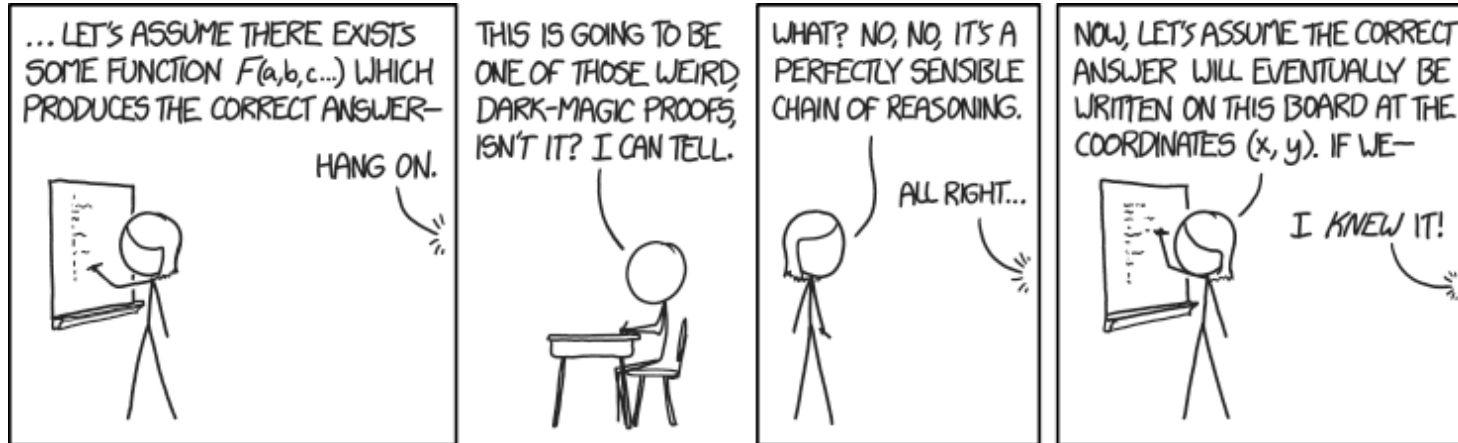


CSE 311: Foundations of Computing

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:

<i>p</i>	<i>q</i>	<i>A(p,q)</i>	<i>B(p,q)</i>
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:

<i>p</i>	<i>q</i>	<i>A(p,q)</i>	<i>B(p,q)</i>
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?

$$(A \rightarrow B) \equiv T$$

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 Wednesday, then you have a 311 lecture today.
 - It is Wednesday.
- Therefore, by Modus Ponens:
 - You have a 311 lecture today.

My First Proof!

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

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

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

My First Proof!

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

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

Proofs can use equivalences too

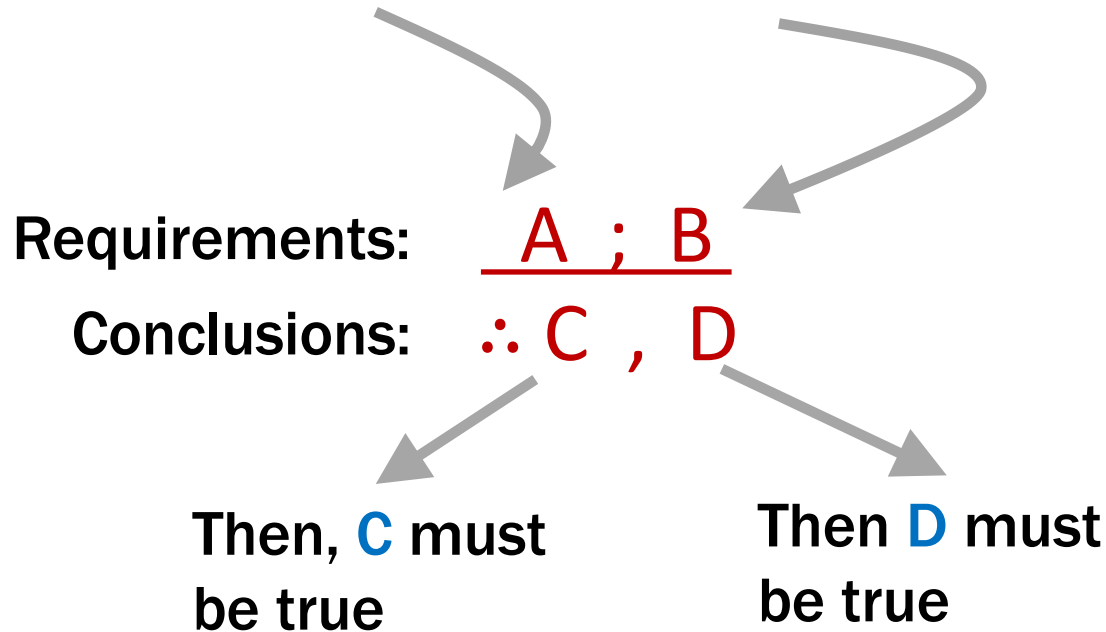
Show that $\neg p$ follows from $p \rightarrow q$ and $\neg q$

