

CSE 311 Lecture 08: Inference Rules and Proofs for Predicate Logic

Emina Torlak and Kevin Zatloukal

Topics

Propositional logic proofs

A brief review of Lecture 07.

A quick look at predicate logic proofs

Inference rules for quantifiers and a "hello" world example.

An in-depth look at predicate logic proofs

Understanding rules for quantifiers through more advanced examples.

Propositional logic proofs

A brief review of Lecture 07.

Inference rules for propositional logic

Two rules per binary connective: to eliminate and introduce it.

Intro
$$\wedge$$
 $A; B$ Intro \vee A Direct Proof Rule $A \implies B$ $\therefore A \land B$ $\therefore A \lor B, B \lor A$ \square \square \square $A \implies B$ Elim \wedge $A \land B$ \square $A \lor B; \neg A$ \square \square $\therefore A, B$ \square \square \square \square \square

Direct Proof Rule is special: not like the other rules.

Proving implications with the direct proof rule

Direct Proof Rule
$$\frac{A \implies B}{\therefore A \rightarrow B}$$

The premise $A \implies B$ means "Given A, we can prove B."

So the direct proof rule says that if we have such a proof, then we can conclude that $A \rightarrow B$ is true.

Proving implications with the direct proof rule

Direct Proof Rule
$$\frac{A \implies B}{\therefore A \rightarrow B}$$

The premise $A \implies B$ means "Given A, we can prove B."

So the direct proof rule says that if we have such a proof, then we can conclude that $A \rightarrow B$ is true.

Example: prove
$$(p \land q) \rightarrow (p \lor q)$$
.

1.1. $p \wedge q$	Assumption
1.2. <i>p</i>	
1.3. $p \lor q$	

2. $(p \land q) \rightarrow (p \lor q)$ Direct Proof Rule

- Indent the proof subroutine.
- Write the assumption and the goal.

Proving implications with the direct proof rule

Direct Proof Rule
$$\frac{A \implies B}{\therefore A \rightarrow B}$$

The premise $A \implies B$ means "Given A, we can prove B."

So the direct proof rule says that if we have such a proof, then we can conclude that $A \rightarrow B$ is true.

Example: prove $(p \land q) \rightarrow (p \lor q)$.

1.1. $p \wedge q$	Assumption
1.2. <i>p</i>	Elim ∧: 1.1
1.3. <i>p</i> ∨ <i>q</i>	Intro V: 1.2

- Indent the proof subroutine.
- Write the assumption and the goal.
- Fill in the steps.

2. $(p \land q) \rightarrow (p \lor q)$ Direct Proof Rule

Inference rules let us derive facts that are *implied* by the existing facts.

Inference rules let us derive facts that are *implied* by the existing facts.

So, for every rule
$$\frac{P}{\therefore Q}$$
, $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$).

Inference rules let us derive facts that are *implied* by the existing facts.

So, for every rule
$$\frac{P}{\therefore Q}$$
, $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$).

The proof $P \implies Q$ shows that $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$), since it just a series of implications that we know are tautologies.

Inference rules let us derive facts that are *implied* by the existing facts.

So, for every rule
$$\frac{P}{\therefore Q}$$
, $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$).

The proof $P \implies Q$ shows that $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$), since it just a series of implications that we know are tautologies.

So the Direct Proof Rule $\frac{A \implies B}{\therefore A \rightarrow B}$ says that we can add $A \rightarrow B$ to our set of facts, if we can show that $A \rightarrow B$ is a tautology.

Inference rules let us derive facts that are *implied* by the existing facts.

So, for every rule
$$\frac{P}{\therefore Q}$$
, $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$).

The proof $P \implies Q$ shows that $P \rightarrow Q$ is a tautology ($P \rightarrow Q \equiv T$), since it just a series of implications that we know are tautologies.

So the Direct Proof Rule
$$\frac{A \implies B}{\therefore A \rightarrow B}$$
 says that we can add $A \rightarrow B$ to

our set of facts, if we can show that $A \rightarrow B$ is a tautology.

One way to show that $A \rightarrow B \equiv T$ is by writing a subproof, using all the facts we have inferred up to that point.

 $\mathsf{Prove}\left((p \to q) \land (q \to r)\right) \to (p \to r).$

Prove
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
.
1.1. $(p \rightarrow q) \land (q \rightarrow r)$ Assumption
1.2.
1.3.

1.5. $p \rightarrow r$

2.
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
 Direct
Proof
Rule

• Write the premise and the conclusion.

Prove
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
.

1.1. $(p \rightarrow q) \land (q \rightarrow r)$ 1.2. $p \rightarrow q$ 1.3. $q \rightarrow r$

Assumption Elim ∧: 1.1 Elim ∧: 1.1

- Write the premise and the conclusion.
- Work forwards and backwards.
 - We'll need parts of 1.1 so Elim ∧ to get 1.2, 1.3.

1.5. $p \rightarrow r$

2.
$$((p \to q) \land (q \to r)) \to (p \to r)$$
 Di
Pr

Direct Proof Rule

Prove
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
.

1.1. $(p \to q)$	$\wedge (q \rightarrow r)$	Assumption
1.2. $p \rightarrow q$		Elim ∧: 1.1
1.3. $q \rightarrow r$		Elim ∧: 1.1
1.4.1. <i>p</i>	Assumption	

- 1.4.2.
- 1.4.3. *r*
- 1.5. $p \rightarrow r$ Direct Proof Rule

2.
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
 Direct
Proof
Rule

- Write the premise and the conclusion.
- Work forwards and backwards.
 - We'll need parts of 1.1 so Elim ∧ to get 1.2, 1.3.
 - We can use DPR to get 1.5.

Prove
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
.

