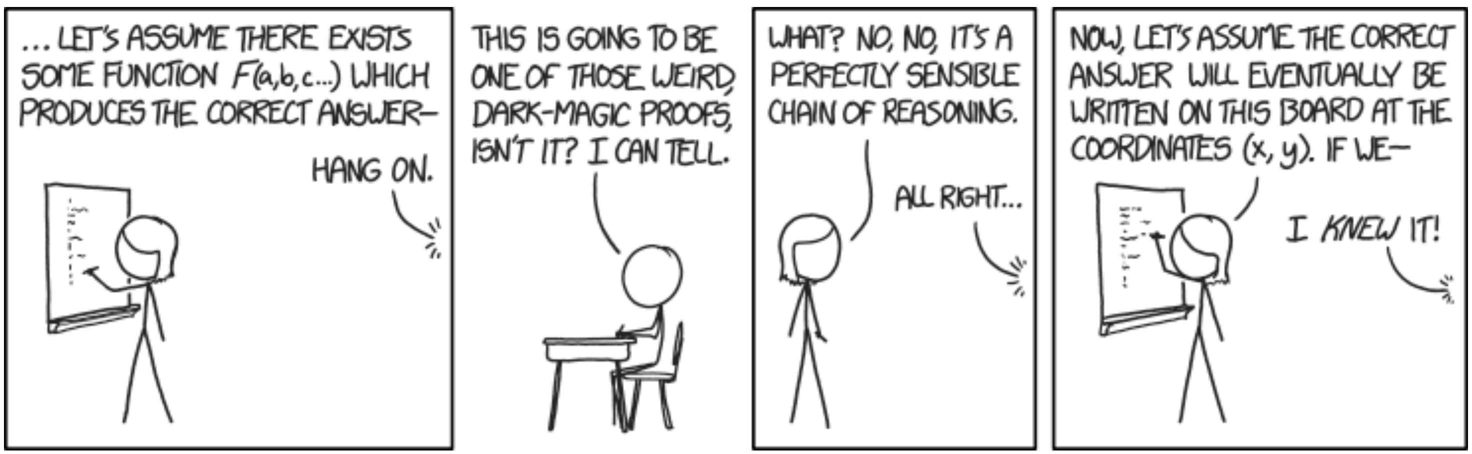
CSE 311: Foundations of Computing

Topic 2: Proofs



Logical Inference

- So far, we've considered:
  - how to understand and *express* things using propositional and predicate logic
  - how to *compute* using Propositional logic (circuits)
  - how to show that different ways of expressing or computing them are *equivalent* to each other
- Logic also has methods that let us *infer* implied properties from ones that we know
  - equivalence is a small part of this

New Perspective

Rather than comparing A and B as columns, zooming in on just the rows where A is true:

p	*q*	A(*p*,*q*)	B(*p*,*q*)
T	T	T	
T	F	T	
F	T	F	
F	F	F	

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	q	A(p,q)	B(p,q)
T	T	T	T
T	F	T	T
F	T	F	
F	F	F	

Given that A is true, we see that B is also true.

$$A \Rightarrow B$$

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	q	A(p,q)	B(p,q)
T	T	T	T
T	F	T	T
F	T	F	?
F	F	F	?

When we zoom out, what have we proven?

New Perspective

Rather than comparing **A** and **B** as columns, zooming in on just the rows where A is true:

p	q	A(p,q)	B(p,q)	A $\rightarrow$ B
T	T	T	T	T
T	F	T	T	T
F	T	F	T	T
F	F	F	F	T

When we zoom out, what have we proven?

$$(A \rightarrow B) \equiv \mathbf{T}$$

New Perspective

Equivalences

$A \equiv B$ and $(A \leftrightarrow B) \equiv T$ are the same

Inference

$A \Rightarrow B$ and $(A \rightarrow B) \equiv T$ are the same

Proofs

- Start with given facts (hypotheses)
- Use rules of inference to extend set of facts
- Result is proved when it is included in the set

An inference rule: *Modus Ponens*

- If A and $A \rightarrow B$ are both true, then B must be true
- Write this rule as

$$\frac{A\ ;\ A \rightarrow B}{\therefore\ B}$$

- Given:
  - If it is Friday, then you have a 311 lecture today.
  - It is Friday.
- Therefore, by Modus Ponens:
  - You have a 311 lecture today.