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

Inference Rules

If **A** is true and **B** is true

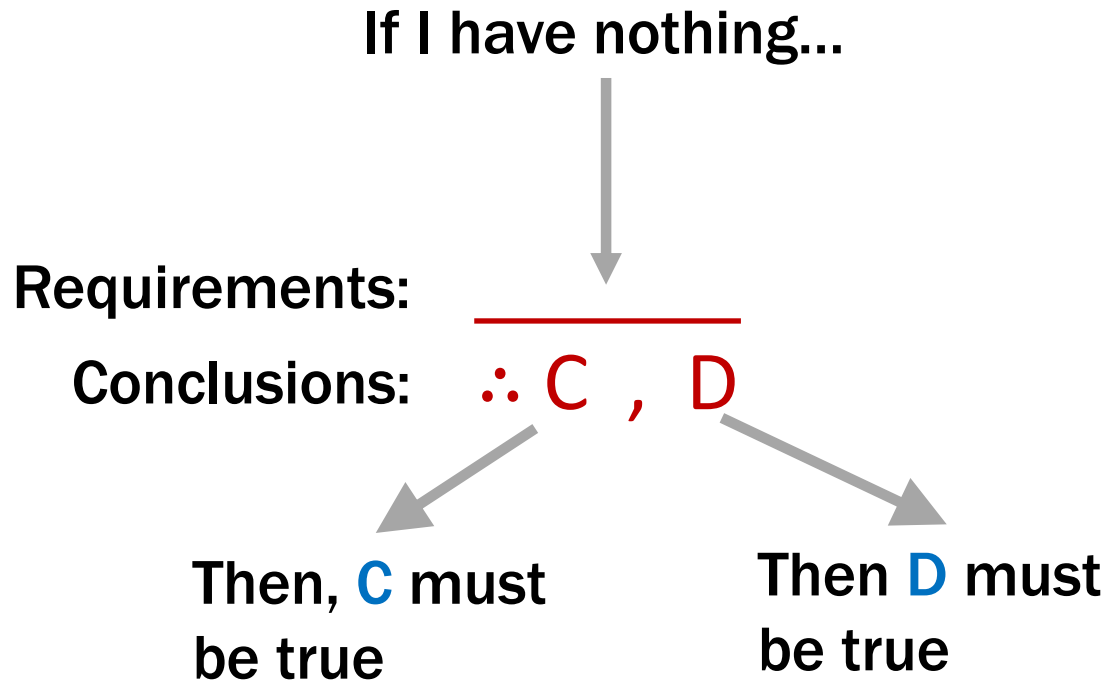


Example (Modus Ponens):

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

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

Axioms: Special inference rules



Example (Excluded Middle):

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

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

Simple Propositional Inference Rules

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

$$\boxed{\text{Elim } \wedge} \frac{A \wedge B}{\therefore A, B}$$

$$\boxed{\text{Intro } \wedge} \frac{A; B}{\therefore A \wedge B}$$

$$\boxed{\text{Elim } \vee} \frac{A \vee B; \neg A}{\therefore B}$$

$$\boxed{\text{Intro } \vee} \frac{A}{\therefore A \vee B, B \vee A}$$

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

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

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 $p, p \rightarrow q$, and $p \wedge q \rightarrow r$