1.1. $(p \to q) \land (q \to r)$	Assumption
1.2. $p \rightarrow q$	Elim ∧: 1.1
1.3. $q \rightarrow r$	Elim ∧: 1.1

 1.4.1. p
 Assumption

 1.4.2. q
 MP: 1.2, 1.4.1

 1.4.3. r

1.5. $p \rightarrow r$ Direct Proof Rule

2.
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
 Direct
Proof
Rule

- Write the premise and the conclusion.
- Work forwards and backwards.
 - We'll need parts of 1.1 so Elim ∧ to get 1.2, 1.3.
 - We can use DPR to get 1.5.
 - Using MP on 1.2, 1.4.1 gives us 1.4.2.

Prove
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
.

Assumption
Elim ∧: 1.1
Elim ∧: 1.1

1.4.1. pAssumption1.4.2. qMP: 1.2, 1.4.11.4.3. rMP: 1.3, 1.4.2

1.5. $p \rightarrow r$ Direct Proof Rule

2.
$$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$$
 Direct
Proof
Rule

- Write the premise and the conclusion.
- Work forwards and backwards.
 - We'll need parts of 1.1 so Elim ∧ to get 1.2, 1.3.
 - We can use DPR to get 1.5.
 - Using MP on 1.2, 1.4.1 gives us 1.4.2.
 - Using MP on 1.3, 1.4.2 gives us 1.4.3.

1.1. $(p \rightarrow q) \land (q \rightarrow r)$ 1.2. $p \rightarrow q$	Assumption Elim ∧: 1.1
1.3. $q \rightarrow r$	Elim ∧: 1.1
1.4.1. p Assumption 1.4.2. q MP: 1.2, 1.4.1 1.4.3. r MP: 1.3, 1.4.2 1.5. $p \rightarrow r$ Direct Proof	
2. $((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (q \rightarrow r))$	$p \rightarrow r$) Direct Proof Rule

 A line k in a (sub)proof can use a fact at line i if the set of assumptions and givens that k is derived from contains all the assumptions and givens that i is derived from.

1.1. $(p \rightarrow q) \land$ 1.2. $p \rightarrow q$ 1.3. $q \rightarrow r$	Elim	mption ∧: 1.1 ∧: 1.1
1.4.2. q M 1.4.3. r M	ssumption IP: 1.2, 1.4.1 IP: 1.3, 1.4.2 Direct Proof Rule	
2. $((p \rightarrow q) \land (q$	$\rightarrow r)) \rightarrow (p \rightarrow r)$	r) Direct Proof Rule

- A line k in a (sub)proof can use a fact at line i if the set of assumptions and givens that k is derived from contains all the assumptions and givens that i is derived from.
- So, 1.4.2 can use 1.2 because they are derived from the assumptions {1.1, 1.4.1} and {1.1}, respectively.

1.1. $(p \rightarrow q) \land (q \rightarrow r)$ Assume1.2. $p \rightarrow q$ Elim \land 1.3. $q \rightarrow r$ Elim \land	: 1.1
1.4.1. p Assumption 1.4.2. q MP: 1.2, 1.4.1 1.4.3. r MP: 1.3, 1.4.2 1.5. $p \rightarrow r$ Direct Proof Rule	
2. $((p \to q) \land (q \to r)) \to (p \to r)$	Direct Proof Rule

- A line k in a (sub)proof can use a fact at line i if the set of assumptions and givens that k is derived from contains all the assumptions and givens that i is derived from.
- So, 1.4.2 can use 1.2 because they are derived from the assumptions {1.1, 1.4.1} and {1.1}, respectively.
- Can 1.5 use 1.4.3?

1.1. $(p \rightarrow q) \land (q)$ 1.2. $p \rightarrow q$ 1.3. $q \rightarrow r$	$ \rightarrow r) $ Assumption Elim \wedge : 1.1 Elim \wedge : 1.1
1.4.2. q MP: 1	mption 1.2, 1.4.1 1.3, 1.4.2 oct Proof Rule
2. $((p \rightarrow q) \land (q \rightarrow q))$	$(r)) \rightarrow (p \rightarrow r)$ Direct Proof Rule

- A line k in a (sub)proof can use a fact at line i if the set of assumptions and givens that k is derived from contains all the assumptions and givens that i is derived from.
- So, 1.4.2 can use 1.2 because they are derived from the assumptions {1.1, 1.4.1} and {1.1}, respectively.
- Can 1.5 use 1.4.3?
 - No. Because 1.5 is derived from {1.1} and 1.4.3 from {1.1, 1.4.1}.

1.1. $(p \rightarrow q) \land (q \rightarrow r)$ Assum1.2. $p \rightarrow q$ Elim \land 1.3. $q \rightarrow r$ Elim \land	: 1.1
1.4.1. p Assumption 1.4.2. q MP: 1.2, 1.4.1 1.4.3. r MP: 1.3, 1.4.2 1.5. $p \rightarrow r$ Direct Proof Rule	
2. $((p \to q) \land (q \to r)) \to (p \to r)$	Direct Proof Rule

- A line k in a (sub)proof can use a fact at line i if the set of assumptions and givens that k is derived from contains all the assumptions and givens that i is derived from.
- So, 1.4.2 can use 1.2 because they are derived from the assumptions {1.1, 1.4.1} and {1.1}, respectively.
- Can 1.5 use 1.4.3?
 - No. Because 1.5 is derived from {1.1} and 1.4.3 from {1.1, 1.4.1}.
- Can 2 use 1.2?

1.1. $(p \rightarrow q) \land (q \rightarrow r)$ Assump1.2. $p \rightarrow q$ Elim \land :1.3. $q \rightarrow r$ Elim \land :	1.1
1.4.1. p Assumption 1.4.2. q MP: 1.2, 1.4.1 1.4.3. r MP: 1.3, 1.4.2 1.5. $p \rightarrow r$ Direct Proof Rule	
2. $((p \to q) \land (q \to r)) \to (p \to r)$	Direct Proof Rule

- A line k in a (sub)proof can use a fact at line i if the set of assumptions and givens that k is derived from contains all the assumptions and givens that i is derived from.
- So, 1.4.2 can use 1.2 because they are derived from the assumptions {1.1, 1.4.1} and {1.1}, respectively.
- Can 1.5 use 1.4.3?
 - No. Because 1.5 is derived from {1.1} and 1.4.3 from {1.1, 1.4.1}.
- Can 2 use 1.2?
 - No. Because 2 is derived from {} and 1.2 from {1.1}.

