wedge Q(c) \vdash \exists x (P(x) \wedge Q(x))$;
- (b) $R(c, c) \vdash \exists x R(x, c) \wedge \exists x R(x, x)$; and decide whether one $\exists I$ step leads from $\exists x R(x, x)$ to $\exists x R(x, c)$;
- (c) $\forall x R(x, x) \vdash \forall x \exists y R(x, y)$;
- (d) $\forall x (P(x) \rightarrow Q(f(x))), P(c) \vdash \exists y Q(y)$.

Solution.

- (a) *Idea.* The goal is an existential, and the premise already is an instance of a suitable φ : mark both occurrences of c . One goal-directed step finishes.

1	$P(c) \wedge Q(c)$	
2	$\exists x (P(x) \wedge Q(x))$	$\exists I$ 1

Here $\varphi = P(x) \wedge Q(x)$ and $t = c$. Marking only the first c , with $\varphi = P(x) \wedge Q(c)$, would give the legal but weaker line $\exists x (P(x) \wedge Q(c))$, which is not the goal.

- (b) *Idea.* The goal is a conjunction, so it splits into two goals (Section 1.2), and each is an existential with the line $R(c, c)$ as an instance, read in two different ways (the first and third rows of the table above). The goal at the bottom (left); then the two subgoals

that $\wedge I$ asks for (right).

1	$R(c, c)$			1	$R(c, c)$		
	$\vdots$				$\vdots$		
2	$\exists x R(x, c)$		?	2	$\exists x R(x, c)$		?
	$\vdots$				$\vdots$		
3	$\exists x R(x, x)$		?	3	$\exists x R(x, x)$		?
4	$\exists x R(x, c) \wedge \exists x R(x, x)$		?	4	$\exists x R(x, c) \wedge \exists x R(x, x)$	$\wedge I$ 2, 3	

1	$R(c, c)$		
2	$\exists x R(x, c)$	$\exists I$ 1	
3	$\exists x R(x, x)$	$\exists I$ 1	
4	$\exists x R(x, c) \wedge \exists x R(x, x)$	$\wedge I$ 2, 3	

Line 2 uses $\varphi = R(x, c)$ and line 3 uses $\varphi = R(x, x)$, both with the witness c .

Now the second question. From the line $\exists x R(x, x)$, the step to $\exists x R(x, c)$ is **not** an $\exists I$ step. The new line is $\exists x \varphi$ with $\varphi = R(x, c)$, so the cited line would have to be $R(t, c)$ for some term t . The line $\exists x R(x, x)$ is not of that form: its main symbol is $\exists x$, not R . The rule passes from an **instance** to an existential, never from one existential to another. Nor is the step safe by any other route: read over $\mathbb{Z}$ with $R(x, y)$ as “ $x \cdot y = 1$ ” and c as 0, the line $\exists x R(x, x)$ is true (take $x = 1$), and $\exists x R(x, c)$, “some integer times 0 is 1”, is false.

- (c) *Idea.* The goal is a $\forall$, so the step of Section 5.4 opens a flagged box with a fresh name x_0 , and the new goal is $\exists y R(x_0, y)$. That is an existential: postpone it and look at the premise. The premise is a $\forall$; instantiate it at the term the goal mentions, x_0 . The result, $R(x_0, x_0)$, shows the witness: it is x_0 itself, a variable used as a term, as x was in Proposition 5.5.1. The box with its postponed goal (left); then the instance that shows the witness (right).

1	$\forall x R(x, x)$			1	$\forall x R(x, x)$		
	$x_0 \mid \vdots$				$x_0 \mid \vdots$		
2	$\exists y R(x_0, y)$		?	2	$x_0 \mid R(x_0, x_0)$	$\forall E$ 1	
	$\vdots$				$\vdots$		
3	$\forall x \exists y R(x, y)$		?	3	$\exists y R(x_0, y)$		?
4	$\forall x \exists y R(x, y)$		?	4	$\forall x \exists y R(x, y)$		?

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

Line 3 uses $\varphi = R(x_0, y)$, the variable y , and the witness x_0 ; it marks the second occurrence of x_0 and keeps the first. Line 4 is $\forall I$ with the flag x_0 (Definition 5.4.1): x_0 appears in no premise, there is no open assumption, and x_0 does not appear in line 4. The $\exists I$ inside the box needed no box of its own, although its witness is a fresh name. Read over $\mathbb{N}$ with $R(x, y)$ as “ $x \leq y$ ”: every number is at most itself, so every number is at most something.