My First Proof!

Show that r follows from p, p → q, and q → r

1. p Given
2. $p \to q$ Given
3. $q \to r$ Given
4.
5.

Modus Ponens $\dfrac{A\ ;\ A \to B}{\therefore\ B}$

My First Proof!

Show that r follows from p, p → q, and q → r

1. p Given
2. $p \rightarrow q$ Given
3. $q \rightarrow r$ Given
4. q MP: 1, 2
5. r MP: 4, 3

Modus Ponens $\dfrac{A\ ;\ A \rightarrow B}{\therefore\ B}$

Proofs can use equivalences too

Show that $\neg p$ follows from $p \rightarrow q$ and $\neg q$

1.	$p \rightarrow q$	Given
2.	$\neg q$	Given
3.	$\neg q \rightarrow \neg p$	Contrapositive: 1
4.	$\neg p$	MP: 2, 3

Modus Ponens $\dfrac{A\ ;\ A \rightarrow B}{\therefore\ B}$

Inference Rules

If A is true and B is true ....

Requirements: $\underline{A \;;\; B}$

Conclusions: $\therefore C \;,\; D$

Then, C must be true

Then D must be true

Example (Modus Ponens):

$$\frac{A \;;\; A \rightarrow B}{\therefore \quad B}$$

If I have A and A $\rightarrow$ B both true,
Then B must be true.

Axioms: Special inference rules

If I have nothing...

Requirements:

Conclusions: $\therefore C\ ,\ D$

Then, C must be true

Then D must be true

Example (Excluded Middle):

$$\therefore A \vee \neg A$$

$A \vee \neg A$ must be true.

Simple Propositional Inference Rules

Two inference rules per binary connective, one to eliminate it and one to introduce it

Elim ∧

$$\frac{A \land B}{\therefore A, B}$$

Intro ∧

$$\frac{A \,;\, B}{\therefore A \land B}$$

Elim ∨

$$\frac{A \lor B \,;\, \neg A}{\therefore B}$$

Intro ∨

$$\frac{A}{\therefore A \lor B,\ B \lor A}$$

Modus Ponens

$$\frac{A \,;\, A \rightarrow B}{\therefore B}$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Proofs

Show that r follows from $p, p \rightarrow q,$ and $p \wedge q \rightarrow r$

How To Start:

We have givens, find the ones that go together and use them. Now, treat new things as givens, and repeat.

$$\frac{A\ ;\ A \rightarrow B}{\therefore\ B}$$

$$\frac{A \wedge B}{\therefore\ A,\ B}$$

$$\frac{A\ ;\ B}{\therefore\ A \wedge B}$$

Proofs

Show that r follows from $p, p \to q,$ and $p \land q \to r$

1.	p	Given
2.	$p \to q$	Given
3.	$p \land q \to r$	Given

$$\frac{A \,;\, A \to B}{\therefore\ B}$$

$$\frac{A \land B}{\therefore\ A,\ B}$$

$$\frac{A \,;\, B}{\therefore\ A \land B}$$

Proofs

Show that r follows from $p, p \rightarrow q,$ and $p \wedge q \rightarrow r$

1.	p	Given
2.	$p \rightarrow q$	Given
3.	$p \wedge q \rightarrow r$	Given
4.	q	MP: 1, 2
5.	$p \wedge q$	Intro $\wedge$: 1, 4
6.	r	MP: 5, 3

Proofs

Show that r follows from $p, p \to q,$ and $p \wedge q \to r$

$$\dfrac{\dfrac{p \quad ; \quad \dfrac{p \quad ; \quad p \to q}{q}\,\text{MP}}{p \wedge q}\,\text{Intro} \wedge \quad ; \quad p \wedge q \to r}{r}\,\text{MP}$$

Proofs

Show that r follows from $p, p \rightarrow q,$ and $p \wedge q \rightarrow r$

1.	p	Given
2.	$p \rightarrow q$	Given
3.	q	MP: 1, 2
4.	$p \wedge q$	Intro $\wedge$: 1, 3
5.	$p \wedge q \rightarrow r$	Given
6.	r	MP: 4, 5

Two visuals of the same proof. We will use the right one, but if the bottom one helps you think about it, that's great!

$$\dfrac{\dfrac{p \;;\; \dfrac{p \;;\; p \rightarrow q}{q}\,\text{MP}}{p \wedge q}\,\text{Intro } \wedge \;;\; p \wedge q \rightarrow r}{r}\,\text{MP}$$

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1. $p \wedge s$ Given
2. $q \rightarrow \neg r$ Given
3. $\neg s \vee q$ Given

First: Write down givens and goal

20. $\neg r$?