Which facts can be used in a subproof? A mnemonic

```
{
   1.1. (p \rightarrow q) \land (q \rightarrow r) Assumption
   1.2. p \rightarrow q
                                   Elim ∧: 1.1
                                      Elim ∧: 1.1
   1.3. q \rightarrow r
    ł
     1.4.1. p Assumption
      1.4.2. q MP: 1.2, 1.4.1
      1.4.3. r MP: 1.3, 1.4.2
    }
   1.5. p \rightarrow r Direct Proof Rule
 }
2. ((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r) Direct Proof
                                                   Rule
```

}

This is just like Java's scoping rules.

A general proof strategy

- 1. Look at the rules for introducing connectives to see how you would build up the formula you want to prove from pieces of what is given.
- 2. Use the rules for eliminating connectives to break down the given formulas so that you get the pieces need for 1
- 3. Write the proof beginning with what you figured out for 2 followed by 1.

Intro
$$\wedge$$
 $A; B$ Intro \vee A Direct Proof Rule $A \implies B$ $\therefore A \land B$ $\therefore A \lor B, B \lor A$ \square \square \square \square \square \square \square Elim \wedge $A \land B$ \square \square

A quick look at predicate logic proofs

Inference rules for quantifiers and a "hello" world example.

Inference rules for quantifiers

Elim $\forall \quad \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$

Intro $\exists \frac{P(c) \text{ for some } c}{\therefore \exists x. P(x)}$

Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$

Elim $\exists x. P(x)$ $\therefore P(c) \text{ for a specific } c$

The name *a* stands for an arbitrary value in the domain. No other name in P depends on a.

The name c is **fresh** and stands for a value in the domain where P(c) is true. List all dependencies for c.

Predicate logic proofs can use ...

Predicate logic inference rules

Applied to whole formulas only.

Predicate logic equivalences

Even on subformulas.

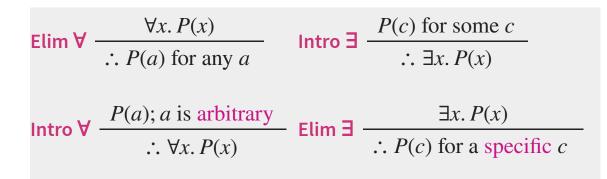
Propositional logic inference rules

Applied to whole formulas only.

Propositional logic equivalences

Even on subformulas.

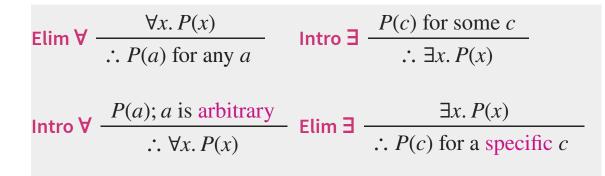
Prove $(\forall x. P(x)) \rightarrow (\exists x. P(x)).$



Prove $(\forall x. P(x)) \rightarrow (\exists x. P(x)).$

- 1.1. $\forall x. P(x)$ Assumption
- 1.2.
- 1.3. $\exists x. P(x)$

2. $(\forall x. P(x)) \rightarrow (\exists x. P(x))$ Direct Proof Rule



• Given \rightarrow , so use Direct Proof Rule.

Prove $(\forall x. P(x)) \rightarrow (\exists x. P(x)).$

- 1.1. $\forall x. P(x)$ Assumption
- 1.2. *P*(*c*)
- 1.3. $\exists x. P(x)$ Intro **∃**: 1.2
- 2. $(\forall x. P(x)) \rightarrow (\exists x. P(x))$ Direct Proof Rule

Elim 🗸 -	$\forall x. P(x)$	Intro ∃	P(c) for some c
	$\therefore P(a)$ for any <i>a</i>		$\therefore \exists x. P(x)$
Intro ∀	P(a); <i>a</i> is arbitrary	Elim 3	$\exists x. P(x)$
	$\therefore \forall x. P(x)$		$\therefore P(c)$ for a specific c

- Given \rightarrow , so use Direct Proof Rule.
- We can use Intro \exists to get 1.3, but need P(c) for some c.

Prove $(\forall x. P(x)) \rightarrow (\exists x. P(x)).$

- 1.1. $\forall x. P(x)$ Assumption
- 1.2. P(c) Elim \forall : 1.1
- 1.3. $\exists x. P(x)$ Intro **∃**: 1.2
- 2. $(\forall x. P(x)) \rightarrow (\exists x. P(x))$ Direct Proof Rule

Elim 🗸	$\forall x. P(x)$	Intro ∃	P(c) for some c
	$\therefore P(a)$ for any a		$\therefore \exists x. P(x)$
Intro ∀	P(a); <i>a</i> is arbitrary	Elim 3	$\exists x. P(x)$
	$\therefore \forall x. P(x)$		$\therefore P(c)$ for a specific c

- Given \rightarrow , so use Direct Proof Rule.
- We can use Intro \exists to get 1.3, but need P(c) for some c.
- We have P(c) from Elim \forall on 1.1.

Prove $(\forall x. P(x)) \rightarrow (\exists x. P(x)).$

1.1.	$\forall x. P(x)$	Assumption

- 1.2. P(c) Elim \forall : 1.1
- 1.3. $\exists x. P(x)$ Intro **∃**: 1.2
- 2. $(\forall x. P(x)) \rightarrow (\exists x. P(x))$ Direct Proof Rule

Elim 🗸	$\forall x. P(x)$	Intro ∃	P(c) for some c
	$\therefore P(a)$ for any a		$\therefore \exists x. P(x)$
Intro ∀	P(a); <i>a</i> is arbitrary	Elim 3	$\exists x. P(x)$
	$\therefore \forall x. P(x)$		$\therefore P(c)$ for a specific c

- Given \rightarrow , so use Direct Proof Rule.
- We can use Intro \exists to get 1.3, but need P(c) for some c.
- We have P(c) from Elim \forall on 1.1.