- (d) *Idea.* The goal $\exists y Q(y)$ is an existential, and no line yet has the form $Q(t)$. Postpone,

and work forwards. The premise $\forall x (\dots)$ is a $\forall$; the only term in sight is c , so instantiate at c (Section 5.3), and $\rightarrow E$ with the premise $P(c)$ fires. The result $Q(f(c))$ shows the witness: the compound term $f(c)$. In the Givens/Goal table:

Givens	Goal
$\forall x (P(x) \rightarrow Q(f(x))), P(c)$	$\exists y Q(y)$: postponed, no instance yet
$+ P(c) \rightarrow Q(f(c))$ ($\forall E$ at c)	$\exists y Q(y)$
$+ Q(f(c))$ ($\rightarrow E$)	$\exists y Q(y) \checkmark$ by $\exists I$, witness $f(c)$

The postponed goal (left); then the two forward steps, after which the witness is visible (right).

1	$\forall x (P(x) \rightarrow Q(f(x)))$		1	$\forall x (P(x) \rightarrow Q(f(x)))$	
2	$P(c)$		2	$P(c)$	
	$\vdots$		3	$P(c) \rightarrow Q(f(c))$	$\forall E 1$
	$\vdots$		4	$Q(f(c))$	$\rightarrow E 3, 2$
5	$\exists y Q(y)$	?	5	$\exists y Q(y)$	?

1	$\forall x (P(x) \rightarrow Q(f(x)))$	
2	$P(c)$	
3	$P(c) \rightarrow Q(f(c))$	$\forall E 1$
4	$Q(f(c))$	$\rightarrow E 3, 2$
5	$\exists y Q(y)$	$\exists I 4$

Line 5 uses $\varphi = Q(y)$ and $t = f(c)$. Now see what choosing the witness first would have done. The term in sight at the start is c , and “take $y = c$ ” leaves the goal $Q(c)$. Nothing gives it: the premise speaks of Q only at terms of the form $f(\dots)$, and $Q(c)$ need not hold at all. Read over $\mathbb{Z}$ with P as “odd”, Q as “even”, $f(x)$ as $x + 1$, and c as 3: the premises say that the successor of every odd integer is even and that 3 is odd, the conclusion says that some integer is even, and the witness the derivation finds is $f(3) = 4$, while $Q(c)$ says that 3 is even. The search stalls exactly because it chose the witness before the derivation had produced it.

The four Ideas share a pattern. In (a) and (b) the witness stood on a premise line from the start; in (c) and (d) it appeared only after other rules had run, and in (d) it was a term that no line mentioned at the start. Postponing costs nothing in (a) to (c), where the right witness was already a term in sight when the existential goal appeared (in (c) the goal names x_0), and it is necessary in (d), where the only term in sight at the start, c , is the wrong witness.

5.5.5 How this rule looks in a mathematical proof

In a written proof, $\exists I$ is the word “take”, followed by a check. “6 is even: take $k = 3$; then $6 = 2 \cdot 3$.” Over $\mathbb{Z}$, with one line of school arithmetic justified “arith” as in Section 5.3:

1	$6 = 2 \cdot 3$	arith
2	$\exists k (6 = 2 \cdot k)$	$\exists I$ 1

Line 2 marks the 3 with k , and keeps the 6 and the 2: $\varphi = (6 = 2 \cdot k)$. In the same way “7 is odd: take $k = 3$, since $7 = 2 \cdot 3 + 1$ ” is an $\exists I$ with $\varphi = (7 = 2 \cdot k + 1)$.

A bounded witness. Analysis states its existentials with bounds. “There is an $N \in \mathbb{N}$ with $1/(N + 1) < 1/100$ ” abbreviates $\exists N (N \in \mathbb{N} \wedge 1/(N + 1) < 1/100)$ (Definition 5.1.1), so the witness must satisfy both conjuncts. Taking $N = 100$ is two steps: $\wedge I$ puts the bound and the inequality together, and $\exists I$ forgets the witness.