Idea: Work backwards!

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
20.	$\neg r$	MP: 2, ?

Idea: Work backwards!

We want to eventually get $\neg r$. How?

- We can use $q \rightarrow \neg r$ to get there.
- The justification between 2 and 20 looks like "elim →" which is MP.

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
19.	q	?
20.	$\neg r$	MP: 2, 19

<u>Idea: Work backwards!</u>

We want to eventually get $\neg r$. How?

- Now, we have a new "hole"
- We need to prove q...
  - Notice that at this point, if we prove q, we've proven $\neg r$...

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
19.	q	?
20.	$\neg r$	MP: 2, 19

This looks like or-elimination.

Elim ∨ $\dfrac{A \vee B\ ;\ \neg A}{\therefore B}$

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1. $p \wedge s$ Given
2. $q \rightarrow \neg r$ Given
3. $\neg s \vee q$ Given

$\neg\neg s$ doesn't show up in the givens but s does and we can use equivalences

18. $\neg\neg s$?
19. q $\vee$ Elim: 3, 18
20. $\neg r$ MP: 2, 19

Proofs

Prove that $\neg r$ follows from $p \land s$, $q \rightarrow \neg r$, and $\neg s \lor q$.

1.	$p \land s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \lor q$	Given
17.	s	?
18.	$\neg\neg s$	Double Negation: 17
19.	q	Elim $\lor$: 3, 18
20.	$\neg r$	MP: 2, 19

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
17.	s	Elim ∧: 1
18.	$\neg\neg s$	Double Negation: 17
19.	q	Elim ∨: 3, 18
20.	$\neg r$	MP: 2, 19

No holes left! We just need to clean up a bit.

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
4.	s	Elim $\wedge$: 1
5.	$\neg\neg s$	Double Negation: 4
6.	q	Elim $\vee$: 3, 5
7.	$\neg r$	MP: 2, 6

Important: Applications of Inference Rules

- You can use equivalences to make substitutions of any sub-formula.

  e.g. $(p \rightarrow r) \vee q \equiv (\neg p \vee r) \vee q$

- Inference rules only can be applied to whole formulas (not correct otherwise).

  e.g. 1. $p \rightarrow r$ given

  ~~2. $(p \vee q) \rightarrow r$ intro $\vee$ from 1.~~

  Does not follow! e.g . p=F, q=T, r=F

Recall: Propositional Inference Rules

Two inference rules per binary connective, one to eliminate it and one to introduce it

Elim ∧
$$\frac{A \wedge B}{\therefore A, B}$$

Intro ∧
$$\frac{A \,;\, B}{\therefore A \wedge B}$$

Elim ∨
$$\frac{A \vee B \,;\, \neg A}{\therefore B}$$

Intro ∨
$$\frac{A}{\therefore A \vee B, B \vee A}$$

Modus Ponens
$$\frac{A \,;\, A \rightarrow B}{\therefore B}$$

Direct Proof
$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Not like other rules

To Prove An Implication: $A \rightarrow B$

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

- We use the direct proof rule
- The "pre-requisite" $A \Rightarrow B$ for the direct proof rule is **a proof** that "**Assuming** A, we can prove B."
- The direct proof rule:

  If you have such a proof, then you can conclude that $A \rightarrow B$ is true

Proofs using the direct proof rule

Show that $p \rightarrow r$ follows from q and $(p \land q) \rightarrow r$

1. q Given
2. $(p \land q) \rightarrow r$ Given

This is a proof of $p \rightarrow r$

3.1. p Assumption

3.2.

3.3. r ??

3. $p \rightarrow r$ Direct Proof

If we know p is true…
Then, we've shown
r is true

Proofs using the direct proof rule

Show that $p \rightarrow r$ follows from q and $(p \wedge q) \rightarrow r$

1. q Given
2. $(p \wedge q) \rightarrow r$ Given
    - 3.1. p Assumption
    - 3.2. $p \wedge q$ Intro $\wedge$: 1, 3.1
    - 3.3. r MP: 2, 3.2
3. $p \rightarrow r$ Direct Proof

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

There MUST be an application of the Direct Proof Rule (or an equivalence) to prove this implication.