Working forwards and backwards:

In applying Intro \exists rule, we didn't know what expression we might be able to prove P(c) for, so we worked forwards to figure out what might work.

An in-depth look at predicate logic proofs

Understanding rules for quantifiers through more advanced examples.

Advanced proofs: considering domain semantics

So far, we have treated the predicate definitions as black boxes, and the domain of discourse as a set of objects with no additional properties.

In practice, we want to prove theorems for specific domains, and use the properties of those domains in our proofs.

Advanced proofs: considering domain semantics

So far, we have treated the predicate definitions as black boxes, and the domain of discourse as a set of objects with no additional properties.

In practice, we want to prove theorems for specific domains, and use the properties of those domains in our proofs.

For example, the set of integers is equipped with the operators $+, \cdot, =$.

Advanced proofs: considering domain semantics

So far, we have treated the predicate definitions as black boxes, and the domain of discourse as a set of objects with no additional properties.

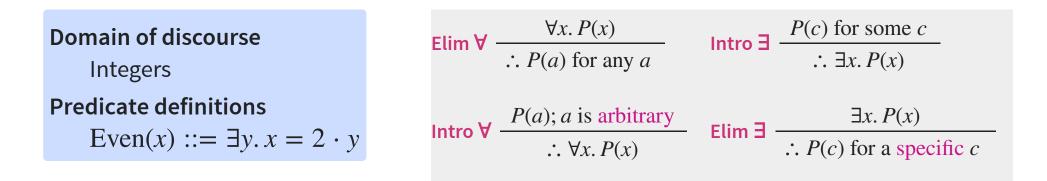
In practice, we want to prove theorems for specific domains, and use the properties of those domains in our proofs.

For example, the set of integers is equipped with the operators $+, \cdot, =$.

We can use these operators in our predicates (below) and proofs (next):

Domain of discourse	Predicate definitions
Integers	$\operatorname{Even}(x) ::= \exists y. x = 2 \cdot y$

Prove that there is an even number: $\exists x. Even(x)$.



Prove that there is an even number: $\exists x. Even(x)$.

1. 2.

3.

4. $\exists x$. Even(x)

Domain of discourse Integers Predicate definitions $Even(x) ::= \exists y. x = 2 \cdot y$

Elim ∀	$\forall x. P(x)$ $\therefore P(a) \text{ for any } a$	Intro ∃	$\frac{P(c) \text{ for some } c}{\therefore \exists x. P(x)}$
Intro ∀	$\frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Elim 3	$\exists x. P(x)$ $\therefore P(c) \text{ for a specific } c$

Prove that there is an even number: $\exists x. Even(x)$.

1. 2. 3. Even(2) 4. $\exists x. \text{Even}(x)$ Intro $\exists : 3$ Domain of discourse Integers Predicate definitions Even(x) ::= $\exists y. x = 2 \cdot y$ Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$ Elim $\exists \frac{\exists x. P(x)}{\therefore P(c) \text{ for a specific } c}$

Prove that there is an even number: $\exists x. Even(x)$.

1. 2. $\exists y. 2 = 2 \cdot y$

3. Even(2)

```
Definition of Even: 2
4. \exists x. Even(x) Intro \exists: 3
```

Domain of discourse

Integers

Predicate definitions

 $\operatorname{Even}(x) ::= \exists y. \, x = 2 \cdot y$

Elim 🗸 ·	$\forall x. P(x)$ $\therefore P(a) \text{ for any } a$	Intro ∃	$\frac{P(c) \text{ for some } c}{\therefore \exists x. P(x)}$
Intro ∀	$\frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Elim 3	$\exists x. P(x)$ $\therefore P(c) \text{ for a specific } c$

Prove that there is an even number: $\exists x. Even(x)$.

1. $2 = 2 \cdot 1$	Arithmetic
2. $\exists y. 2 = 2 \cdot y$	Intro ∃: 1
3. Even(2)	Definition of Even: 2
4. $\exists x. \operatorname{Even}(x)$	Intro ∃: 3

Domain of discourse

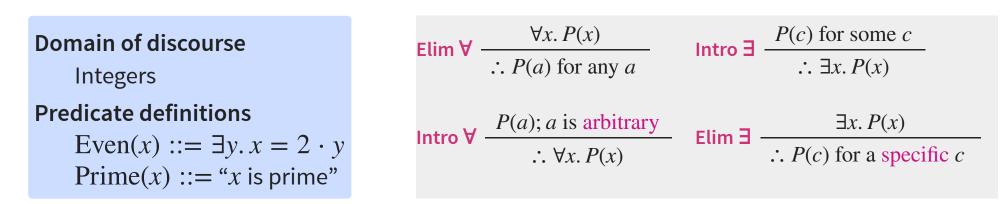
Integers

Predicate definitions

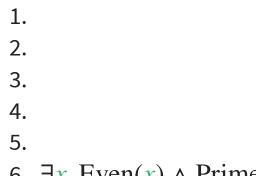
 $\operatorname{Even}(x) ::= \exists y. \, x = 2 \cdot y$

С

Prove that there is an even prime number: $\exists x. Even(x) \land Prime(x)$.