1	$100 \in \mathbb{N}$	arith
2	$1/(100 + 1) < 1/100$	arith
3	$100 \in \mathbb{N} \wedge 1/(100 + 1) < 1/100$	$\wedge I$ 1, 2
4	$\exists N (N \in \mathbb{N} \wedge 1/(N + 1) < 1/100)$	$\exists I$ 3

Line 4 marks two of the three occurrences of 100 in line 3 and keeps the one on the right. The witness 100 is the least that works, since $N = 99$ gives $1/100$, which is not less than $1/100$; but the proof does not need the least witness, only one.

A witness built from what is available. Often the witness is a term made from other names. To show that for every integer n there is an odd integer greater than $2n$, a proof says “let n be an integer; $2n + 1$ will do, since it is odd and greater than $2n$ ”. The words “let n be an integer” open the flagged box of Section 5.4, and “ $2n + 1$ will do” is $\exists I$ with the compound witness $2n + 1$, as in (d) above. In general, the witness may be any term the reader can check.

Warning. $\exists I$ runs one way only. From $P(c)$ it gives $\exists x P(x)$; from $\exists x P(x)$ it gives nothing, and in particular not $P(c)$. “Some integer is even” is true and “3 is even” is false: the existential does not say **which** object has the property, so it cannot be read back as a statement about a named one. Using an existential takes a rule of its own, with a box, and that is Section 5.6.

5.5.6 The rule card

Before the card, the rule at work on lines larger than $R(c, c)$. The schema sees the cited line as $\varphi[t/x]$ however much is inside t and φ .

Example. Instances of $\exists I$

Cited line	φ	Witness t	New line
$P(f(f(c))) \wedge Q(f(c))$	$P(f(x)) \wedge Q(x)$	$f(c)$	$\exists x (P(f(x)) \wedge Q(x))$
$ a - b < \varepsilon/2$	$ a - b < \delta$	$\varepsilon/2$	$\exists \delta (a - b < \delta)$
$(n + 1) \cdot (n + 1) =$ $n \cdot n + 2 \cdot n + 1$	$m \cdot m = n \cdot n + 2 \cdot n + 1$	$n + 1$	$\exists m (m \cdot m =$ $n \cdot n + 2 \cdot n + 1)$

In each row $\varphi[t/x]$ is exactly the cited line, and the marked places are whole occurrences of t (in the third, both factors on the left; the n ’s on the right are not occurrences of $n + 1$, and they stay).

Not an instance. From $P(c) \wedge Q(d)$, the line $\exists x (P(x) \wedge Q(x))$ is not written by $\exists\text{I}$: $\varphi[t/x]$ puts **one** term in every marked place, and no single t turns $P(x) \wedge Q(x)$ into $P(c) \wedge Q(d)$.

Quick check. Line 1 is $Q(g(c), c)$. Write the $\exists\text{I}$ line with the witness c that marks only the c inside $g(c)$, and name its φ .

Solution. $\exists x Q(g(x), c)$, with $\varphi = Q(g(x), c)$; $\varphi[c/x]$ is line 1.

Chapters 1 and 2’s thirteen rules are on the card at the end of Section 3.1; here are this chapter’s so far. Nothing later depends on the last column, and Section 5.7 collects the whole table.

Rule	Shape	Side condition	You write	Lean
$\forall\text{E}$	$\forall x \varphi \implies \varphi[t/x]$	t free for x in φ	“In particular, for $x = t, \dots$ ”; “applying the hypothesis to $t, \dots$ ”	h t (or specialize h t)
$\forall\text{I}$	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
$\exists\text{I}$	$\varphi[t/x] \implies \exists x \varphi$	t free for x in φ	“Take $x = t$. Then ...”; “ $2k + 1$ will do.”	use t (or Exists.intro t h)

The phrase names the witness and then checks it. A proof that names the witness without the check (“take $N = 100$.”) has written the line $\exists x \varphi$ without the instance $\varphi[t/x]$ it cites; the reader must supply the instance, and should be able to.

In the Givens/Goal table, $\exists\text{I}$ ticks off the goal $\exists x \varphi$ once a Given is an instance $\varphi[t/x]$; until then the goal row waits.

Warning (Not allowed: $\exists\text{I}$). Each step is offered as one application of $\exists\text{I}$; each breaks the rule where shown.