1.	p	Given	$\frac{A ; A \rightarrow B}{\therefore B}$
2.	$p \rightarrow q$	Given	
3.	$p \wedge q \rightarrow r$	Given	$\frac{A \wedge B}{\therefore A, B}$
			$\frac{A ; B}{\therefore A \wedge B}$

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 $p, p \rightarrow q$, and $p \wedge q \rightarrow r$

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

Proofs

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

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!

- | | | |
|----|----------------------------|-----------------------|
| 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 |

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

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

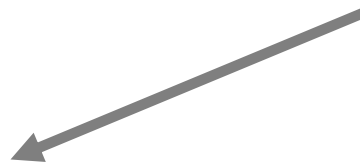
Idea: Work backwards!

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 \rightarrow ” which is MP.

20. $\neg r$

MP: 2,



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

Idea: Work backwards!

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 $\neg r$...

19. q



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

This looks like or-elimination.

19. q

?

20. $\neg r$


MP: 2, 19

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

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

18. $\neg\neg s$  $\neg\neg s$ doesn't show up in the givens but s does and we can use equivalences
19. q \vee Elim: 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 

18. $\neg\neg s$ Double Negation: 17

19. q Elim \vee : 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 \wedge : 1

18. $\neg\neg s$ Double Negation: 17

19. q Elim \vee : 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

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

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

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

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

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

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

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 $(p \wedge q) \rightarrow r$

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

...

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

?



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



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

Our General Proof Strategy

1. $p \rightarrow q$

Given

2. p

Given

3. q

MP: 2, 1

...

?. $p \vee r$

?. q

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

Intro \wedge

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

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

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

1.? $p \rightarrow r$

1. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ 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 \wedge : 1.1

1.3. $q \rightarrow r$ Elim \wedge : 1.1

1.? $p \rightarrow r$

1. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ 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 \wedge : 1.1

1.3. $q \rightarrow r$ Elim \wedge : 1.1

1.4.1. p Assumption

1.4.? r

1.4. $p \rightarrow r$ Direct Proof

1. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ 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 \wedge : 1.1

1.3. $q \rightarrow r$ Elim \wedge : 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. $p \rightarrow r$ Direct Proof

1. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ 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:

$$\boxed{\text{Elim } \wedge} \frac{A \wedge B}{\therefore A, B}$$

$$\boxed{\text{Intro } \wedge} \frac{A; B}{\therefore A \wedge B}$$

$$\boxed{\text{Elim } \vee} \frac{A \vee B; \neg A}{\therefore B}$$

$$\boxed{\text{Intro } \vee} \frac{A}{\therefore A \vee B, B \vee A}$$

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

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

$$\boxed{\text{Excluded Middle}} \frac{}{\therefore A \vee \neg A}$$

Note: only this tautology

Proof by Cases

Some rules can be written in different ways

- e.g., two different elimination rules for “ \vee ”

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

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

second rule is more useful

Example: Absorption via Cases

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

1. $P \vee (P \wedge Q)$

Given

4. P

?

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

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 $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$

Given

2. $P \rightarrow P$

Direct Proof

3.1. $P \wedge Q$

Assumption

3.?. P

?

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. $P \rightarrow P$

Direct Proof

3.1. $P \wedge Q$

Assumption

3.2. P

Elim \wedge : 3.1

3. $(P \wedge Q) \rightarrow P$

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 \wedge : 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. $P \vee (P \wedge Q)$

