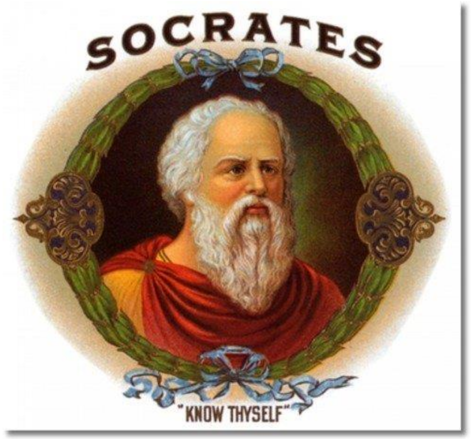
Rules of inference & methods of proof



Dr S Waqar Nabi

School of Computing Science
University of Glasgow

syed.nabi@glasgow.ac.uk

MOTIVATING THE TOPIC

First: Defining “Premise”

- A proposition that is *assumed to be true* in a certain context. E.g.:
  - All men are mortal
  - Socrates is a man
  - All GA students take PA
  - Someone took that last cupcake I had my eye on

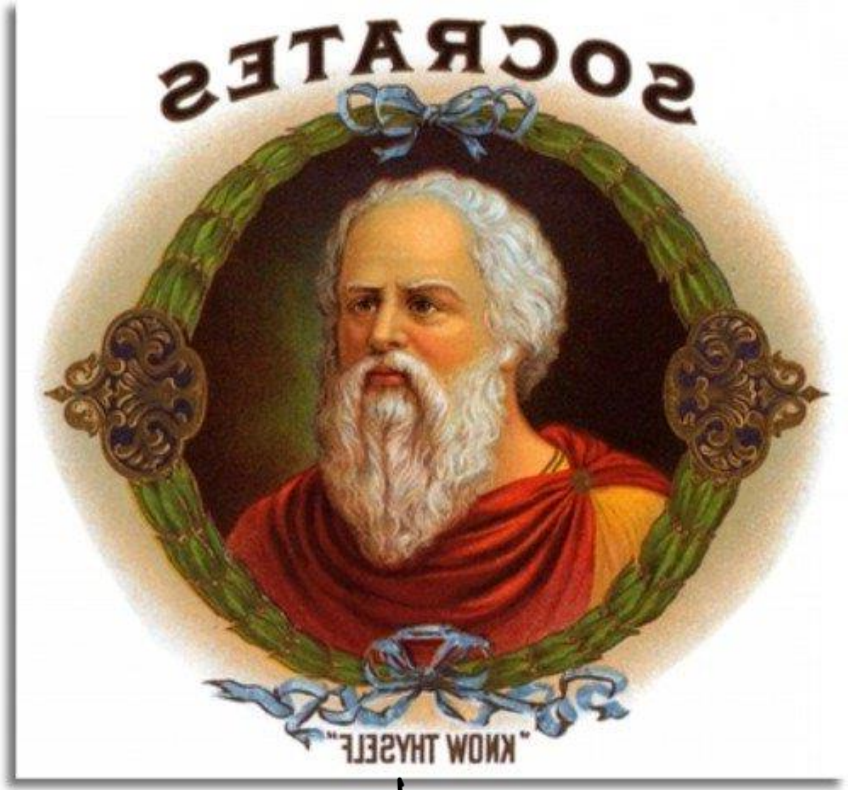
- Premises are used as the basis of *logical reasoning:*
  - e.g., contructing valid arguments

With Apologies to The Socrates Example

- **Say we have the two *premises*:**
  - “All men are mortal.”
  - “My pet cat is a mortal.”

- **And the conclusion:**
  - “My pet cat is a man.”

- **Huh?!**



That doesn't
sound right..

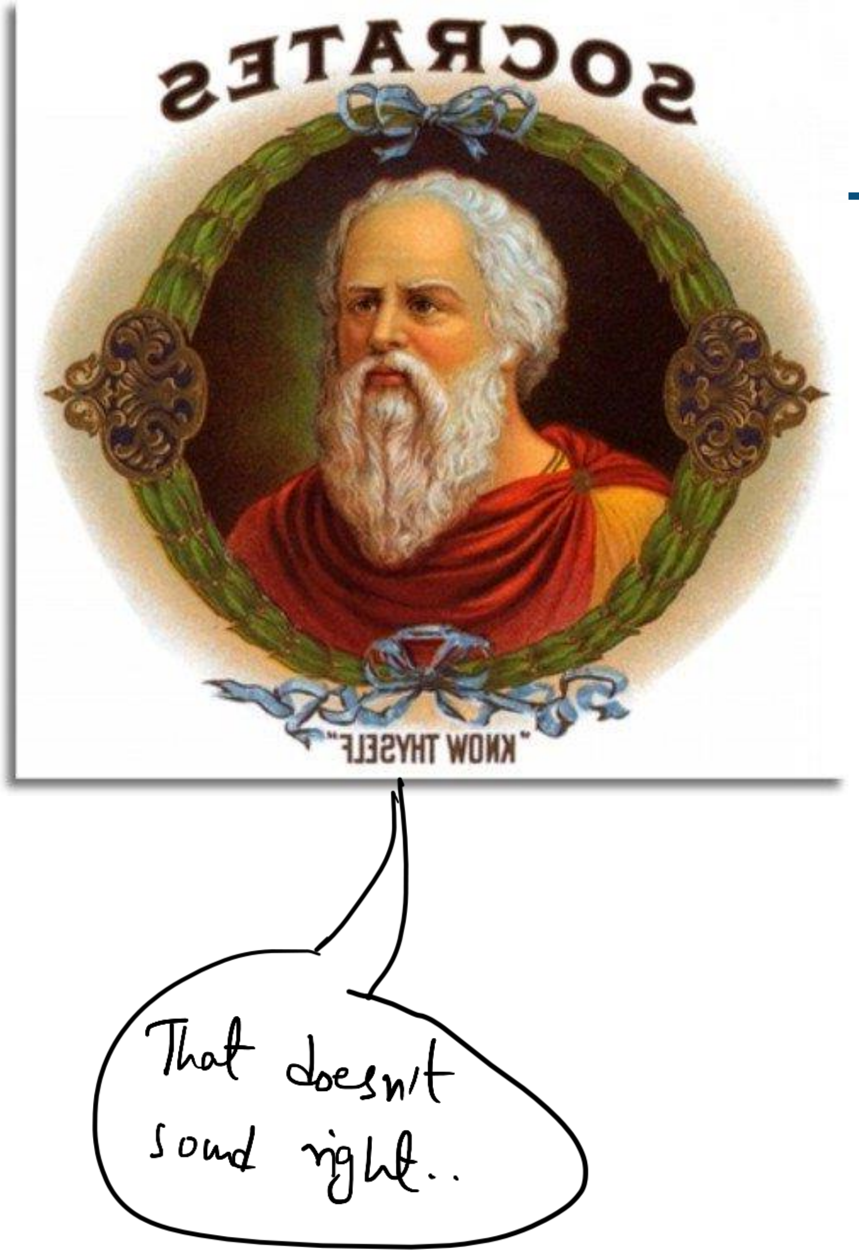
With Apologies to The Socrates Example

- Say we have the two *premises*:
  - "All men are mortal."
  - "My pet cat is a mortal."

- And the conclusion:
  - "My pet cat is a man."

- Huh?!

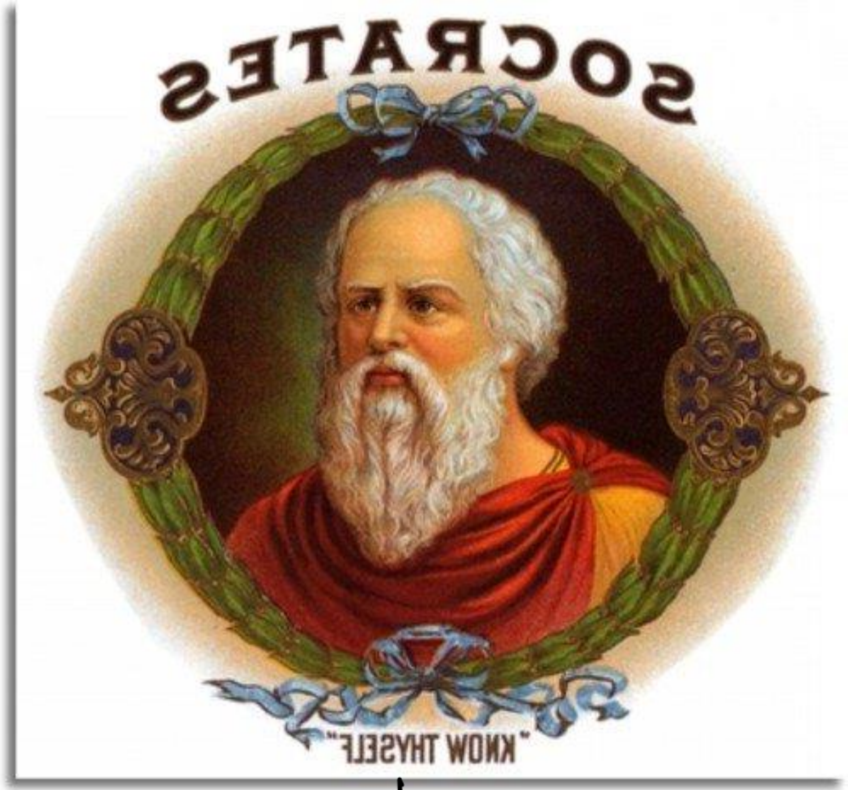
Invalid argument!