- “From $P(c) \wedge Q(d)$, write $\exists x (P(x) \wedge Q(x))$ ”: the cited line must be exactly $\varphi[t/x]$, with one term t in every marked place.
- “From $\forall y (y < y + 1)$, write $\exists x \forall y (y < x)$ ”: the side condition; the witness $y + 1$ is not free for x in $\forall y (y < x)$.
- “From $P(t)$, write $\exists x \in A P(x)$ ”: the cited line must be the instance; the bounded form is $\exists x (x \in A \wedge P(x))$, whose instance is $t \in A \wedge P(t)$ (“A bounded witness”).

The search method: one more step. Each rule section adds a step to the method of Section 3.1.

- **Goal $\exists x \varphi$.** Postpone. Work on the premises and on other goals until an available line is an instance $\varphi[t/x]$, with t free for x in φ ; then $\exists I$. The witness may be a compound term that appears only after other rules have run, as $f(c)$ did in (d).

5.5.7 Exercises

5.5.7.1 A. Check your understanding

Exercise. A1

- State $\exists I$ as a schema, with its side condition.
- Line 1 of a derivation is $R(c, f(c))$. Which of the following may line 2 be, by one application of $\exists I$ to line 1? For each that may, give φ and the witness t ; for each that may not, say why.
 - $\exists x R(x, f(c))$; (ii) $\exists x R(c, x)$; (iii) $\exists x R(x, f(x))$; (iv) $\exists x R(x, x)$; (v) $\exists x R(f(c), x)$.
- Line 1 of a derivation is $\forall y (y \leq y \cdot y)$. Is $\exists x \forall y (y \leq x \cdot x)$ a legal $\exists I$ step from line 1? Read both lines over $\mathbb{Z}$: which is true?
- True or false, with a reason: from the line $\exists x P(x)$, one application of $\exists I$ gives $P(c)$.
- The current goal of a search is $\exists x \varphi$ and no available line is an instance of φ . What does the search method say to do, and why not choose a witness now?

Solution. (a) From $\varphi[t/x]$ on an available line i , write $\exists x \varphi$ on line k , justified “ $\exists I i$ ”. Side condition: t is free for x in φ .

(b) (i) Yes: $\varphi = R(x, f(c))$, $t = c$; only the first c is marked. (ii) Yes: $\varphi = R(c, x)$, $t = f(c)$; the witness is the compound term. (iii) Yes: $\varphi = R(x, f(x))$, $t = c$; both occurrences of c are marked, and $\varphi[c/x]$ is $R(c, f(c))$. (iv) No: the conclusion fixes $\varphi = R(x, x)$, whose instances $R(t, t)$ have equal arguments, while the arguments c and $f(c)$ of line 1 differ. (v) No: the conclusion fixes $\varphi = R(f(c), x)$, whose instances $R(f(c), t)$ have $f(c)$ as first argument, while line 1 has c there. (Read over $\mathbb{N}$ with $R(x, y)$ as “ $x < y$ ”, $f(x)$ as $x + 1$, and c as 0: line 1 says $0 < 1$, and (v) says that something exceeds 1, true but not by this step; (iv) says that some number is less than itself, which is false.)

(c) No. With $\varphi = \forall y (y \leq x \cdot x)$, the formula $\varphi[y/x]$ is line 1, so the witness would be the variable y ; but the free occurrences of x in φ lie in the scope of $\forall y$, so y is not free for x in φ . Over $\mathbb{Z}$, line 1 is true: for $y \leq 0$, $y \leq 0 \leq y \cdot y$, and for $y \geq 1$, $y \leq y \cdot y$ after multiplying $1 \leq y$ by $y > 0$. The other line is false: whatever integer x is proposed, $y = x \cdot x + 1$ gives $y > x \cdot x$. So the step would lead from a true line to a false one, which is what the side condition prevents.

(d) False. $\exists I$ concludes an existential from an instance; it never concludes an instance. The line $P(c)$ does not follow from $\exists x P(x)$ at all: over $\mathbb{Z}$ with P as “even” and c as 3, the first is true and the second false.

(e) Postpone the goal: work on the premises ($\forall E$ at the terms the goal mentions, $\rightarrow E$, and so on) until a line $\varphi[t/x]$ appears, then use $\exists I$. A witness chosen now leaves the goal $\varphi[t/x]$,

which may not follow from the resources even when $\exists x \varphi$ does, as “take $y = c$ ” did in [Example \(Derivations with existential introduction\)](#) (d).

Exercise. A2: Drill

Each part takes a line or two. The parts run from single steps, through a missing line, a justification column and steps to judge, to short derivations.