2.1. P

2. $P \rightarrow P$

3.1. $P \wedge Q$

3.2. P

3. $(P \wedge Q) \rightarrow P$

4. P

Given

Assumption

Direct Proof

Assumption

Elim \wedge : 3.1

Direct Proof

Cases: 1, 2, 3

More Rules for Propositional Logic

More rules makes proofs easier

$$\begin{array}{c} \text{Principium} \\ \text{Contradictionis} \end{array} \frac{\neg A ; A}{\therefore F}$$

$$\begin{array}{c} \text{Reductio Ad} \\ \text{Absurdum} \end{array} \frac{B \Rightarrow F}{\therefore \neg B}$$

$$\begin{array}{c} \text{Ex Falso} \\ \text{Quodlibet} \end{array} \frac{F}{\therefore A}$$

$$\begin{array}{c} \text{Ad Litteram} \\ \text{Verum} \end{array} \frac{}{\therefore T}$$

$$A \wedge \neg A \equiv F \quad \text{Negation}$$

useful for many proving things...

$$F \wedge A \equiv F \quad \text{Domination}$$

$$\begin{aligned} B \rightarrow F &\equiv \neg B \vee F \\ &\equiv \neg B \end{aligned} \quad \text{Law of Implication} \\ \text{Identity}$$

Better Rules for Propositional Logic

	Elimination	Introduction
\wedge	Elim \wedge	Intro \wedge
\vee	Cases	Intro \vee
\rightarrow	Modus Ponens	Direct Proof
\neg	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum

Note: these can't prove everything...

Recall: Important Equivalences

- **Identity**

- $p \wedge \text{T} \equiv p$

- $p \vee \text{F} \equiv p$

- **Domination**

- $p \vee \text{T} \equiv \text{T}$

- $p \wedge \text{F} \equiv \text{F}$

- **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**

- $p \vee \neg p \equiv \text{T}$

Does not follow
from Latin rules

- $p \wedge \neg p \equiv \text{F}$

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

6. $(P \wedge Q) \vee (P \wedge R)$

?

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 \wedge : 1

3. $Q \vee R$

Elim \wedge : 1

hint: proof by cases

6. $(P \wedge Q) \vee (P \wedge R)$

?

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 \wedge : 1

3. $Q \vee R$

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

1. $P \wedge (Q \vee R)$

Given

2. P

Elim \wedge : 1

3. $Q \vee R$

Elim \wedge : 1

4.1. Q

Assumption

4.?. $(P \wedge Q) \vee (P \wedge R)$

?

4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$

Direct Proof

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

1. $P \wedge (Q \vee R)$

Given

2. P

Elim \wedge : 1

3. $Q \vee R$

Elim \wedge : 1

4.1. Q

Assumption

4.2. $P \wedge Q$

Intro \wedge : 2, 4.1

4.3. $(P \wedge Q) \vee (P \wedge R)$

Intro \vee : 4.2

4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$

Direct Proof

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

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

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

Example: De Morgan's Law via Latin Rules

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

1. $\neg A \wedge \neg B$

Given

4. $\neg(A \vee B)$

?

Example: De Morgan's Law via Latin Rules

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

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

hint: proof by contradiction

4. $\neg(A \vee B)$

?

Example: De Morgan's Law via Latin Rules

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

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

4. $\neg(A \vee B)$

Absurdum

$$\begin{array}{c} \text{Reductio Ad} \\ \text{Absurdum} \end{array} \frac{A \Rightarrow F}{\therefore \neg A}$$

Example: De Morgan's Law via Latin Rules

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

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

4.1. $A \vee B$

Assumption

can we work forward?

4.4. **F**

?

4. $\neg(A \vee B)$

Absurdum

Example: De Morgan's Law via Latin Rules

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

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

4.1. $A \vee B$

Assumption

4.2. $A \rightarrow F$

?

4.3. $B \rightarrow F$

?

4.4. 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 $\neg A \wedge \neg B \dots$

1. $\neg A \wedge \neg B$

2. $\neg A$

3. $\neg B$

4.1. $A \vee B$

4.2.1. A

4.2.2. F

4.2. $A \rightarrow F$

4.3. $B \rightarrow F$

4.4. F

4. $\neg(A \vee B)$

Given

Elim \wedge : 1

Elim \wedge : 1

Assumption

Assumption

?

Direct Proof

?