Where do we start? We have no givens...

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

1.1.	$p \wedge q$	Assumption
1.9.	$p \vee q$	??
1.	$(p \wedge q) \rightarrow (p \vee q)$	Direct Proof

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

1.1.	$p \wedge q$	Assumption
1.2.	p	Elim $\wedge$: 1.1
1.3.	$p \vee q$	Intro $\vee$: 1.2
1.	$(p \wedge q) \rightarrow (p \vee q)$	Direct Proof

Our General Proof Strategy

1. Use introduction rules to see how you would build up the formula you want to prove from pieces of what is given

2. Use elimination rules to break down the given formulas to get the pieces you need to do 1.

3. Write the proof beginning with what you figured out for 2 followed by 1.

Our General Proof Strategy

1. $p \rightarrow q$ Given
2. p Given

...

?. $(p \vee r) \wedge q$?

Use **elimination** rules to move **down**

Our General Proof Strategy

1. $p \rightarrow q$ Given
2. p Given
3. q MP: 2, 1

Use **elimination** rules to move **down**

...

Use **introduction** rules to move **up**

?. $(p \vee r) \wedge q$?

Our General Proof Strategy

1. $p \to q$ Given
2. p Given
3. q MP: 2, 1

Use **elimination** rules to move **down**

...

?. $p \vee r$

?. q

?. $(p \vee r) \wedge q$ Intro ∧

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $p \rightarrow q$ Given
2. p Given

...

?. $p \vee r$ Intro $\vee$??

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro $\vee$
(**must** wait until you know which one is true)

Our General Proof Strategy

1.	$p \rightarrow q$	Given
2.	p	Given
...		
?.	r	?
?.	$p \vee r$	Intro $\vee$

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro $\vee$
(**must** wait until you know which one is true)

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Example

Prove: $((p \to q) \wedge (q \to r)) \to (p \to r)$

1.1. $(p \to q) \wedge (q \to r)$ Assumption

1.? $p \to r$

1. $\big((p \to q) \wedge (q \to r)\big) \to (p \to r)$ Direct Proof

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

1.1. $(p \rightarrow q) \wedge (q \rightarrow r)$ Assumption

1.2. $p \rightarrow q$ Elim ∧: 1.1

1.3. $q \rightarrow r$ Elim ∧: 1.1

1.? $p \rightarrow r$

1. $\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$ Direct Proof

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

1.1. $(p \rightarrow q) \wedge (q \rightarrow r)$ Assumption

1.2. $p \rightarrow q$ Elim ∧: 1.1

1.3. $q \rightarrow r$ Elim ∧: 1.1

1.4.1. p Assumption

1.4.? r

1.4. $p \rightarrow r$ Direct Proof

1. $\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$ Direct Proof

Example

Prove: $((p \to q) \land (q \to r)) \to (p \to r)$

1.1.	$(p \to q) \land (q \to r)$	Assumption
1.2.	$p \to q$	Elim $\land$: 1.1
1.3.	$q \to r$	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
1.4.	$p \to r$	Direct Proof
1.	$\big((p \to q) \land (q \to r)\big) \to (p \to r)$	Direct Proof

Applications of Logical Inference

- Software Engineering
  - Express desired properties of program as set of logical constraints
  - Use inference rules to show that program implies that those constraints are satisfied
- Artificial Intelligence
  - Automated reasoning
- Algorithm design and analysis
  - e.g., Correctness, Loop invariants.
- Logic Programming, e.g. Prolog
  - Express desired outcome as set of constraints
  - Automatically apply logic inference to derive solution

Minimal Rules for Propositional Logic

Can get away with just these:

Elim ∧

$$\frac{A \land B}{\therefore A, B}$$

Intro ∧

$$\frac{A \ ; \ B}{\therefore A \land B}$$

Elim ∨

$$\frac{A \lor B \ ; \ \neg A}{\therefore B}$$

Intro ∨

$$\frac{A}{\therefore A \lor B, B \lor A}$$

Modus Ponens

$$\frac{A \ ; \ A \to B}{\therefore B}$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore A \to B}$$