- (a) Line 1 is $3 + 4 = 7$. Name φ and t so that $\exists I$ gives $\exists x (x + 4 = 7)$.
- (b) Line 2 is $c + c = 2 \cdot c$. Write the $\exists I$ lines with the witness c that mark (i) all three occurrences of c , (ii) the two on the left only.
- (c) Line 1 is $P(f(c))$. Give two different $\exists I$ conclusions.
- (d) Line 5 is $\exists y (y > x_0 + 1)$, justified “ $\exists I$ 4”. Give two possible lines 4, with their witnesses.
- (e) Justify each line: 1 $\forall x (P(x) \rightarrow Q(f(x)))$, premise; 2 $P(c)$, premise; 3 $P(c) \rightarrow Q(f(c))$; 4 $Q(f(c))$; 5 $P(c) \wedge Q(f(c))$; 6 $\exists x (P(x) \wedge Q(f(x)))$.
- (f) Line 1 is $R(c, c)$. Which of $\exists x R(x, c)$, $\exists x R(c, x)$, $\exists x R(x, y)$ can one $\exists I$ **not** give?
- (g) Line 1 is $\forall y (y = y)$. Is $\exists x \forall y (x = y)$ a legal $\exists I$ line?
- (h) True or false: $\exists I$ may cite $\exists x P(x)$ and write $P(c)$.
- (i) Premises $P(a)$, $Q(b)$; goal $\exists x (P(x) \wedge Q(x))$. Should a witness be chosen now?
- (j) Derive $P(c) \vdash \exists x (P(x) \vee Q(x))$.
- (k) Derive $\forall x P(x) \vdash \exists x P(f(x))$.
- (l) Derive $\forall x \forall y R(x, y) \vdash \exists x \exists y R(y, x)$.

Solution.

- (a) $\varphi = (x + 4 = 7)$, $t = 3$.
- (b) (i) $\exists x (x + x = 2 \cdot x)$; (ii) $\exists x (x + x = 2 \cdot c)$.
- (c) $\exists x P(x)$ (witness $f(c)$) and $\exists x P(f(x))$ (witness c).
- (d) Any line $t > x_0 + 1$ with t free for y (every term is, since the formula has no quantifier): for example $x_0 + 2 > x_0 + 1$ (witness $x_0 + 2$) or $7 > x_0 + 1$ (witness 7).
- (e) 3 $\forall E$ 1 (at c); 4 $\rightarrow E$ 3, 2; 5 $\wedge I$ 2, 4; 6 $\exists I$ 5 (witness c , marking the c of $P(c)$ and the one inside $f(c)$).
- (f) $\exists x R(x, y)$: its instances $R(t, y)$ have y in the second place, and line 1 has c .
- (g) No: the witness would be y , which $\forall y$ captures. Over $\mathbb{Z}$ line 1 is true and the other line, “some integer equals every integer”, false.
- (h) False: $\exists I$ goes from an instance to an existential, never back.
- (i) No: neither a nor b has both properties on a line. In fact a counter-reading exists: the domain $\{a, b\}$, with P true of a only and Q of b only.
- (j) 2 $P(c) \vee Q(c)$, $\forall I$ 1; 3 $\exists x (P(x) \vee Q(x))$, $\exists I$ 2.
- (k) 2 $P(f(x))$, $\forall E$ 1 (at the term $f(x)$); 3 $\exists x P(f(x))$, $\exists I$ 2 (with $\varphi = P(f(x))$ and the witness x).
- (l) 1 $\forall y R(x, y)$, $\forall E$ 1 (at x); 3 $R(x, x)$, $\forall E$ 2; 4 $\exists y R(y, x)$, $\exists I$ 3 (witness x , marking the first place); 5 $\exists x \exists y R(y, x)$, $\exists I$ 4 (witness x).

5.5.7.2 B. Practice

Exercise. B1: Postpone, then choose

A search for $\forall x (P(x) \rightarrow Q(x))$, $P(a) \vdash \exists x (P(x) \wedge Q(x))$ has reached the stage below. *Name the move, then complete it, saying for each line whether the goal or a premise chose it.*

1		$\forall x (P(x) \rightarrow Q(x))$	
2		$P(a)$	
		$\vdots$	
6		$\exists x (P(x) \wedge Q(x))$	?

Solution. The move is *postpone the witness*.