With Apologies to The Socrates Example

- Say we have the two *premises*:
  - "All men are mortal."
  - "*Socrates* is a mortal."

- And the conclusion:
  - "*Socrates* is a man."



That doesn't sound right either

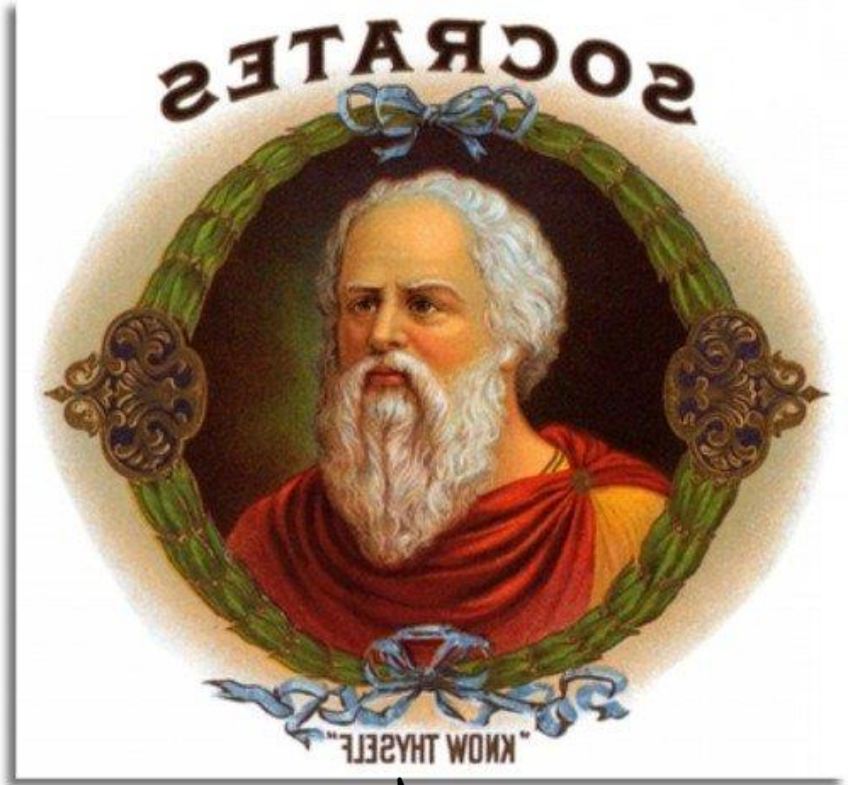
With Apologies to The Socrates Example

- Say we have the two *premises*:
  - "All men are mortal."
  - "*Socrates* is a mortal."

- And the conclusion:
  - "*Socrates* is a man." ✗

Invalid argument!

Still not a valid argument! even if the conclusion happens to be correct.

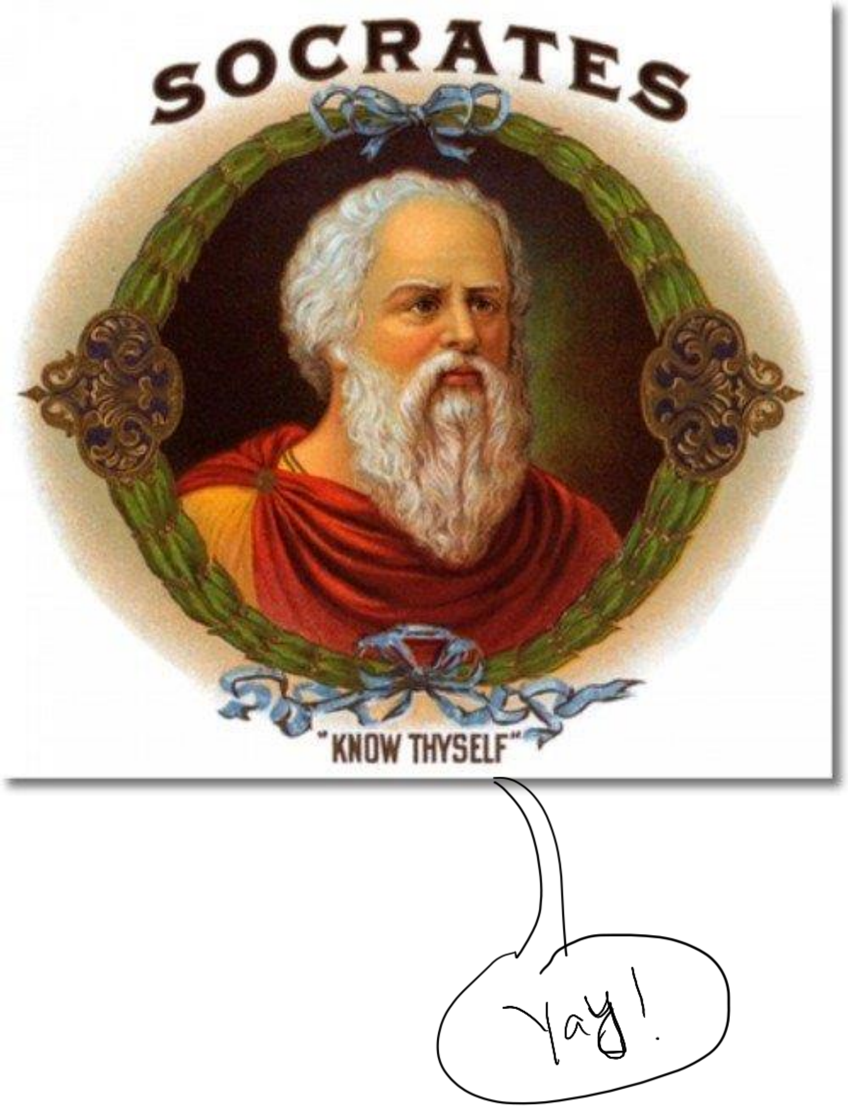


That doesn't sound right either

The Socrates ARGUMENT Example

- Say we have the two *premises*:
  - "All men are mortal."
  - "Socrates is a man."

- And the conclusion:
  - "Socrates is mortal."

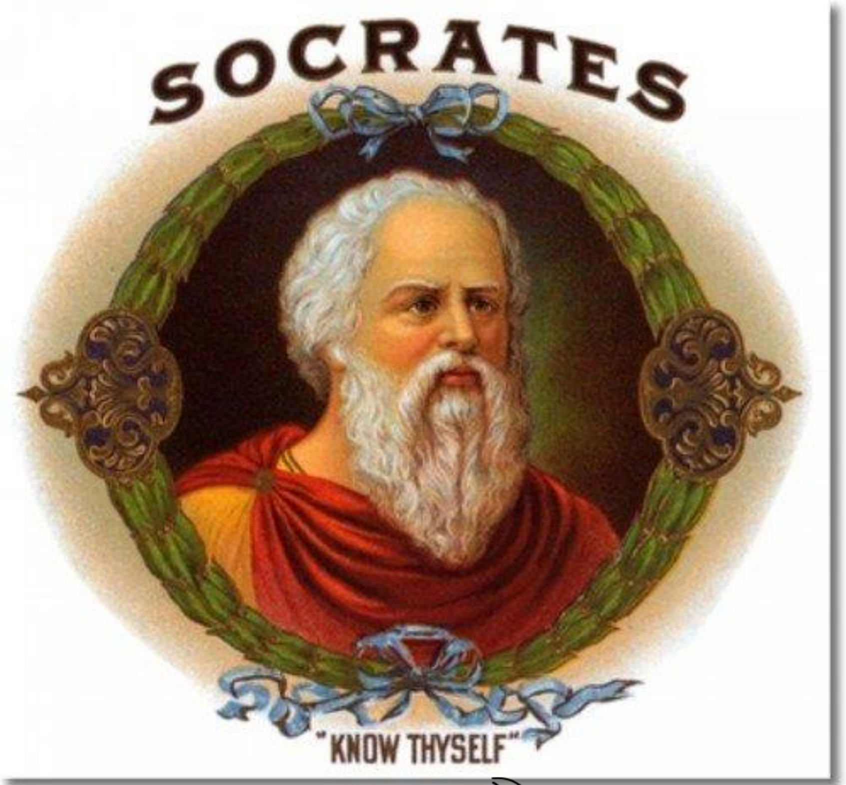


The Socrates ARGUMENT Example

- Say we have the two *premises*:
  - "All men are mortal."
  - "Socrates is a man."