Excluded Middle

$$\frac{}{\therefore A \lor \neg A}$$

Note: only **this** tautology

Rules for Propositional Logic *with Tautology*

More rules makes proofs easier

Elim ∧
$$\frac{A \land B}{\therefore A, B}$$

Intro ∧
$$\frac{A \;;\; B}{\therefore A \land B}$$

Elim ∨
$$\frac{A \lor B \;;\; \neg A}{\therefore B}$$

Intro ∨
$$\frac{A}{\therefore A \lor B, B \lor A}$$

Modus Ponens
$$\frac{A \;;\; A \rightarrow B}{\therefore B}$$

Direct Proof
$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Tautology
$$\frac{A \equiv T}{\therefore A}$$

Equivalent
$$\frac{A \equiv B \;;\; B}{\therefore A}$$

any known

Proof by Cases

Some rules can be written in different ways

- e.g., two different elimination rules for "$\vee$"

Elim ∨

$$\frac{A \vee B \; ; \; \neg A}{\therefore B}$$

Cases

$$\frac{A \vee B \; ; \; A \rightarrow C \; ; \; B \rightarrow C}{\therefore C}$$

second rule is more useful

Example: Absorption via Cases

Show that P follows from $P \lor (P \land Q)$...

1. $P \lor (P \land Q)$ Given

Cases $\dfrac{A \lor B \,;\, A \to C \,;\, B \to C}{\therefore C}$

4. P ?

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2. $P \rightarrow P$	?
3. $(P \wedge Q) \rightarrow P$	?
4. P	Cases: 1, 2, 3

Example: Absorption via Cases

Show that P follows from $P \lor (P \land Q)$...

1. $P \lor (P \land Q)$ Given

2. $P \to P$ Direct Proof

    3.1. $P \land Q$ Assumption

    3.?. P ?

3. $(P \land Q) \to P$ Direct Proof

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2. $P \to P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim ∧: 3.1
3. $(P \wedge Q) \to P$	Direct Proof
4. P	Cases: 1, 2, 3

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2.1. P	Assumption
2.?. P	?
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim ∧: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof

Example: Absorption via Cases

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$ Given
    2.1. P Assumption
2. $P \rightarrow P$ Direct Proof
    3.1. $P \wedge Q$ Assumption
    3.2. P Elim ∧: 3.1
3. $(P \wedge Q) \rightarrow P$ Direct Proof
4. P Cases: 1, 2, 3

More Rules for Propositional Logic

More rules makes proofs easier

Principium Contradictionis

$$\frac{\neg A \;;\; A}{\therefore\ F}$$

Reductio Ad Absurdum

$$\frac{B \Rightarrow F}{\therefore\ \neg B}$$

Ex Falso Quodlibet

$$\frac{F}{\therefore\ A}$$

Ad Litteram Verum

$$\frac{\quad}{\therefore\ T}$$

useful for proving things
(and necessary without the Tautology rule)

Rules for Propositional Logic *w/o Tautology*

	Elimination	Introduction
∧	Elim ∧	Intro ∧
∨	Cases	Intro ∨
→	Modus Ponens	Direct Proof
¬	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum

Recall: Important Equivalences

- **Identity**
  - $p \wedge \mathrm{T} \equiv p$
  - $p \vee \mathrm{F} \equiv p$
- **Domination**
  - $p \vee \mathrm{T} \equiv \mathrm{T}$
  - $p \wedge \mathrm{F} \equiv \mathrm{F}$
- **Idempotent**
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- **Commutative**
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- **Associative**
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive**
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Absorption**
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- **Negation**
  - $p \vee \neg p \equiv \mathrm{T}$ — **Does not follow from Latin rules**
  - $p \wedge \neg p \equiv \mathrm{F}$

Example: Distributivity via Latin Rules

Show $(P \land Q) \lor (P \land R)$ follows from $P \land (Q \lor R)$...

1. $P \land (Q \lor R)$	Given
6. $(P \land Q) \lor (P \land R)$	?

Example: Distributivity via Latin Rules

Show $(P \land Q) \lor (P \land R)$ follows from $P \land (Q \lor R)$...