Idea. The goal is an existential: postpone it. The premise $\forall x (\dots)$ is instantiated at the only term in sight, a , and $\rightarrow E$ with $P(a)$ gives $Q(a)$; both steps are premise-directed. Now the witness a is visible, and the instance the goal needs is $P(a) \wedge Q(a)$, which $\wedge I$ builds. The last step is the postponed $\exists I$.

1		$\forall x (P(x) \rightarrow Q(x))$	
2		$P(a)$	
3		$P(a) \rightarrow Q(a)$	$\forall E$ 1
4		$Q(a)$	$\rightarrow E$ 3, 2
5		$P(a) \wedge Q(a)$	$\wedge I$ 2, 4
6		$\exists x (P(x) \wedge Q(x))$	$\exists I$ 5

Line 6 uses $\varphi = P(x) \wedge Q(x)$ and the witness a .

Exercise. B2

Over $\mathbb{R}$, with the premise $\forall x (x + (-x) = 0)$, derive $\forall x \exists y (x + y = 0)$, the true sentence (i) of Example (Swapping two quantifiers). Say what the witness is, and what it depends on.

Solution. Idea. The goal is a $\forall$: open a flagged box with a fresh name x_0 (Section 5.4); the new goal is $\exists y (x_0 + y = 0)$. Postpone it, and instantiate the premise at the term the goal mentions, x_0 . The line $x_0 + (-x_0) = 0$ shows the witness: $-x_0$.

1		$\forall x (x + (-x) = 0)$	
2		$x_0 + (-x_0) = 0$	$\forall E$ 1
3		$\exists y (x_0 + y = 0)$	$\exists I$ 2
4		$\forall x \exists y (x + y = 0)$	$\forall I$ 2–3

Line 3 uses $\varphi = (x_0 + y = 0)$ and the witness $-x_0$, which contains no variable bound in φ . At line 4, x_0 appears in no premise, there is no open assumption, and x_0 does not appear in the conclusion, so $\forall I$ applies (Definition 5.4.1).

The witness $-x_0$ is built from x_0 , so it depends on x_0 : a different number for each x . That is legal, because $\exists I$ is applied **inside** the box, where x_0 is available as a term. It is the box picture of the game of Section 5.1: the $\exists y$ is played after the $\forall x$, and may use it.

Exercise. B3

Over $\mathbb{Z}$, prove “there is an integer n with $n^2 = n + 2$ ” as a derivation whose only line not justified by a rule is one line of arithmetic justified “arith”; write n^2 as $n \cdot n$. Then write the proof as one sentence.

Solution. The witness 2 works, since $2 \cdot 2 = 4 = 2 + 2$.

1	$2 \cdot 2 = 2 + 2$	arith
2	$\exists n (n \cdot n = n + 2)$	$\exists I$ 1

Line 2 uses $\varphi = (n \cdot n = n + 2)$ with the witness 2. Line 1 contains four 2’s, and φ marks three of them: both factors on the left and the first term of the sum on the right. The last 2 is the constant of the statement and stays. Marking all four would give $\exists n (n \cdot n = n + n)$, a different statement.

In one sentence: *Take $n = 2$; then $n^2 = 4 = n + 2$.*

The witness -1 works too, since $(-1) \cdot (-1) = 1 = -1 + 2$; a proof needs only one.

Exercise. B4: Derive or break

For each claim, derive it with the rules of Chapters 1–2, $\forall E$, $\forall I$ and $\exists I$, or break it with a counter-reading (Section 5.3).

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

Solution.

- (a) Derive. Instantiate at the variable x , weaken, and forget the witness.

1	$\forall x P(x)$	
2	$P(x)$	$\forall E$ 1
3	$P(x) \vee Q(x)$	$\vee I$ 2
4	$\exists x (P(x) \vee Q(x))$	$\exists I$ 3

Line 4 uses $\varphi = P(x) \vee Q(x)$ and the witness x .

- (b) Break. The domain $\{0, 1\}$, with P true of 0 only. The premise holds (at 0), and the conclusion fails at 1.
- (c) Break. The domain $\{0, 1\}$, with c naming 0, d naming 1, and R true of the pairs $(0, 1)$ and $(1, 0)$ only. The premise holds, and no element is related to itself.
- (d) Derive. Two witnesses, one for each place, forgotten one at a time.