- And the conclusion:
  - "Socrates is mortal."

Valid argument!

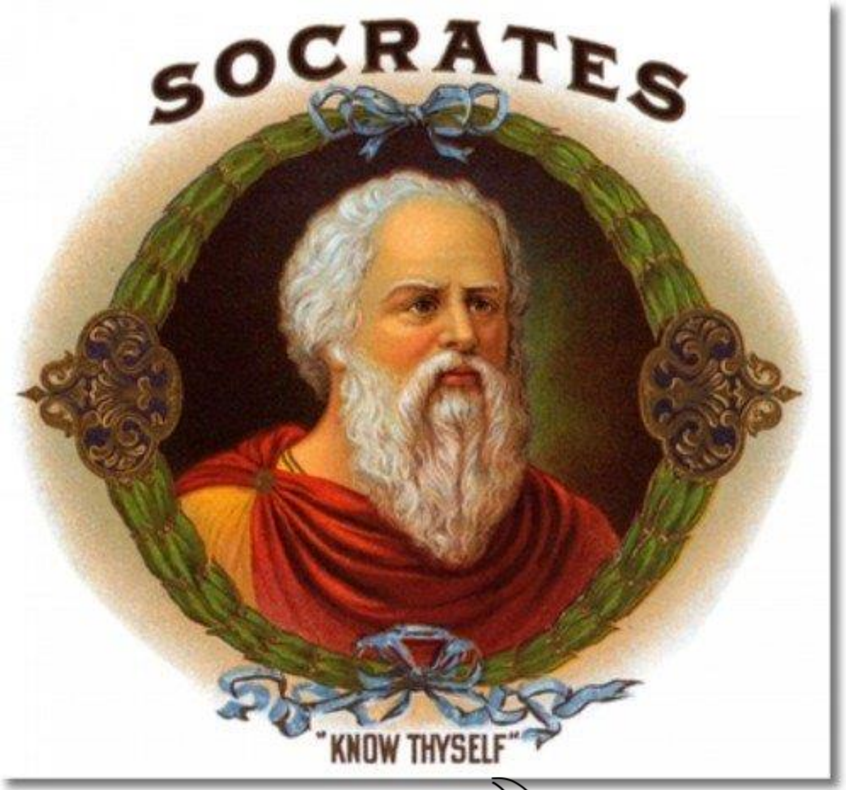


Yay!

The Socrates ARGUMENT Example

- Say we have the two *premises*:
  - "All men are mortal."
  - "Socrates is a man."
- And the conclusion:
  - "Socrates is mortal."

Valid argument!



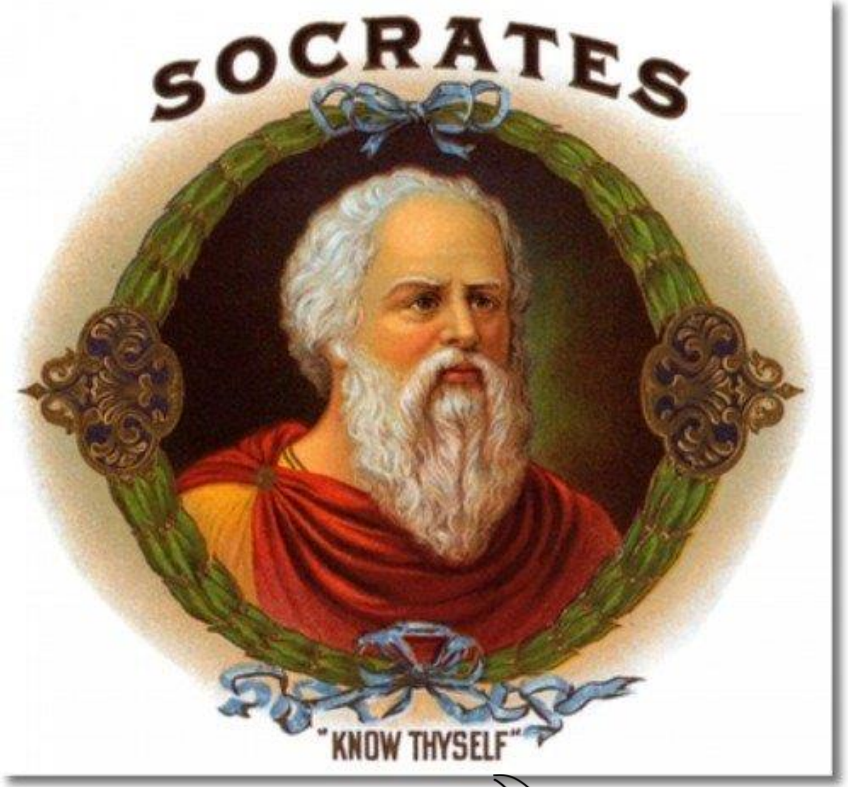
Yay!

- This conclusion is correct? (Yes it is)
- How do we ensure our conclusions are correct given certain premises
  - That is: how do we construct valid arguments
- Are there are other such "valid" *forms* of *arguments*?
- Can we build more complex arguments from simpler arguments?
- How does this apply to CS and SE?

The Socrates ARGUMENT Example

- Say we have the two *premises*:
  - "All men are from Mars."
  - "Socrates is a man."

- And the conclusion:
  - "Socrates is from Mars."



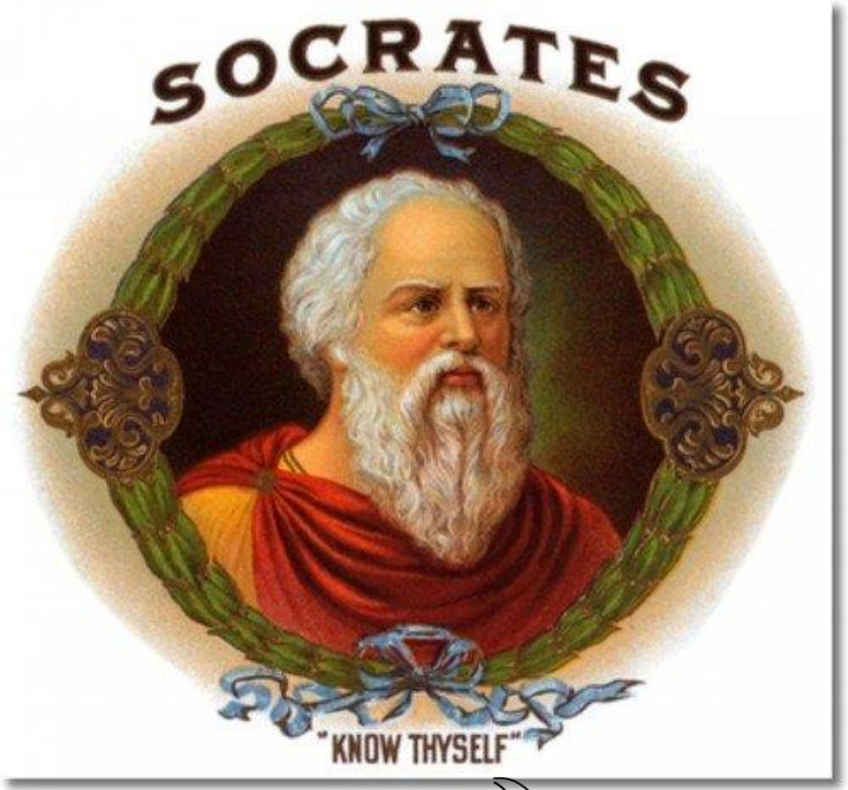
Yay!

The Socrates ARGUMENT Example

- Say we have the two *premises*:
  - "All men are from Mars."
  - "Socrates is a man."

- And the conclusion:
  - "Socrates is from Mars."

Valid argument!



Yay!

Achtung!*

- **We are *only* looking at the *structure of valid arguments*.**
  - That is, going from premises (propositions **assumed** to be true) to
  - a conclusion that *logically follows* from the premises.