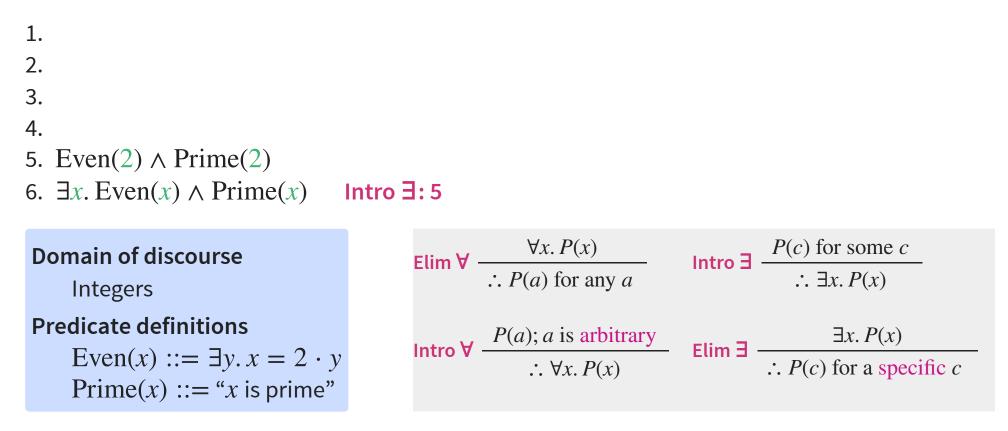
Prove that there is an even prime number: $\exists x. Even(x) \land Prime(x)$.



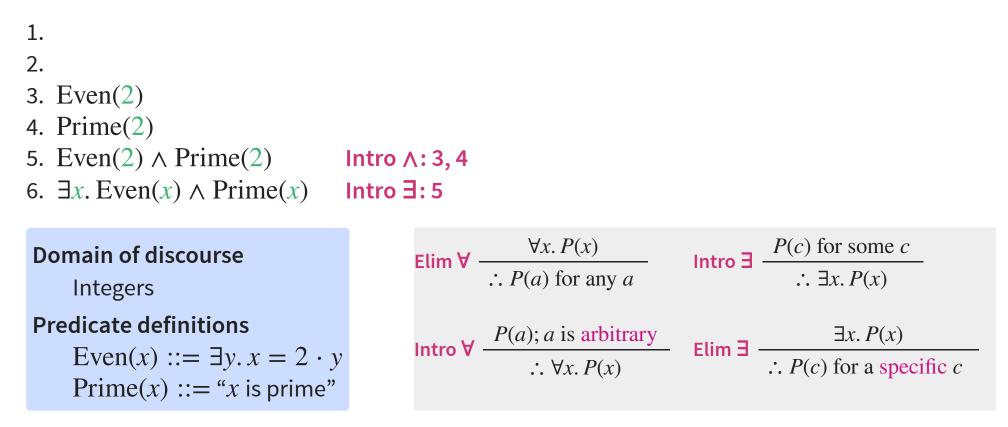
6. $\exists x. \operatorname{Even}(x) \land \operatorname{Prime}(x)$

Domain of discourse Integers	Elim $\forall \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$	Intro $\exists \frac{P(c) \text{ for some } c}{\therefore \exists x. P(x)}$
Predicate definitions $Even(x) ::= \exists y. x = 2 \cdot y$ Prime(x) ::= "x is prime"	Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Elim $\exists \frac{\exists x. P(x)}{\therefore P(c) \text{ for a specific } c}$

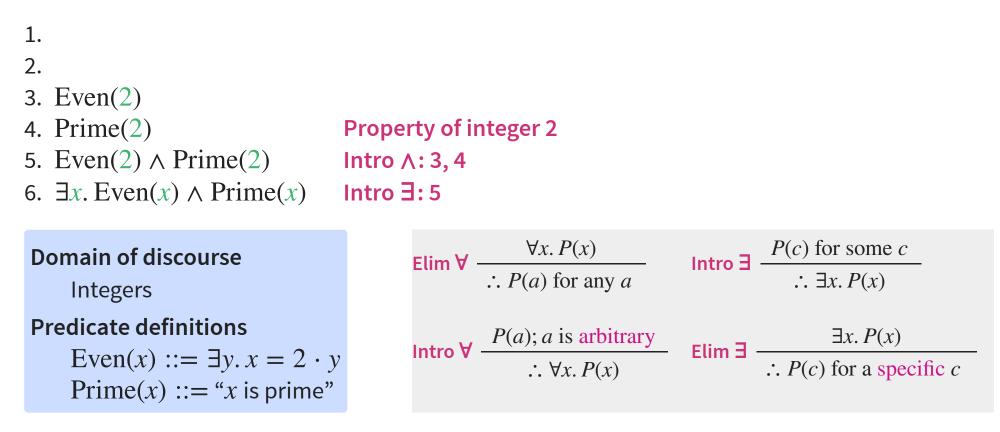
Prove that there is an even prime number: $\exists x. Even(x) \land Prime(x)$.



Prove that there is an even prime number: $\exists x. Even(x) \land Prime(x)$.



Prove that there is an even prime number: $\exists x. Even(x) \land Prime(x)$.

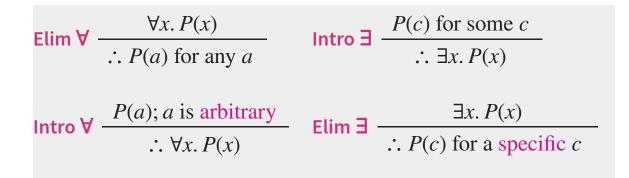


Prove that there is an even prime number: $\exists x. Even(x) \land Prime(x)$.

1. $2 = 2 \cdot 1$ 2. $\exists y. 2 = 2 \cdot y$ 3. Even(2) 4. Prime(2) 5. Even(2) \land Prime(2) 6. $\exists x. Even(x) \land$ Prime(x)	Arithmetic Intro \exists : 1 Definition of Even: 2 Property of integer 2 Intro \land : 3, 4 Intro \exists : 5	
Domain of discourse Integers	Elim $\forall \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$	Intro $\exists \frac{P(c) \text{ for some } c}{\therefore \exists x. P(x)}$
Predicate definitions $Even(x) ::= \exists y. x = 2 \cdot y$ Prime(x) ::= "x is prime"	, Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Elim $\exists \frac{\exists x. P(x)}{\therefore P(c) \text{ for a specific } c}$

Prove that $\forall y. \exists z. y = z$ follows from $\forall x. x = x$.