1	$R(c, d) \wedge R(d, c)$	
2	$\exists y (R(c, y) \wedge R(y, c))$	$\exists I$ 1
3	$\exists x \exists y (R(x, y) \wedge R(y, x))$	$\exists I$ 2

Line 2 uses $\varphi = R(c, y) \wedge R(y, c)$ and the witness d ; line 3 uses $\varphi = \exists y (R(x, y) \wedge R(y, x))$ and the witness c , which is free for x since it is a constant.

- (e) Derive. Fix x_0 first; the witness $f(x_0)$ is found after the flag.

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

At line 4, x_0 appears in no premise, no box is open, and x_0 is not in line 4.

- (f) Break. The domain $\{0, 1\}$, with f the identity ($f(0) = 0$, $f(1) = 1$) and R true of $(0, 0)$ and $(1, 1)$ only. The premise holds, since each element is related to itself; and no y has both $R(0, y)$ and $R(1, y)$.
- (g) Derive. A box with its assumption as its only line, then $\exists I$ at the variable x .

1	$\boxed{P(x)}$	asm, for $\rightarrow I$
2	$P(x) \rightarrow P(x)$	$\rightarrow I$ 1–1
3	$\exists x (P(x) \rightarrow P(x))$	$\exists I$ 2

Line 3 has the witness x ; the variable names an object, since domains are not empty (Section 5.1).

The pairs: (c) and (d) are look-alikes (one witness for both places, against two witnesses); (e) and (f) differ only in the order of $\forall$ and $\exists$, the swap of Section 5.1, and the witness $f(x_0)$ in (e) depends on the flag; (b) is the converse of [Proposition 5.5.1](#). Worked examples of these types: [Example \(Derivations with existential introduction\)](#); [Proposition 5.5.1](#).

Marking scheme. (10 points)

- 1 each: (a), (b), (c), (d), (f), (g), with the derivation or the counter-reading in full.
- 2: (e), with the flag opened first and the witness $f(x_0)$ found after it.
- 2: the closing pairing.

Fatal errors (0 for the claim): an $\exists$ I whose witness is not free for the variable; a “break” in which the premise is false.

5.5.7.3 C. Going deeper

Exercise. C1: The conclusion clause of for-all-introduction, used later

The side condition of $\forall$ I (Definition 5.4.1) has three clauses about the flag x_0 : it appears in no premise, in no assumption of a box still open at the $\forall$ I line, and not in the conclusion $\forall x \varphi$. Show that the third clause is needed: give a “derivation” that breaks **only** that clause, from a premise that is true over $\mathbb{N}$ to a sentence (Definition 5.2.4) that is false over $\mathbb{N}$. Check that every other step is legal.

Solution (Hint 1). The conclusion of the illegal $\forall$ I still mentions the flag, so it is not yet a sentence. Which rule of this section can replace a name on a line by a bound variable?

Solution (Hint 2). Start from the premise $\forall x (x \leq x)$, and open a flagged box with the name y_0 .

Solution.

1	$\forall x (x \leq x)$	
2	$y_0 \mid y_0 \leq y_0$	$\forall$ E 1
3	$\forall x (x \leq y_0)$	$\forall$ I 2–2
4	$\exists y \forall x (x \leq y)$	$\exists$ I 3

The illegal line. Line 3 is $\forall$ I with the flag y_0 and $\varphi = (x \leq y_0)$: the instance $\varphi[y_0/x]$ is $y_0 \leq y_0$, the last line of the box. The flag y_0 appears in no premise (line 1 has no y_0), and there is no open assumption at all. But y_0 appears in the conclusion $\forall x (x \leq y_0)$, so the third clause fails, and only it.

The other lines are legal. Line 2 is $\forall$ E at the term y_0 , which is free for x in $x \leq x$ since that formula has no quantifier. Line 4 is $\exists$ I with $\varphi = \forall x (x \leq y)$ and the witness y_0 : $\varphi[y_0/y]$ is line 3, and y_0 is free for y in φ , since the only quantifier of φ is on x .

Over $\mathbb{N}$. Line 1 says that every natural number is at most itself: true. Line 4 says that some natural number is at least every natural number, that is, that there is a largest natural number: false, since for any y , $x = y + 1$ is larger.

What the clause prevents. The box proved $y_0 \leq y_0$, a fact about y_0 in which the two sides are the same name. Line 3 generalized only one side and kept the other, so it claimed that **one** fixed y_0 is at least every x : a claim about y_0 that the box never proved. The flag is “let y_0 be arbitrary”; it must not survive into the statement that “since y_0 was arbitrary” produces. Line 4 then shows the damage, by turning the leaked name into a witness.