- **We are not concerned (here at least) about the "factful-ness" of our conclusions.**
  - Our premises may "in actual fact" be false, but if we use *valid forms of argument,* then the conclusions are also *valid*
    - the conclusions may "in actual fact" be false, we don't care
  - Similarly: We arrive at a conclusion that is "in actual fact" true, but if the argument we used to arrive at that conclusion was *invalid*, so is the conclusion!

* Meaning of Achtung https://www.merriam-webster.com/dictionary/Achtung%21
** Why I know this word: https://www.youtube.com/watch?v=MRpTtNLM6pk&list=PLv8ZCmeG525b0jnqIinTk2m33pMJpfJLa

This Topic...

- We will look at what *arguments* are, and how to construct *valid arguments*
- Once we know how to build correct arguments, we will learn how to create:

proofs for *theorems*

What kind of theorems do want to prove in Computing Science?

  - program verification (correctness, termination, invariance, liveness)
  - security (operating systems, file systems)
  - software specification (consistent, quality of service, functional behaviour)
  - types are correct in a program (type checking)
  - ...

Topic Outline

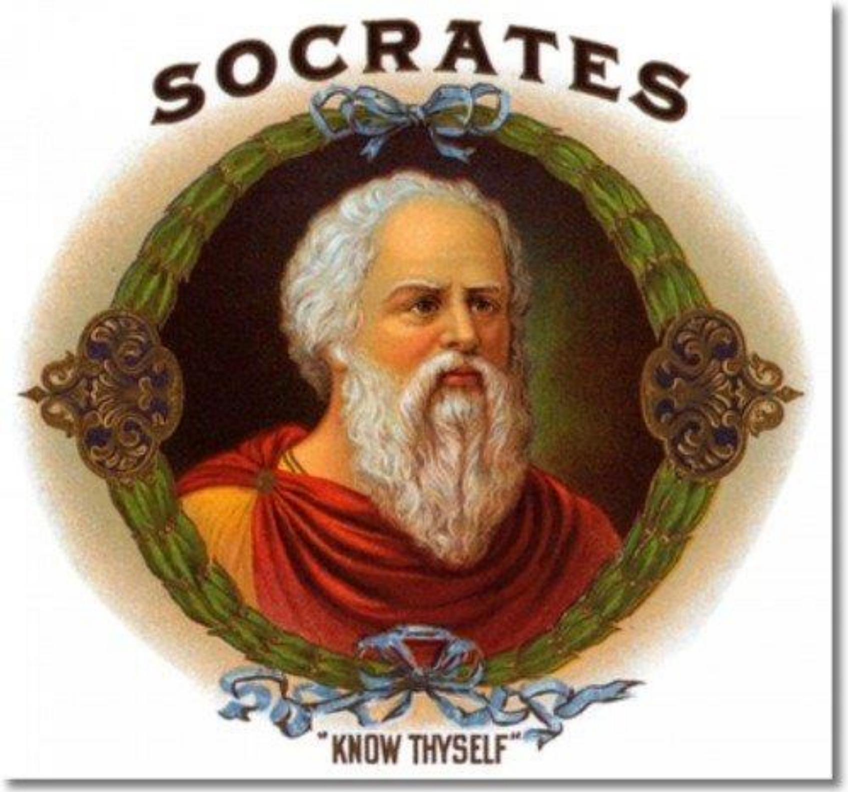
- Valid Arguments and Rules of Inference
- Proof Methods and Strategies

VALID ARGUMENTS & RULES OF INFERENCE

Topic Outline

- Valid Arguments and Rules of Inference
  - Valid Arguments
  - Inference Rules for Propositional Logic
  - Using Rules of Inference to Build Arguments
  - Rules of Inference for Quantified Statements
  - Building Arguments for Quantified Statements

- Proof Methods and Strategies



The Argument: Definition

- An **argument**, more fully a *premise–conclusion* argument, is a two-part system composed of premises and conclusion.

- An argument is *valid* **if and only if** its conclusion is a consequence of its premises.

https://en.wikipedia.org/wiki/Argument%E2%80%93deduction%E2%80%93proof_distinctions

The Argument

- An **argument**, more fully a premise-conclusion argument, is a two-part system composed of premises and conclusion.
- An argument is *valid* if and only if its conclusion is a consequence of its premises.
- **We can express the premises (above the line) and the conclusion (below the line) as an argument:**

premises listed above the bar
$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$
conclusion given below the bar

($\therefore$ stands for "therefore")

Valid Arguments and Rules of Inference

- **We will show how to construct valid arguments in two stages;**
  - first for propositional logic and then
  - for predicate logic.

- **The rules of inference are the essential building block in the construction of valid arguments.**

1. Inference rules for Propositional Logic

2. Inference rules for Predicate Logic
   - Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers.

Valid Arguments and Rules of Inference

- We will show how to construct valid arguments in two stages;
  - first for propositional logic and then
  - for predicate logic.

- The **rules of inference** are the essential building block in the construction of valid arguments.

1. Inference rules for Propositional Logic

2. Inference rules for Predicate Logic
   - Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers.

Arguments in Propositional Logic

premises listed above the bar
conclusion given below the bar

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

- A *argument* in propositional logic is a sequence of propositions.
  - All but the final proposition are called *premises*.
  - The last statement is the *conclusion*.

- The argument is valid if the premises imply the conclusion.

- An *argument form* is an argument that is valid no matter what propositions are substituted into its *propositional variables*.

- Given that an argument form is valid; then if the premises are $p_1, p_2, \ldots, p_n$ and the conclusion is q then

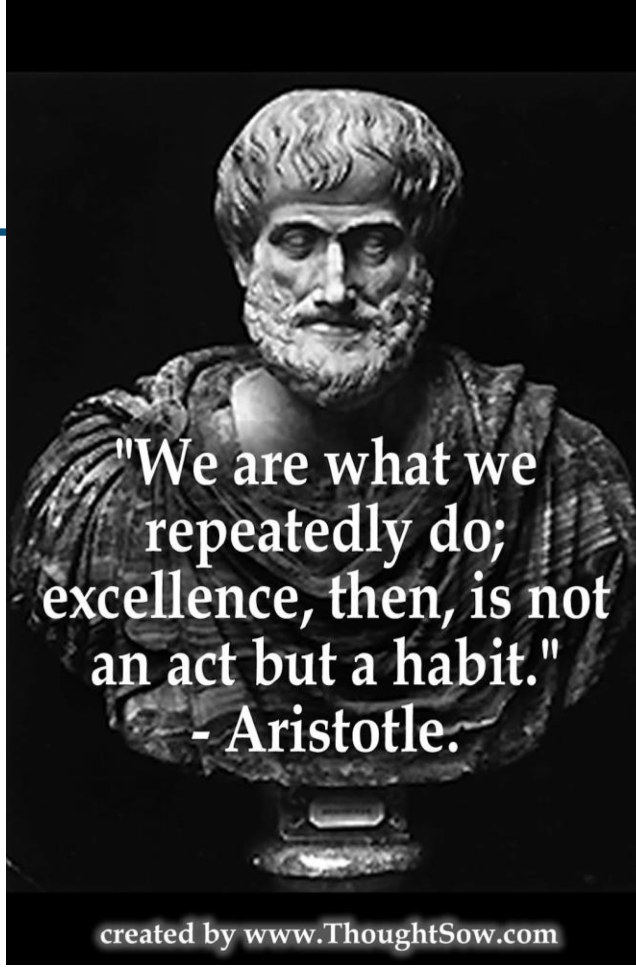
  $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is (i.e. should be) a *tautology*.

- Inference rules are all simple argument forms that will be used to construct more complex argument forms.

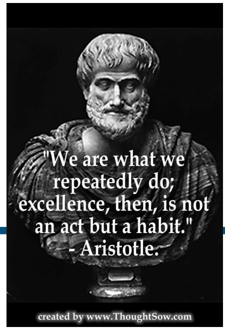
Topic Outline

- Valid Arguments and Rules of Inference
  - Valid Arguments
  - Inference Rules for Propositional Logic
  - Using Rules of Inference to Build Arguments
  - Rules of Inference for Quantified Statements
  - Building Arguments for Quantified Statements

- Proof Methods and Strategies



Rules of Inference for Propositional Logic: *Modus Ponens*



$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

Corresponding Tautology:

$$(p \land (p \to q)) \to q$$

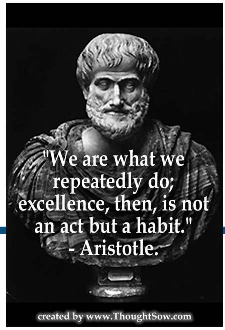
Example:
Let *p* be "It is snowing."
Let *q* be "I will study discrete math."

"If it is snowing, then I will study discrete math."
"It is snowing."

"Therefore , I will study discrete math."