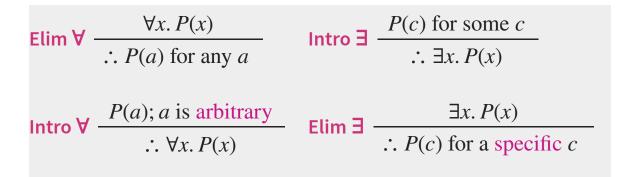
Domain of discourse Integers



Prove that $\forall y. \exists z. y = z$ follows from $\forall x. x = x$.

```
1. \forall x. x = x Given
2.
3.
4. \forall y. \exists z. y = z
```

Domain of discourse Integers



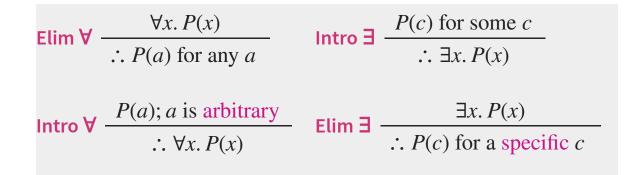
Prove that $\forall y. \exists z. y = z$ follows from $\forall x. x = x$.

1. $\forall x. x = x$ Given2. a = aElim $\forall : 1, a \text{ is arbitrary}$

3.

4. $\forall y. \exists z. y = z$

Domain of discourse Integers

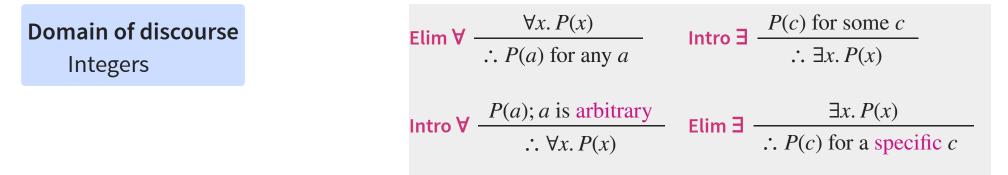


Prove that $\forall y. \exists z. y = z$ follows from $\forall x. x = x$.

- 1. $\forall x. x = x$ Given

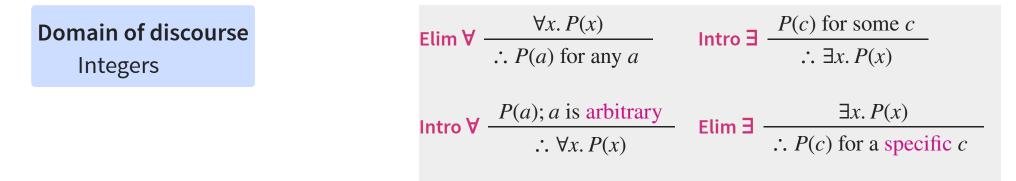
```
2. a = a Elim \forall: 1, a is arbitrary
3. \exists z. a = z Intro ∃: 2
```

4. $\forall y. \exists z. y = z$



Prove that $\forall y. \exists z. y = z$ follows from $\forall x. x = x$.

- 1. $\forall x. x = x$ Given
- 2. a = a Elim \forall : 1, a is arbitrary
- 3. $\exists z. a = z$ Intro $\exists : 2$
- 4. $\forall y. \exists z. y = z$ Intro $\forall: 3$



Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

Domain of discourse	Elim $\forall \dots \forall x. P(x)$	Int
Integers	$\therefore P(a)$ for any a	
Predicate definitions	Intro \forall <u>$P(a); a \text{ is arbitrary}$</u>	Fli
$\operatorname{Even}(x) ::= \exists y. x = 2 \cdot y$	$\cdot \forall \omega D(\omega)$	_

$$\forall x. P(x)$$
Intro \exists $P(c)$ for some c $\therefore P(a)$ for any a $\therefore \exists x. P(x)$ $P(a); a$ is arbitrary $\exists x. P(x)$ $\therefore \forall x. P(x)$ $\exists x. P(c)$ for a specific c

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

4. $\forall x. \operatorname{Even}(x) \to \operatorname{Even}(x^2)$

Domain of discourse Integers Predicate definitions $Even(x) ::= \exists y. x = 2 \cdot y$

Elim
$$\forall$$
 $\forall x. P(x)$
 $\therefore P(a)$ for any a Intro \exists $P(c)$ for some c
 $\therefore \exists x. P(x)$ Intro \forall $P(a); a$ is arbitrary
 $\therefore \forall x. P(x)$ Elim \exists $\exists x. P(x)$
 $\therefore P(c)$ for a specific c

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

1. Let *a* be an arbitrary integer.



3. $\operatorname{Even}(a) \to \operatorname{Even}(a^2)$ 4. $\forall x. \operatorname{Even}(x) \to \operatorname{Even}(x^2)$ Intro $\forall: 1, 3$

Domain of discourse Integers Predicate definitions $Even(x) ::= \exists y. x = 2 \cdot y$

Elim $\forall \dots \forall x. P(x)$	Intro $\exists \frac{P(c) \text{ for some } c}{2}$
$\therefore P(a)$ for any a	$\therefore \exists x. P(x)$
Intro \forall <u>$P(a); a \text{ is arbitrary}$</u>	Elim $\exists x. P(x)$
$\therefore \forall x. P(x)$	$\therefore P(c)$ for a specific c

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

1. Let *a* be an arbitrary integer.

2.1. Even(<i>a</i>)	Assumption
2.2.	
2.3.	
2.4.	
2.5.	
2.6. Even(a^2)	
\mathbf{E}	Dive et Dve et

- 3. Even(a) \rightarrow Even(a²)
- 4. $\forall x. \operatorname{Even}(x) \to \operatorname{Even}(x^2)$ Intro

Direct Proof Rule Intro ∀: 1, 3

Domain of discourse

Integers

Predicate definitions

```
\operatorname{Even}(x) ::= \exists y. \, x = 2 \cdot y
```

Elim $\forall x. P(x)$	Intro $\exists \frac{P(c) \text{ for some } c}{2}$
$\therefore P(a)$ for any a	$\therefore \exists x. P(x)$
Intro \forall <u>$P(a); a \text{ is arbitrary}$</u>	Elim $\exists x. P(x)$
$\therefore \forall x. P(x)$	$\therefore P(c)$ for a specific c

- Use Intro \forall on 1 and 2.
- \rightarrow so use DRP to get 3.