Cases: 4.1, 4.2, 4.3

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 $\neg A \wedge \neg B \dots$

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

4.1. $A \vee B$

Assumption

4.2.1. A

Assumption

4.2.2. F

Contradiction: 4.2.1, 2

4.2. $A \rightarrow F$

Direct Proof

4.3. $B \rightarrow F$

?

4.4. 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 $\neg A \wedge \neg B \dots$

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

4.1. $A \vee B$

Assumption

4.2.1. A

Assumption

4.2.2. F

Contradiction: 4.2.1, 2

4.2. $A \rightarrow F$

Direct Proof

4.3.1. B

Assumption

4.3.2. F

?

4.3. $B \rightarrow F$

Direct Proof

4.4. 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 $\neg A \wedge \neg B \dots$

1. $\neg A \wedge \neg B$

Given

2. $\neg A$

Elim \wedge : 1

3. $\neg B$

Elim \wedge : 1

4.1. $A \vee B$

Assumption

4.2.1. A

Assumption

4.2.2. F

Contradiction: 4.2.1, 2

4.2. $A \rightarrow F$

Direct Proof

4.3.1. B

Assumption

4.3.2. F

Contradiction: 4.3.1, 3

4.3. $B \rightarrow F$

Direct Proof

4.4. F

Cases: 4.1, 4.2, 4.3

4. $\neg(A \vee B)$

Absurdum

Rules for Propositional Logic

	Elimination	Introduction
\wedge	Elim \wedge	Intro \wedge
\vee	Cases	Intro \vee
\rightarrow	Modus Ponens	Direct Proof
\neg	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum
	Excluded Middle	Equivalences...

Inference Rules for Quantifiers: First look

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

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

$\boxed{\text{Elim } \exists}$

$\boxed{\text{Intro } \forall}$

My First Predicate Logic Proof

Domain of Discourse
Integers

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

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

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

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

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

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

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

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

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

1.5. $\exists x P(x)$



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

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

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

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

1.5. $\exists x P(x)$

Intro \exists : 

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

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

1.1. $\forall x P(x)$

Assumption

1.4. $P(5)$

1.5. $\exists x P(x)$



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

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

1.1. $\forall x P(x)$

Assumption

1.4. $P(5)$

Elim \forall : 1.1

1.5. $\exists x P(x)$

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

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

1.1. $\forall x P(x)$

Assumption

1.2. $P(5)$

Elim \forall : 1.1

1.3. $\exists x P(x)$

Intro \exists : 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. $\forall x ((x > 9) \rightarrow P(x))$ 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 \forall / \exists
(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