(Remember: p is *sufficient* for q

Rules of Inference for Propositional Logic: *Modus Tollens*



$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Corresponding Tautology:
$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

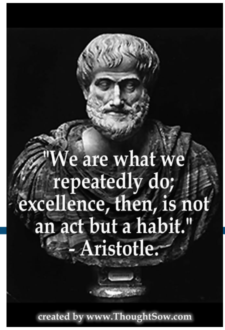
Example:
Let *p* be "it is snowing."
Let *q* be "I will study discrete math."

"If it is snowing, then I will study discrete math."
"I will *not* study discrete math."

"Therefore , it is not snowing."

(Remember: q is *necessary* for p

Rules of Inference for Propositional Logic: *Hypothetical Syllogism*



$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

Corresponding Tautology:

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

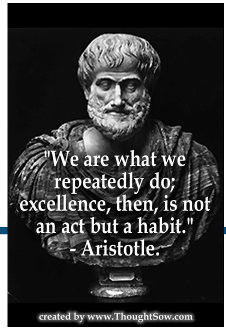
Example:
Let *p* be "it snows."
Let *q* be "I will study discrete math."
Let *r* be "I will get an A."

"If it snows, then I will study discrete math."
"If I study discrete math, I will get an A."

"Therefore , If it snows, I will get an A."

$$\begin{tikzcd} p \arrow[r] \arrow[rr, bend left] & q \arrow[r] & r \end{tikzcd}$$

Rules of Inference for Propositional Logic: *Disjunctive Syllogism*



$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

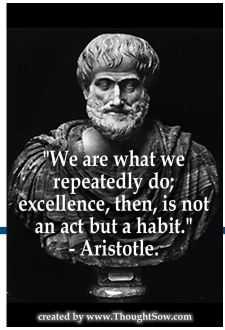
Corresponding Tautology:
$(\neg p \wedge (p \vee q)) \rightarrow q$

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math or I will study English literature."
"I will not study discrete math."

"Therefore , I will study English literature."

Rules of Inference for Propositional Logic: *Addition*



$$\frac{p}{\therefore p \vee q}$$

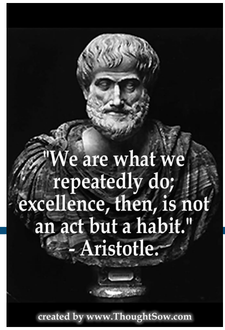
Corresponding Tautology:
$p \rightarrow (p \vee q)$

Example:
Let p be "I will study discrete math."
Let q be "I will visit Paris."

"I will study discrete math."
(p is TRUE)

"Therefore, I will study discrete math or I will visit Paris."
(p V q) is TRUE

Rules of Inference for Propositional Logic: *Addition*



$$\frac{p}{\therefore p \vee q}$$

Corresponding Tautology:

$p \rightarrow (p \vee q)$

Another example: Recall from before

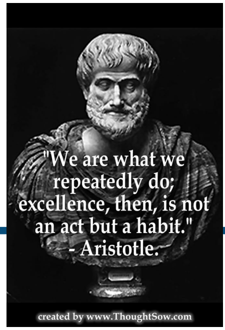
This compound statement is logically correct:

The charge on an electron is negative

OR

Waqar is an amphibious shape-shifting alien.

Rules of Inference for Propositional Logic: *Simplification*



$$\frac{p \wedge q}{\therefore q}$$

Corresponding Tautology:

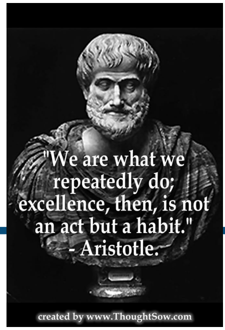
$(p \wedge q) \rightarrow p$

Example:
Let *p* be "I will study discrete math."
Let *q* be "I will study English literature."

"I will study discrete math and English literature"
(p and q is TRUE)

"Therefore, I will study discrete math."
(p is TRUE)

Rules of Inference for Propositional Logic: *Conjunction*



$$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$$

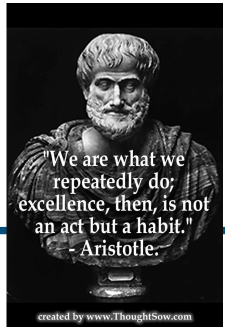
Corresponding Tautology:
$((p) \wedge (q)) \rightarrow (p \wedge q)$

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math."
"I will study English literature."

"Therefore, I will study discrete math and I will study English literature."

Rules of Inference for Propositional Logic: *Resolution*



$$\begin{array}{l} \neg p \vee r \\ p \vee q \\ \hline \therefore q \vee r \end{array}$$

Corresponding Tautology:

$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$

Example:
Let p be "I will study discrete math."
Let r be "I will study English literature."
Let q be "I will study databases."

"I will not study discrete math or I will study English literature."
"I will study discrete math or I will study databases."

"Therefore, I will study databases or I will study English literature."

Rules of Inference for Propositional Logic: Summary

Modus ponens

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline q \end{array}$$

Modus tollens

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \neg p \end{array}$$

Hypothetical Syll'm

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$$

Disjunctive Syll'm

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}$$

Resolution

$$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline q \vee r \end{array}$$

Conjunction

$$\begin{array}{l} p \\ q \\ \hline p \wedge q \end{array}$$

Simplification

$$\begin{array}{l} p \wedge q \\ \hline p \end{array}$$

Addition

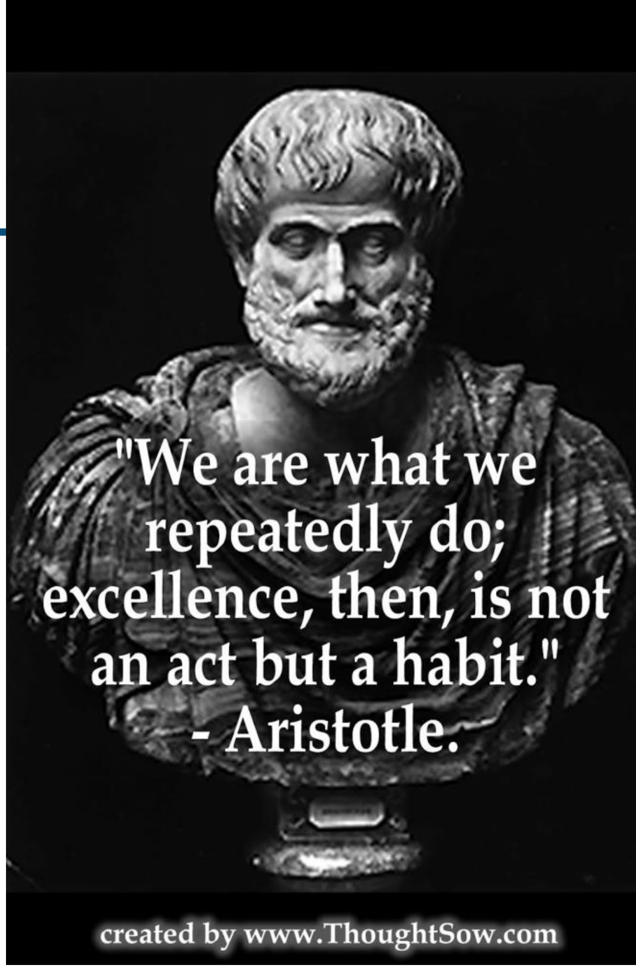
$$\begin{array}{l} p \\ \hline p \vee q \end{array}$$

Rules of Inference for Propositional Logic

Topic Outline

- Valid Arguments and Rules of Inference
  - Valid Arguments
  - Inference Rules for Propositional Logic
  - Using Rules of Inference to Build Arguments
  - Rules of Inference for Quantified Statements
  - Building Arguments for Quantified Statements

- Proof Methods and Strategies



Using the Rules of Inference to Build Valid Arguments

- A *valid argument* is a sequence of statements.
- Each statement is either a premise or follows from previous statements by *rules of inference*.
- The last statement is called conclusion.
- A valid argument takes the following form:

$$\begin{array}{c} S_1 \\ S_2 \\ \cdot \\ \cdot \\ \cdot \\ S_n \\ \hline \therefore C \end{array}$$

Modus ponens
$$\begin{array}{l} p \\ p \rightarrow q \\ \hline q \end{array}$$

Modus tollens
$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \neg p \end{array}$$

Hypothetical Syll'm
$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$$

Disjunctive Syll'm
$$\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}$$

Resolution
$$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline q \vee r \end{array}$$

Conjunction
$$\begin{array}{l} p \\ q \\ \hline p \wedge q \end{array}$$

Simplification
$$\begin{array}{l} p \wedge q \\ \hline p \end{array}$$

Addition
$$\begin{array}{l} p \\ \hline p \vee q \end{array}$$

Rules of Inference for Propositional Logic

Motivating Example

- It is not sunny this afternoon and it is colder than yesterday. If we go swimming, then it is sunny. If we do not go swimming, then we will take a canoe trip. If we take a canoe trip, then we will be home by sunset.