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

1. Let *a* be an arbitrary integer.

• \rightarrow so use DRP to get 3. 2.1. Even(*a*) Assumption • Use definition of Even to break 2.2. $\exists y. a = 2y$ **Definition of Even: 2.1** down 2.1 and 2.6. 2.3. 2.4. 2.5. $\exists y. a^2 = 2y$ 2.6. Even(a^2) **Definition of Even: 2.5** 3. Even(*a*) \rightarrow Even(*a*²) Direct Proof Rule 4. $\forall x. \operatorname{Even}(x) \to \operatorname{Even}(x^2)$ Intro \forall : 1, 3

Domain of discourse

Integers

Predicate definitions

 $\operatorname{Even}(x) ::= \exists y. \, x = 2 \cdot y$

Elim \forall $\forall x. P(x)$
 $\therefore P(a)$ for any aIntro \exists P(c) for some c
 $\therefore \exists x. P(x)$ Intro \forall P(a); a is arbitrary
 $\therefore \forall x. P(x)$ Elim \exists $\exists x. P(x)$
 $\therefore P(c)$ for a specific c

• Use Intro \forall on 1 and 2.

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

- 1. Let *a* be an arbitrary integer.
 - 2.1. Even(*a*) 2.2. $\exists y. a = 2y$ 2.3. a = 2b2.4. 2.5. $\exists y. a^2 = 2y$ 2.6. Even(a^2)

Domain of discourse

Predicate definitions

Integers

3. Even(*a*) \rightarrow Even(*a*²) 4. $\forall x$. Even(x) \rightarrow Even(x^2) Assumption **Definition of Even: 2.1** Elim \exists : 2.2, **b** depends on **a**

Definition of Even: 2.5

 $Even(x) ::= \exists y. x = 2 \cdot y$

Direct Proof Rule Intro \forall : 1, 3

• Use Intro \forall on 1 and 2.

- \rightarrow so use DRP to get 3.
- Use definition of Even to break down 2.1 and 2.6.
- Use Elim \exists on 2.2.

Elim
$$\forall$$
 $\forall x. P(x)$
 $\therefore P(a)$ for any a Intro \exists $P(c)$ for some c
 $\therefore \exists x. P(x)$ Intro \forall $P(a); a$ is arbitrary
 $\therefore \forall x. P(x)$ Elim \exists $\exists x. P(x)$
 $\therefore P(c)$ for a specific c

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

- 1. Let *a* be an arbitrary integer.
 - 2.1. Even(a) 2.2. $\exists y. a = 2y$ 2.3. a = 2b2.4. $a^2 = 4b^2 = 2(2b^2)$ 2.5. $\exists y. a^2 = 2y$ 2.6. Even(a^2)
- 3. $\operatorname{Even}(a) \to \operatorname{Even}(a^2)$ 4. $\forall x. \operatorname{Even}(x) \to \operatorname{Even}(x^2)$

Assumption Definition of Even: 2.1 Elim ∃: 2.2, b depends on a Algebra

Definition of Even: 2.5 Direct Proof Rule

Intro \forall : 1, 3

• Use Intro \forall on 1 and 2.

- \rightarrow so use DRP to get 3.
- Use definition of Even to break down 2.1 and 2.6.
- Use Elim \exists on 2.2.
- Use algebra on 2.3 to match the body of 2.5.

Domain of discourse

Integers

Predicate definitions

 $\operatorname{Even}(x) ::= \exists y. \, x = 2 \cdot y$

Elim \forall $\forall x. P(x)$
 $\therefore P(a)$ for any aIntro \exists P(c) for some c
 $\therefore \exists x. P(x)$ Intro \forall P(a); a is arbitrary
 $\therefore \forall x. P(x)$ Elim \exists $\exists x. P(x)$
 $\therefore P(c)$ for a specific c

Prove that the square of every even number is even: $\forall x. Even(x) \rightarrow Even(x^2)$.

- 1. Let *a* be an arbitrary integer.
 - 2.1. Even(a) 2.2. $\exists y. a = 2y$ 2.3. a = 2b2.4. $a^2 = 4b^2 = 2(2b^2)$ 2.5. $\exists y. a^2 = 2y$ 2.6. Even(a^2)
- 3. $\operatorname{Even}(a) \to \operatorname{Even}(a^2)$ 4. $\forall x. \operatorname{Even}(x) \to \operatorname{Even}(x^2)$

Assumption Definition of Even: 2.1 Elim \exists : 2.2, **b** depends on **a** Algebra Intro \exists : 2.4 Definition of Even: 2.5 Direct Proof Rule Intro \forall : 1, 3

- Use Intro \forall on 1 and 2.
- \rightarrow so use DRP to get 3.
- Use definition of Even to break down 2.1 and 2.6.
- Use Elim \exists on 2.2.
- Use algebra on 2.3 to match the body of 2.5.
- Use Intro \exists on 2.4 to get 2.5.