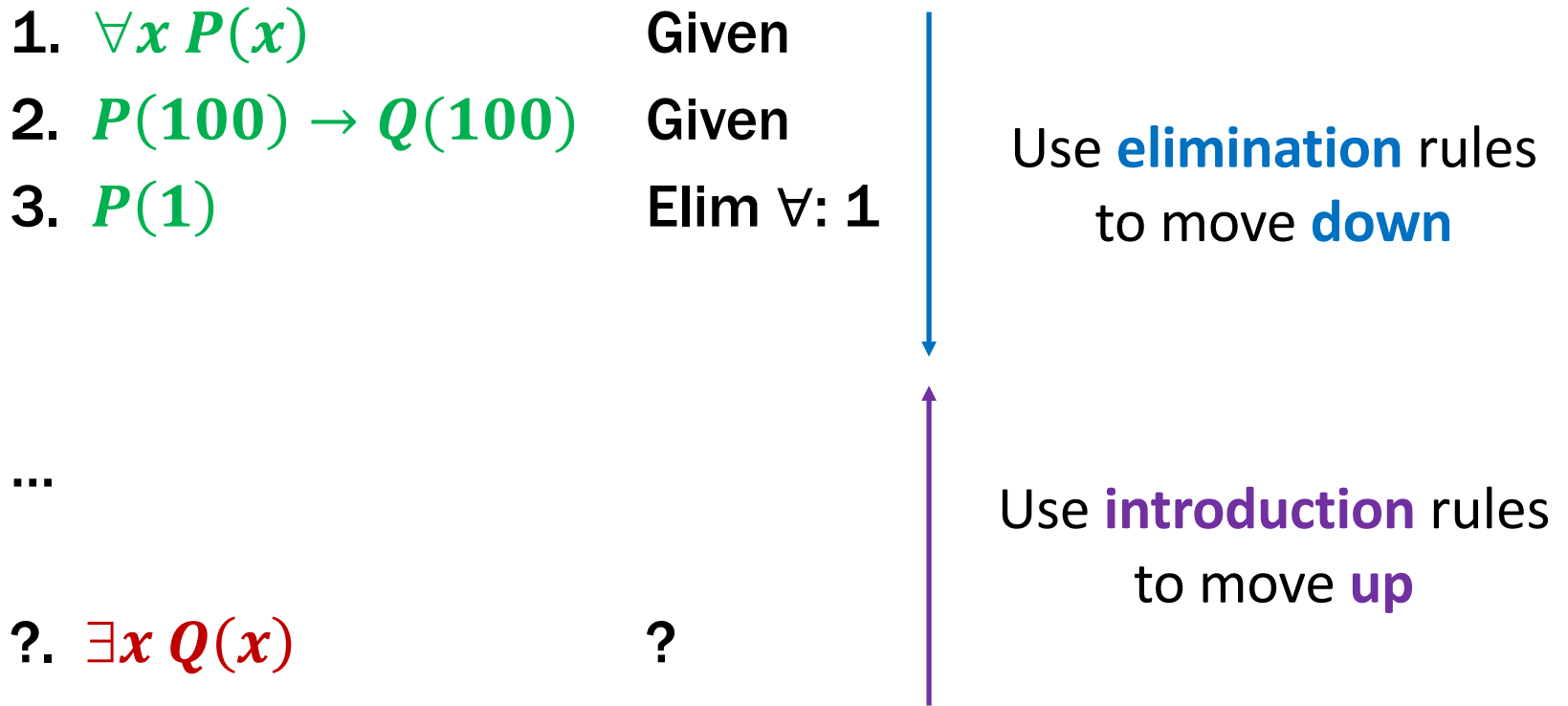
...

- ? $\exists x Q(x)$?

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

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

Our General Proof Strategy



Our General Proof Strategy

1. $\forall x P(x)$

Given

2. $P(100) \rightarrow Q(100)$

Given

3. $P(1)$

Elim \forall : 1

4. $P(2)$

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

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

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 \forall
(must wait until you know which one *you need*)

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

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

Exception: Intro \forall / \exists
(must wait until you know which one is true)

Domain Knowledge

- **Intro \exists and Elim \forall 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
Even(x) := $\exists y (x = 2 \cdot y)$
Odd(x) := $\exists y (x = 2 \cdot y + 1)$

A Not so Odd Example

Domain of Discourse

Integers

Predicate Definitions

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

Odd(x) := $\exists y (x = 2 \cdot y + 1)$

Prove “There is an even number”

Formally: prove $\exists x \text{ Even}(x)$

A Not so Odd Example

Domain of Discourse

Integers

Predicate Definitions

$\text{Even}(x) := \exists y (x = 2 \cdot y)$

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

Prove “There is an even number”

Formally: prove $\exists x \text{ Even}(x)$

- | | | |
|----|-----------------------------|---------------------|
| 1. | $6 = 2 \cdot 3$ | Algebra |
| 2. | $\exists y (6 = 2 \cdot y)$ | Intro \exists : 1 |
| 3. | $\text{Even}(6)$ | Definition of Even |
| 4. | $\exists x \text{ Even}(x)$ | Intro \exists : 3 |

Rules for Definitions

Each definition gives us two new rules, one for *eliminating* and one for introducing it:

$$\boxed{\text{Def of Even}} \quad \frac{\text{Even}(x)}{\therefore \exists y (x = 2y)}$$

$$\boxed{\text{Def of Even}} \quad \frac{\exists y (x = 2y)}{\therefore \text{Even}(x)}$$

We will write "def of" for both rules