Motivating Example

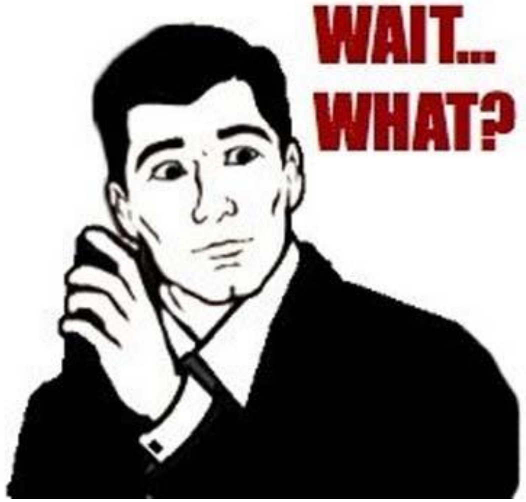
- It is not sunny this afternoon and it is colder than yesterday. If we go swimming, then it is sunny. If we do not go swimming, then we will take a canoe trip. If we take a canoe trip, then we will be home by sunset.

- Therefore: we will be home by sunset

Motivating Example

- It is not sunny this afternoon and it is colder than yesterday. If we go swimming, then it is sunny. If we do not go swimming, then we will take a canoe trip. If we take a canoe trip, then we will be home by sunset.

- Therefore: we will be home by sunset



Rules of Inference to Build Valid Argument – Example

(Atomic) Propositions*

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

**These are simply the base, or "atomic" propositions in our problem statement. We want to assign labels to them to be able to use them in our argument. That is, this is just labelling of propositions. We are not saying (here) which of them are true or false.*

Rules of Inference to Build Valid Argument – Example

(Atomic) Propositions*

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises**

- it is not sunny this afternoon and it is colder than yesterday
- if we go swimming, then it is sunny
- if we do not go swimming, then we will take a canoe trip
- if we take a canoe trip, then we will be home by sunset

**These are simply the base, or "atomic" propositions in our problem statement. We want to assign labels to them to be able to use them in our argument. That is, this is just labelling of propositions. We are not saying (here) which of them are true or false.*

*** The premises are then contructed through the (atomic) propositions and connectives. THESE are the known-to-be-TRUE propositions.*

Rules of Inference to Build Valid Argument – Example

(Atomic) Propositions*

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises**

- it is not sunny this afternoon and it is colder than yesterday
- if we go swimming, then it is sunny
- if we do not go swimming, then we will take a canoe trip
- if we take a canoe trip, then we will be home by sunset

Conclusion

- we will be home by sunset

**These are simply the base, or "atomic" propositions in our problem statement. We want to assign labels to them to be able to use them in our argument. That is, this is just labelling of propositions. We are not saying (here) which of them are true or false.*

*** The premises are then contructed through the (atomic) propositions and connectives. THESE are the known-to-be-TRUE propositions.*

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny
- if we do not go swimming, then we will take a canoe trip
- if we take a canoe trip, then we will be home by sunset

Conclusion

- we will be home by sunset

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny $r \rightarrow p$
- if we do not go swimming, then we will take a canoe trip
- if we take a canoe trip, then we will be home by sunset

Conclusion

- we will be home by sunset

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny $r \rightarrow p$
- if we do not go swimming, then we will take a canoe trip $\neg r \rightarrow s$
- if we take a canoe trip, then we will be home by sunset

Conclusion

- we will be home by sunset

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny $r \rightarrow p$
- if we do not go swimming, then we will take a canoe trip $\neg r \rightarrow s$
- if we take a canoe trip, then we will be home by sunset $s \rightarrow t$

Conclusion

- we will be home by sunset

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny $r \rightarrow p$
- if we do not go swimming, then we will take a canoe trip $\neg r \rightarrow s$
- if we take a canoe trip, then we will be home by sunset $s \rightarrow t$

Conclusion

- we will be home by sunset t

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny $r \rightarrow p$
- if we do not go swimming, then we will take a canoe trip $\neg r \rightarrow s$
- if we take a canoe trip, then we will be home by sunset $s \rightarrow t$

Conclusion

- we will be home by sunset t

Rules of Inference to Build Valid Argument – Example

Propositions

- p: it is sunny this afternoon
- q: it is colder than yesterday
- r: we go swimming
- s: we take a canoe trip
- t: we will be home by sunset

p_1: $\neg p \wedge q$
p_2: $r \rightarrow p$
p_3: $\neg r \rightarrow s$
p_4: $s \rightarrow t$
p_5: t

Premises

- it is not sunny this afternoon and it is colder than yesterday $\neg p \wedge q$
- if we go swimming, then it is sunny $r \rightarrow p$
- if we do not go swimming, then we will take a canoe trip $\neg r \rightarrow s$
- if we take a canoe trip, then we will be home by sunset $s \rightarrow t$

Conclusion

- we will be home by sunset t

We now need to show that given the premises p_1 – p_4, we can build a valid argument to show the conclusion p5 is true

Rules of Inference to Build Valid Argument – Example

Premises $p_1, \dots, p_4$ and conclusion p_5

p_1: $\neg p \wedge q$
p_2: $r \rightarrow p$
p_3: $\neg r \rightarrow s$
p_4: $s \rightarrow t$

---

p_5: t

Modus ponens: $\dfrac{p \quad p \rightarrow q}{q}$

Modus tollens: $\dfrac{\neg q \quad p \rightarrow q}{\neg p}$

Hypothetical Syll'm: $\dfrac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}$

Disjunctive Syll'm: $\dfrac{p \vee q \quad \neg p}{q}$

Resolution: $\dfrac{p \vee q \quad \neg p \vee r}{q \vee r}$

Conjunction: $\dfrac{p \quad q}{p \wedge q}$

Simplification: $\dfrac{p \wedge q}{p}$

Addition: $\dfrac{p}{p \vee q}$

Rules of Inference for Propositional Logic

Rules of Inference to Build Valid Argument – Example

Premises $p_1, \ldots, p_4$ and conclusion p_5

p_1: $\neg p \wedge q$
p_2: $r \rightarrow p$
p_3: $\neg r \rightarrow s$
p_4: $s \rightarrow t$

---

p_5: t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)

Modus ponens: p, $p \rightarrow q$ ∴ q

Modus tollens: $\neg q$, $p \rightarrow q$ ∴ $\neg p$

Hypothetical Syll'm: $p \rightarrow q$, $q \rightarrow r$ ∴ $p \rightarrow r$

Disjunctive Syll'm: $p \vee q$, $\neg p$ ∴ q

Resolution: $p \vee q$, $\neg p \vee r$ ∴ $q \vee r$

Conjunction: p, q ∴ $p \wedge q$

Simplification: $p \wedge q$ ∴ p

Addition: p ∴ $p \vee q$

Rules of Inference for Propositional Logic

Rules of Inference to Build Valid Argument – Example

Premises $p_1, \dots, p_4$ and conclusion p_5

p_1:	$\neg p \wedge q$
p_2:	$r \rightarrow p$
p_3:	$\neg r \rightarrow s$
p_4:	$s \rightarrow t$
p_5:	t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \rightarrow p$ (premise p_2)

Modus ponens: $\dfrac{p \quad p \rightarrow q}{q}$

Modus tollens: $\dfrac{\neg q \quad p \rightarrow q}{\neg p}$

Hypothetical Syll'm: $\dfrac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}$