1.	$P \land (Q \lor R)$	Given
2.	P	Elim $\land$: 1
3.	$Q \lor R$	Elim $\land$: 1
6.	$(P \land Q) \lor (P \land R)$	?

hint: proof by cases

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1.	$P \wedge (Q \vee R)$	Given
2.	P	Elim ∧: 1
3.	$Q \vee R$	Elim ∧: 1
4.	$Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
5.	$R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6.	$(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \land Q) \lor (P \land R)$ follows from $P \land (Q \lor R)$...

1. $P \land (Q \lor R)$	Given
2. P	Elim $\land$: 1
3. $Q \lor R$	Elim $\land$: 1
4.1. Q	Assumption
4.?. $(P \land Q) \lor (P \land R)$	?
4. $Q \rightarrow (P \land Q) \lor (P \land R)$	Direct Proof
5. $R \rightarrow (P \land Q) \lor (P \land R)$	?
6. $(P \land Q) \lor (P \land R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \land Q) \lor (P \land R)$ follows from $P \land (Q \lor R)$...

1. $P \land (Q \lor R)$	Given
2. P	Elim ∧: 1
3. $Q \lor R$	Elim ∧: 1
4.1. Q	Assumption
4.2. $P \land Q$	Intro ∧: 2, 4.1
4.3. $(P \land Q) \lor (P \land R)$	Intro ∨: 4.2
4. $Q \rightarrow (P \land Q) \lor (P \land R)$	Direct Proof
5. $R \rightarrow (P \land Q) \lor (P \land R)$	?
6. $(P \land Q) \lor (P \land R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \land Q) \lor (P \land R)$ follows from $P \land (Q \lor R)$...

1.	$P \land (Q \lor R)$	Given
2.	P	Elim ∧: 1
3.	$Q \lor R$	Elim ∧: 1
4.1.	Q	Assumption
4.2.	$P \land Q$	Intro ∧: 2, 4.1
4.3.	$(P \land Q) \lor (P \land R)$	Intro ∨: 4.2
4.	$Q \to (P \land Q) \lor (P \land R)$	Direct Proof
5.1.	R	Assumption
5.3.	$(P \land Q) \lor (P \land R)$	?
5.	$R \to (P \land Q) \lor (P \land R)$	Direct Proof
6.	$(P \land Q) \lor (P \land R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \land Q) \lor (P \land R)$ follows from $P \land (Q \lor R)$...

1. $P \land (Q \lor R)$	Given
2. P	Elim $\land$: 1
3. $Q \lor R$	Elim $\land$: 1
4.1. Q	Assumption
4.2. $P \land Q$	Intro $\land$: 2, 4.1
4.3. $(P \land Q) \lor (P \land R)$	Intro $\lor$: 4.2
4. $Q \rightarrow (P \land Q) \lor (P \land R)$	Direct Proof
5.1. R	Assumption
5.2. $P \land R$	Intro $\land$: 2, 5.1
5.3. $(P \land Q) \lor (P \land R)$	Intro $\lor$: 5.2
5. $R \rightarrow (P \land Q) \lor (P \land R)$	Direct Proof
6. $(P \land Q) \lor (P \land R)$	Cases: 3, 4, 5

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg \boldsymbol{A} \wedge \neg \boldsymbol{B}$ Given

4. $\neg(\boldsymbol{A} \vee \boldsymbol{B})$?

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1.	$\neg \boldsymbol{A} \wedge \neg \boldsymbol{B}$	Given
2.	$\neg \boldsymbol{A}$	Elim ∧: 1
3.	$\neg \boldsymbol{B}$	Elim ∧: 1

hint: proof by contradiction

4.	$\neg(\boldsymbol{A} \vee \boldsymbol{B})$	?

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \lor B)$ follows from $\neg A \land \neg B$...

1.	$\neg \boldsymbol{A} \land \neg \boldsymbol{B}$	**Given**
2.	$\neg \boldsymbol{A}$	**Elim ∧: 1**
3.	$\neg \boldsymbol{B}$	**Elim ∧: 1**

Reductio Ad Absurdum

$$\frac{A \Rightarrow F}{\therefore \neg A}$$

4.	$\neg(\boldsymbol{A} \lor \boldsymbol{B})$	**Absurdum**

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \lor B)$ follows from $\neg A \land \neg B$...