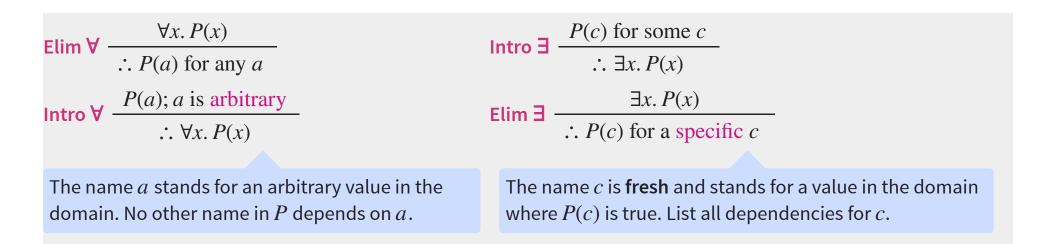
Domain of discourse

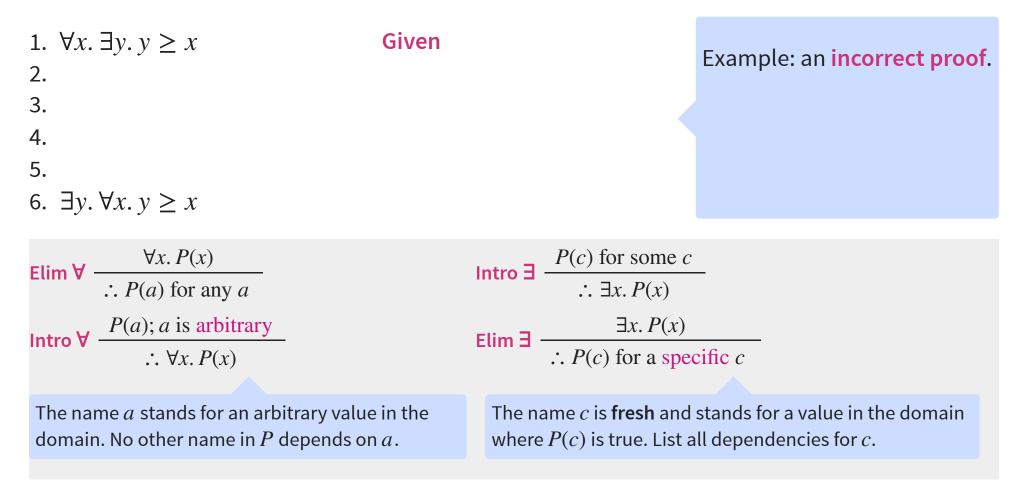
Integers

Predicate definitions

 $\operatorname{Even}(x) ::= \exists y. \, x = 2 \cdot y$

Elim
$$\forall$$
 $\forall x. P(x)$
 $\therefore P(a)$ for any a Intro \exists $P(c)$ for some c
 $\therefore \exists x. P(x)$ Intro \forall $P(a); a$ is arbitrary
 $\therefore \forall x. P(x)$ Elim \exists $\exists x. P(x)$
 $\therefore P(c)$ for a specific c





 ∀x. ∃y. y ≥ x Let <i>a</i> be an arbitrary integer. 4. 5. 	Given	Example: an incorrect proof .
$6. \ \exists y. \forall x. y \ge x$	Intro ∃: 5	
Elim $\forall \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$ Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Intro $\exists \frac{P(c) \text{ for some } c}{\therefore \exists x. P(x)}$ Elim $\exists \frac{\exists x. P(x)}{\therefore P(c) \text{ for a spectrum}}$	
The name <i>a</i> stands for an arbitrary value domain. No other name in <i>P</i> depends on		d stands for a value in the domain all dependencies for c .

1. $\forall x. \exists y. y \ge x$ 2. Let <i>a</i> be an arbitrary integer.	Given	Example: an incorrect proof .	
3. $\exists y. y \ge a$ 4. 5.	Elim∀:1		
$\exists y. \forall x. y \ge x$	Intro ∃: 5		
Elim $\forall \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$	Intro $\exists \frac{P(c) \text{ for some}}{\therefore \exists x. P(x)}$	<u>C</u>	
Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Elim $\exists \frac{\exists x. P(x)}{\therefore P(c) \text{ for a sp}}$	ecific c	
The name <i>a</i> stands for an arbitrary valudomain. No other name in <i>P</i> depends of		The name c is fresh and stands for a value in the domain where $P(c)$ is true. List all dependencies for c .	

1. $\forall x. \exists y. y \ge x$ 2. Let <i>a</i> be an arbitrary integer.	Given	Example: an incorrect proof .
3. $\exists y. y \ge a$ 4. $b \ge a$ 5.	Elim∀:1 Elim∃:3, b depends on a	
6. $\exists y. \forall x. y \ge x$	Intro ∃: 5	
Elim $\forall \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$ Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Intro $\exists \frac{P(c) \text{ for some}}{\therefore \exists x. P(x)}$ Elim $\exists \frac{\exists x. P(x)}{\therefore P(c) \text{ for a sp}}$	
The name <i>a</i> stands for an arbitrary value domain. No other name in <i>P</i> depends of		d stands for a value in the domain all dependencies for <i>c</i> .

 ∀x. ∃y. y ≥ x Let <i>a</i> be an arbitrary integer. ∃y. y ≥ a <i>b</i> ≥ a 	Given Elim∀: 1 Elim∃: 3, b depends on a	Example: an incorrect proof . Can't get rid of <i>a</i> since another name, <i>b</i> , in the	
5. $\forall x. b \ge x$ 6. $\exists y. \forall x. y \ge x$	Intro ∀: 2, 4 Intro ∃: 5	same formula depends on it!	
Elim $\forall \frac{\forall x. P(x)}{\therefore P(a) \text{ for any } a}$	Intro $\exists \frac{P(c) \text{ for som}}{\therefore \exists x. P(x)}$	e <i>c</i>	
Intro $\forall \frac{P(a); a \text{ is arbitrary}}{\therefore \forall x. P(x)}$	Elim $\exists \frac{\exists x. P(c)}{\therefore P(c) \text{ for a s}}$	$\frac{x}{\text{pecific } c}$	
The name <i>a</i> stands for an arbitrary valudomain. No other name in <i>P</i> depends of		The name c is fresh and stands for a value in the domain where $P(c)$ is true. List all dependencies for c .	

Summary

Predicate logic proofs extend propositional logic proofs.

Can use all rules and equivalences for propositional logic.

Plus inference rules for quantifiers and equivalences for predicate logic.

When applying Intro \forall to P(a), make sure that

a is *arbitrary*, and no other name *depends* on *a*.

When applying Elim \exists to $\exists x. P(x)$, make sure that

c in P(c) is fresh, and

all the dependencies for c are listed.