Disjunctive Syll'm: $\dfrac{p \vee q \quad \neg p}{q}$

Resolution: $\dfrac{p \vee q \quad \neg p \vee r}{q \vee r}$

Conjunction: $\dfrac{p \quad q}{p \wedge q}$

Simplification: $\dfrac{p \wedge q}{p}$

Addition: $\dfrac{p}{p \vee q}$

Rules of Inference for Propositional Logic

Rules of Inference to Build Valid Argument – Example

Premises $p_1, \ldots, p_4$ and conclusion p_5

p_1: $\neg p \wedge q$

p_2: $r \rightarrow p$

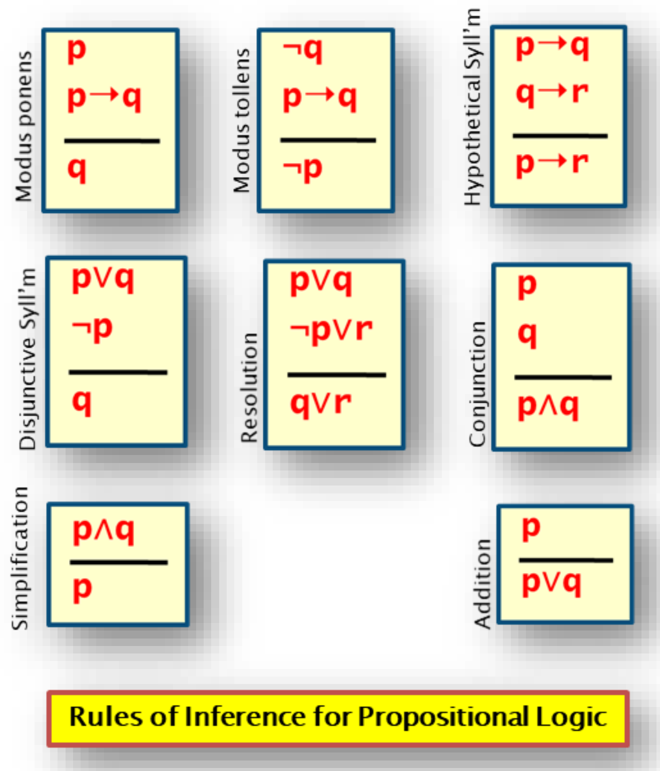
p_3: $\neg r \rightarrow s$

p_4: $s \rightarrow t$

---

p_5: t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \rightarrow p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)



Rules of Inference to Build Valid Argument – Example

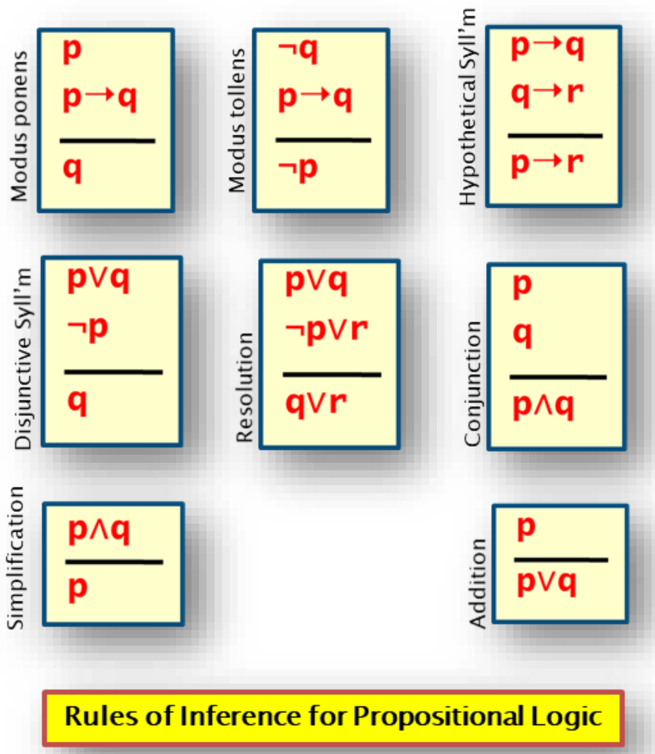
Premises $p_1, \dots, p_4$ and conclusion p_5

p_1: $\neg p \wedge q$
p_2: $r \to p$
p_3: $\neg r \to s$
p_4: $s \to t$

---

p_5: t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \to p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)
5. $\neg r \to s$ (premise p_3)



Rules of Inference to Build Valid Argument – Example

Premises $p_1, \ldots, p_4$ and conclusion p_5

p_1:	$\neg p \wedge q$
p_2:	$r \rightarrow p$
p_3:	$\neg r \rightarrow s$
p_4:	$s \rightarrow t$
p_5:	t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \rightarrow p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)
5. $\neg r \rightarrow s$ (premise p_3)
6. s (modus ponens using 4 and 5)

Modus ponens: $\dfrac{p \quad p \rightarrow q}{q}$

Modus tollens: $\dfrac{\neg q \quad p \rightarrow q}{\neg p}$

Hypothetical Syll'm: $\dfrac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}$

Disjunctive Syll'm: $\dfrac{p \vee q \quad \neg p}{q}$

Resolution: $\dfrac{p \vee q \quad \neg p \vee r}{q \vee r}$

Conjunction: $\dfrac{p \quad q}{p \wedge q}$

Simplification: $\dfrac{p \wedge q}{p}$

Addition: $\dfrac{p}{p \vee q}$

Rules of Inference for Propositional Logic

Rules of Inference to Build Valid Argument – Example

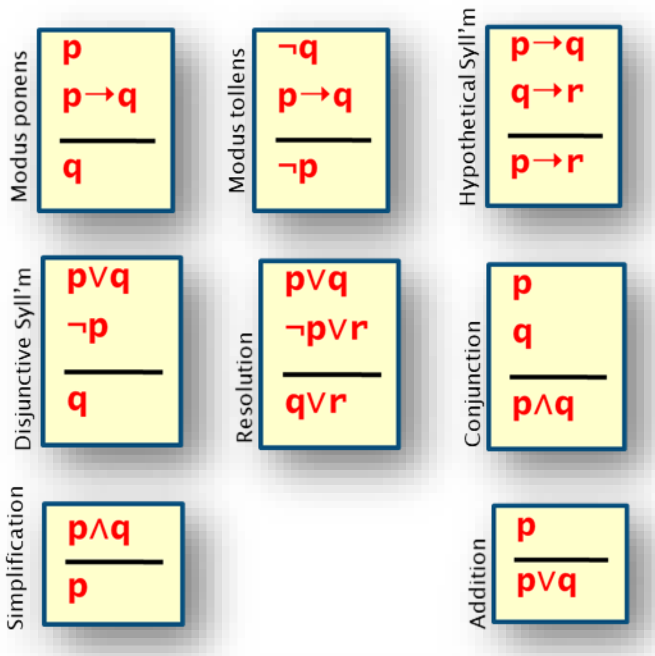
Premises $p_1, \dots, p_4$ and conclusion p_5

p_1: $\neg p \wedge q$
p_2: $r \rightarrow p$
p_3: $\neg r \rightarrow s$
p_4: $s \rightarrow t$

---

p_5: t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \rightarrow p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)
5. $\neg r \rightarrow s$ (premise p_3)
6. s (modus ponens using 4 and 5)
7. $s \rightarrow t$ (premise p_4)



Rules of Inference for Propositional Logic

Rules of Inference to Build Valid Argument – Example

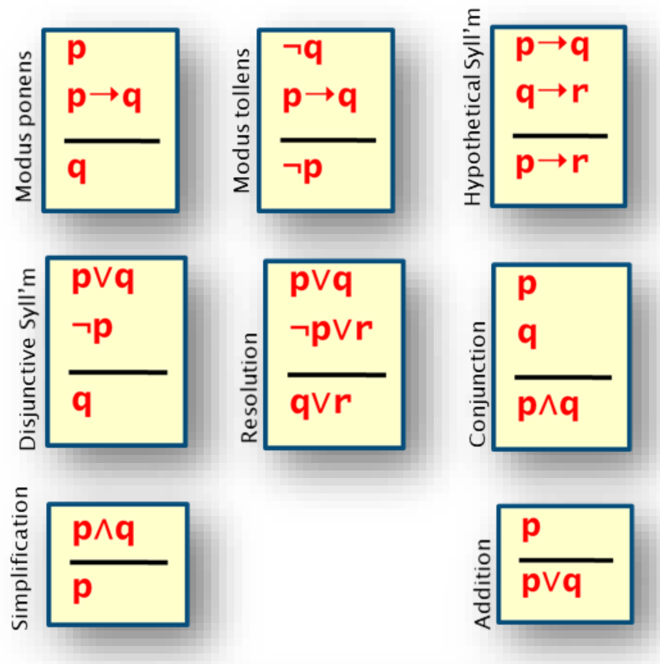
Premises $p_1, \dots, p_4$ and conclusion p_5

p_1: $\neg p \wedge q$
p_2: $r \rightarrow p$
p_3: $\neg r \rightarrow s$
p_4: $s \rightarrow t$

---

p_5: t

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \rightarrow p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)
5. $\neg r \rightarrow s$ (premise p_3)
6. s (modus ponens using 4 and 5)
7. $s \rightarrow t$ (premise p_4)
8. t (modus ponens using 6 and 7)



Rules of Inference for Propositional Logic

Constructing a proof *tree*

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \to p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)
5. $\neg r \to s$ (premise p_3)
6. s (modus ponens using 4 and 5)
7. $s \to t$ (premise p_4)
8. t (modus ponens using 6 and 7)