1. $\neg \boldsymbol{A} \land \neg \boldsymbol{B}$	Given
2. $\neg \boldsymbol{A}$	Elim ∧: 1
3. $\neg \boldsymbol{B}$	Elim ∧: 1
4.1. $\boldsymbol{A} \lor \boldsymbol{B}$	Assumption
4.4. $\mathbf{F}$	?
4. $\neg(\boldsymbol{A} \lor \boldsymbol{B})$	Absurdum

can we work forward?

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \lor B)$ follows from $\neg A \land \neg B$...

1.	$\neg \boldsymbol{A} \land \neg \boldsymbol{B}$	Given
2.	$\neg \boldsymbol{A}$	Elim ∧: 1
3.	$\neg \boldsymbol{B}$	Elim ∧: 1
4.1.	$\boldsymbol{A} \lor \boldsymbol{B}$	Assumption
4.2.	$\boldsymbol{A} \to \mathbf{F}$	?
4.3.	$\boldsymbol{B} \to \mathbf{F}$	?
4.4.	$\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4.	$\neg(\boldsymbol{A} \lor \boldsymbol{B})$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1.	$\neg A \wedge \neg B$	Given
2.	$\neg A$	Elim ∧: 1
3.	$\neg B$	Elim ∧: 1
4.1.	$A \vee B$	Assumption
4.2.1.	A	Assumption
4.2.2.	$\mathbf{F}$	?
4.2.	$A \rightarrow \mathbf{F}$	Direct Proof
4.3.	$B \rightarrow \mathbf{F}$	?
4.4.	$\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4.	$\neg(A \vee B)$	Absurdum

Principium Contradictionis

$$\frac{\neg A \; ; \; A}{\therefore F}$$

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg \boldsymbol{A} \wedge \neg \boldsymbol{B}$ Given
2. $\neg \boldsymbol{A}$ Elim ∧: 1
3. $\neg \boldsymbol{B}$ Elim ∧: 1
   - 4.1. $\boldsymbol{A} \vee \boldsymbol{B}$ Assumption
     - 4.2.1. $\boldsymbol{A}$ Assumption
     - 4.2.2. $\mathbf{F}$ Contradiction: 4.2.1, 2
   - 4.2. $\boldsymbol{A} \rightarrow \mathbf{F}$ Direct Proof
   - 4.3. $\boldsymbol{B} \rightarrow \mathbf{F}$?
   - 4.4. $\mathbf{F}$ Cases: 4.1, 4.2, 4.3
4. $\neg(\boldsymbol{A} \vee \boldsymbol{B})$ Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1.	$\neg A \wedge \neg B$	Given
2.	$\neg A$	Elim ∧: 1
3.	$\neg B$	Elim ∧: 1
4.1.	$A \vee B$	Assumption
4.2.1.	A	Assumption
4.2.2.	$\mathbf{F}$	Contradiction: 4.2.1, 2
4.2.	$A \rightarrow \mathbf{F}$	Direct Proof
4.3.1.	B	Assumption
4.3.2.	$\mathbf{F}$	?
4.3.	$B \rightarrow \mathbf{F}$	Direct Proof
4.4.	$\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4.	$\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim ∧: 1
3. $\neg B$	Elim ∧: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \rightarrow \mathbf{F}$	Direct Proof
4.3.1. B	Assumption
4.3.2. $\mathbf{F}$	Contradiction: 4.3.1, 3
4.3. $B \rightarrow \mathbf{F}$	Direct Proof
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Rules for Propositional Logic

	Elimination	Introduction
∧	Elim ∧	Intro ∧
∨	Cases	Intro ∨
→	Modus Ponens	Direct Proof
¬	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum
	Tautology	Equivalent

Inference Rules for Quantifiers: First look

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \quad \textbf{(for any } a\textbf{)}}$$

Elim ∃

Intro ∀

My First Predicate Logic Proof

Domain of Discourse
Integers

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

Intro ∃: P(c) for some c
∴ ∃x P(x)

Elim ∀: ∀x P(x)
∴ P(a) **for any** a

5. $\forall x\, P(x) \rightarrow \exists x\, P(x)$?

The main connective is implication so Direct Proof seems good

My First Predicate Logic Proof

Domain of Discourse
Integers

Intro ∃	P(c) for some c	
	∴ ∃x P(x)	

Elim ∀	∀x P(x)
	∴ P(a) **for any** a

Prove $(\forall x\ P(x)) \to (\exists x\ P(x))$

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

We need an ∃ we don't have so "intro ∃" rule makes sense

1.5. $\exists x\ P(x)$?