Marking scheme. (10 points) - 3: a derivation whose only illegal line is a $\forall$ I whose flag

appears in its conclusion. - 2: checks the other two clauses at that line (no premise, no open assumption contains the flag). - 2: checks the remaining lines (here $\forall E$ and $\exists I$, with free-for). - 3: shows the premise true and the conclusion false over $\mathbb{N}$, with the witness of the falsity ($y + 1$). Fatal errors (0 for the step): a second illegal line (for instance a capture in $\exists I$); a premise that is false over $\mathbb{N}$.

Exercise. C2: A witness is not a name, used later

Explain why the rules so far (Chapters 1–2 and $\forall E$, $\forall I$, $\exists I$) cannot derive $\exists x P(x) \vdash P(c)$. Go through the rules that could produce the last line $P(c)$, and say what each would need. Then say, in one sentence, why no rule for using $\exists$ **should** give $P(c)$.

Solution. The argument below is informal: it explains why every search stalls, and it does not by itself prove that no derivation exists. Section 7.2 gives a model in which the premise is true and $P(c)$ is false. With the soundness theorem stated there (and proved in the optional Section 7.3), that model shows no derivation exists.

Which rules could write $P(c)$. The line $P(c)$ is atomic, so no introduction rule writes it: $\wedge I$, $\rightarrow I$, $\vee I$, $\neg I$, $\leftrightarrow I$, $\forall I$ and $\exists I$ all write a line whose main symbol is their own connective or quantifier. The remaining rules take $P(c)$ out of something larger: $\wedge E$ needs a conjunction with $P(c)$ as a side; $\rightarrow E$ needs an implication $\psi \rightarrow P(c)$ and ψ ; $\leftrightarrow E$ a biconditional with $P(c)$ as a side; $\vee E$ a disjunction and two boxes each ending in $P(c)$; $\forall E$ a universal $\forall x \psi$ with $\psi[c/x] = P(c)$; $\neg E$ writes only $\perp$, never $P(c)$; $\perp E$ the line $\perp$; RAA a box from $\neg P(c)$ to $\perp$; and R the line $P(c)$ itself.

The derived rules of Chapter 2 abbreviate derivations in these rules (Definition 2.3.1), so they add no new way to write $P(c)$.

What the premise can supply. The only premise is $\exists x P(x)$, whose main symbol is $\exists$. No rule so far looks inside an existential: each elimination rule needs a cited line that is $\perp$ (for $\perp E$) or whose main symbol is $\wedge$, $\rightarrow$, $\vee$, $\leftrightarrow$, $\neg$ or $\forall$, and $\exists I$ produces existentials rather than using them. So the premise can enter a derivation only as a whole: copied, built into a larger formula, set against a line $\neg \exists x P(x)$ by $\neg E$, or cited as the side ψ beside a line $\psi \rightarrow \chi$ or $\psi \leftrightarrow \chi$ by $\rightarrow E$ or $\leftrightarrow E$. None of these reaches the information inside it, and the lines the rules above need (a conjunction containing $P(c)$, an implication ending in it, a biconditional with it as a side, a disjunction for $\vee E$, a universal with it as an instance, a contradiction) have nowhere to come from. A search therefore stalls at once.

Why it should stall. The premise says that **something** has P and does not say what; the conclusion says that the object named c has P . Over $\mathbb{Z}$ with P as “even” and c as 3, the premise is true and the conclusion false. So no rule for using an existential may give $P(c)$, and the rule of Section 5.6 does not: it names the witness with a **fresh** variable, about which nothing else is known, instead of with c .

Marking scheme. (10 points) - 3: identifies that $P(c)$ is atomic, so only elimination rules, $\perp E$, RAA or R can write it, and names what each needs. - 3: observes that no rule so far uses a line whose main symbol is $\exists$, so the premise cannot supply what those rules need. - 2: says that this explains the stall but is not a proof of non-derivability (that needs a counter-model together with soundness, Sections 7.2–7.3). - 2: gives a reading with the premise true and $P(c)$ false, and the one-sentence reason (the premise does not say which object has P). Fatal

errors (0 for the step): claiming that $\exists I$ read backwards gives $P(c)$; claiming that a failed search proves the sequent underivable.