1. $\forall x\ P(x) \to \exists x\ P(x)$ **Direct Proof**

My First Predicate Logic Proof

Domain of Discourse
Integers

Intro ∃: P(c) for some c ∴ $\exists x\, P(x)$

Elim ∀: $\forall x\, P(x)$ ∴ P(a) **for any** a

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

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

We need an ∃ we don't have so "intro ∃" rule makes sense

1.5. $\exists x\, P(x)$ **Intro ∃: ?**

That requires P(c) for some c.

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ **Direct Proof**

My First Predicate Logic Proof

Domain of Discourse
Integers

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

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$

Elim ∀: $\dfrac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$

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

1.4. $P(5)$?

1.5. $\exists x\, P(x)$ **Intro ∃: 1.4**

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ **Direct Proof**

My First Predicate Logic Proof

Domain of Discourse
Integers

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

Intro ∃: P(c) for some c ∴ ∃x P(x)

Elim ∀: ∀x P(x) ∴ P(a) for any a

1.1.	$\forall x\, P(x)$	Assumption
1.4.	$P(5)$	Elim ∀: 1.1
1.5.	$\exists x\, P(x)$	Intro ∃: 1.4
1.	$\forall x\, P(x) \rightarrow \exists x\, P(x)$	Direct Proof

My First Predicate Logic Proof

Domain of Discourse
Integers

Intro ∃: P(c) for some c ∴ $\exists x\, P(x)$

Elim ∀: $\forall x\, P(x)$ ∴ P(a) **for any** a

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

1.1.	$\forall x\ P(x)$	Assumption
1.2.	$P(5)$	Elim ∀: 1.1
1.3.	$\exists x\ P(x)$	Intro ∃: 1.2
1.	$\forall x\ P(x) \rightarrow \exists x\ P(x)$	Direct Proof

This follows our usual strategy — eliminate forward, introduce backward — but it is weird…

How did we know to use 5? We didn't! We just guessed it.

Randomly guessing numbers is not good proof strategy!

Our General Proof Strategy

1. $\forall x\,((x > 9) \rightarrow P(x))$ **Given**

...

?. $\exists x\, P(x)$ **?**

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\,((x > 9) \to P(x))$ Given

...

?. $P(5)$?

?. $\exists x\, P(x)$ Intro $\exists$

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\,((x > 9) \rightarrow P(x))$ Given

...

?. $\exists x\, P(x)$?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ / ∃
(**must** wait until you know which one is true)

Our General Proof Strategy

1. $\forall x\, P(x)$ Given
2. $P(100) \rightarrow Q(100)$ Given

Use **elimination** rules to move **down**

...

?. $\exists x\, Q(x)$?

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
...		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \to Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
4.	$P(2)$	Elim ∀: 1
...		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

Exception: Elim ∀
(**must** wait until you know which one *you need*)

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
4.	$P(2)$	Elim ∀: 1
5.	$P(3)$	Elim ∀: 1
...		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\, P(x)$ Given

...

?. $\exists x\, P(x)$?

Exception: Elim ∀
(**must** wait until you know which one *you need*)

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ / ∃
(**must** wait until you know which one is true)

Domain Knowledge

- Intro ∃ and Elim ∀ are *creative* steps
  - need to know the right object to use

    make the wrong choice and the proof won't work
  - the other rules are *mechanical*

    you can apply them blindly without thinking too hard

- Requires your understanding (and intuition) of the objects in question
  - i.e., your "domain knowledge"

Predicate Logic Proofs with more content

- Want to be able to use domain knowledge so that proofs are about things we understand

- Example:

Domain of Discourse
Integers

- Given the basic properties of arithmetic on integers, define:

Predicate Definitions
$\text{Even}(x) := \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) := \exists y\ (x = 2 \cdot y + 1)$

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)

Prove "There is an even number"

Formally: prove ∃x Even(x)

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)

Prove "There is an even number"

Formally: prove ∃x Even(x)

1.	**6 = 2·3**	**Algebra**
2.	∃y (**6 = 2**·y)	**Intro** ∃**: 1**
3.	Even(**6**)	**Definition of** Even
4.	∃x Even(x)	**Intro** ∃**: 3**