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg p \wedge q \ \text{(prem1)}}{\neg p \ \text{(simplification)}} \quad r \to p \ \text{(prem2)}}{\neg r \ \text{(modus tollens)}} \quad \neg r \to s \ \text{(prem3)}}{s \ \text{(modus ponens)}} \quad s \to t \ \text{(prem4)}}{t \ \text{(modus ponens)}}$$

Constructing a proof *tree*

1. $\neg p \wedge q$ (premise p_1)
2. $\neg p$ (simplification of 1)
3. $r \rightarrow p$ (premise p_2)
4. $\neg r$ (modus tollens using 2 and 3)
5. $\neg r \rightarrow s$ (premise p_3)
6. s (modus ponens using 4 and 5)
7. $s \rightarrow t$ (premise p_4)
8. t (modus ponens using 6 and 7)

$\neg p \wedge q$ (prem1)

$\neg p$ (simplification) $r \rightarrow p$ (prem2)

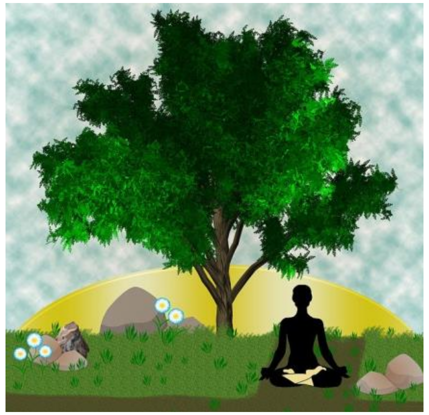
$\neg r$ (modus tollens) $\neg r \rightarrow s$ (prem3)

---

s (modus ponens) $s \rightarrow t$ (prem4)

---

t (modus ponens)



Proof Tree

root at bottom – the (overall) conclusion.

leaves are axioms – the premises *(which themselves may be intermediate "conclusions" from earlier premises)*

Rules of Inference to Build Valid Argument

You might think of this as a game

- you are given some statement(s), and you want to see they form a **valid argument**

A template for solving such problems by building a valid argument

[Think of it as a game ☺]

1. Identify and label the "atomic" propositions

2. Using the given information (relationship between the propositions), list the premises using propositions + connectives

3. Write down the proposition you need to prove (the conclusion)

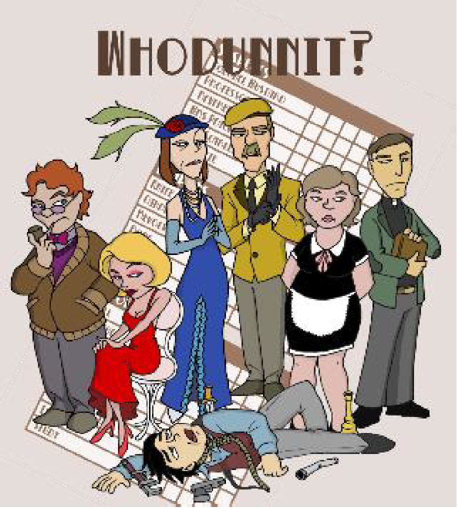
4. Apply RULES OF INFERENCE to derive conclusion from the premises.
   - Creating intermediate premises along the way, as needed

Exercise

- Revisit the "Whodunnit" example from an earlier problem set. Solve it again, only this time, label each step with the appropriate *rule of inference*

Part 4 During a murder investigation, you have gathered the following clues:

1. if the knife is in the store room, then we saw it when we cleared the store room;
2. the murder was committed at the basement or inside the apartment;
3. if the murder was committed at the basement, then the knife is in the yellow dust bin;
4. we did not see a knife when we cleared the store room;
5. if the murder was committed outside the building, then we are unable to find the knife;
6. if the murder was committed inside the apartment, then the knife is in the store room.



The question is: Where is the knife?

Solve this mystery by assigning symbols to propositional statements, building compound propositions from clues provided, and then reasoning through them by applying rules of logical equivalences.

Rules of Inference to Build Valid Argument – A More Relevant Example for Us

invariant

Always true throughout a program

Assume we know:

- if ($y>4$ and $z<10$), then procedure P will be called (premise1)
- ($x>3$ or $y>4$) is an *invariant* of the program (premise2)

Question: when running my program with program variables x,y,z

and given a state where $x=2$ and $z=4$, will procedure P be called?

Rules of Inference to Build Valid Argument – A More Relevant Example for Us

Invariant
Always true throughout a program

Assume we know:

- if ($y>4$ and $z<10$), then procedure P will be called (premise1)
- ($x>3$ or $y>4$) is an *invariant* of the program (premise2)

Question: when running my program with program variables x,y,z and given a state where $x=2$ and $z=4$, will procedure P be called?

1. Identify and label the "atomic" propositions
2. Using the given information (relationship between the propositions), list the premises using propositions + connectives
3. Write down the proposition you need to prove (the conclusion)
4. Apply RULES OF INFERENCE to derive conclusion from the premises.

Rules of Inference to Build Valid Argument – A More Relevant Example for Us

invariant

Always true throughout a program

Assume we know:

- if ($y>4$ and $z<10$), then procedure P will be called (premise1)
- ($x>3$ or $y>4$) is an *invariant* of the program (premise2)

Question: when running my program with program variables **x,y,z**

and given a state where **$x=2$** and **$z=4$**, will procedure P be called?

Let

p: $y > 4$

q: $z < 10$

r: $x > 3$

s: procedure P is called

1. Identify and label the "atomic" propositions
2. Using the given information (relationship between the propositions), list the premises using propositions + connectives
3. Write down the proposition you need to prove (the conclusion)
4. Apply RULES OF INFERENCE to derive conclusion from the premises.

Rules of Inference to Build Valid Argument – A More Relevant Example for Us

invariant
Always true throughout a program

Assume we know:

- if ($y>4$ and $z<10$), then procedure P will be called (premise1)
- ($x>3$ or $y>4$) is an *invariant* of the program (premise2)

Question: when running my program with program variables **x,y,z**

and given a state where **x=2** and **z=4**, will procedure P be called?

Let

p: $y > 4$

q: $z < 10$

r: $x > 3$

s: procedure P is called

p1: $(p \land q) \rightarrow s$

p2: $(r \lor p)$

p3: $\neg r$

p4: q

----

p5: s

1. Identify and label the given propositions
2. Using the given information (relationship between the propositions), list the premises using propositions + connectives
3. Write down the proposition you need to prove (the conclusion)
4. Apply RULES OF INFERENCE to derive conclusion from the premises.

Rules of Inference to Build Valid Argument – A More Relevant Example for Us

Assume we know:

- if (y>4 and z<10), then procedure P will be called (premise1)
- (x>3 or y>4) is an *invariant* of the program (premise2)

Question: when running my program with program variables x,y,z

and given a state where x=2 and z=4, will procedure P **be called?**

- add the premises: ¬(x>3) (premise3) and z<10 (premise4)

Let

p: $y > 4$

q: $z < 10$

r: $x > 3$

s: procedure P is called

p1: $(p \land q) \rightarrow s$

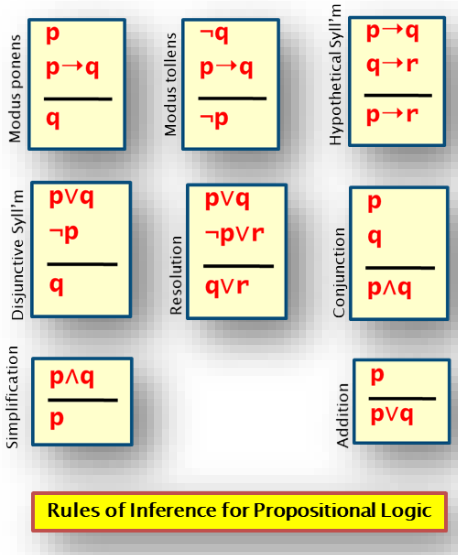
p2: $(r \lor p)$

p3: $\neg r$

p4: q

----

p5: s



Rules of Inference to Build Valid Argument – A More Relevant Example for Us

Assume we know:

- if (y>4 and z<10), then procedure P will be called (premise1)
- (x>3 or y>4) is an *invariant* of the program (premise2)

Question: when running my program with program variables x,y,z

and given a state where x=2 and z=4, will procedure P be called?

- add the premises: ¬(x>3) (premise3)
- and z<10 (premise4)

Let

p: $y > 4$

q: $z < 10$

r: $x > 3$

s: procedure P is called

p1: $(p \wedge q) \rightarrow s$

p2: $(r \vee p)$

p3: $\neg r$

p4: q

----

p5: s

$r \vee p$ *(p2)* $\neg r$ *(p3)*

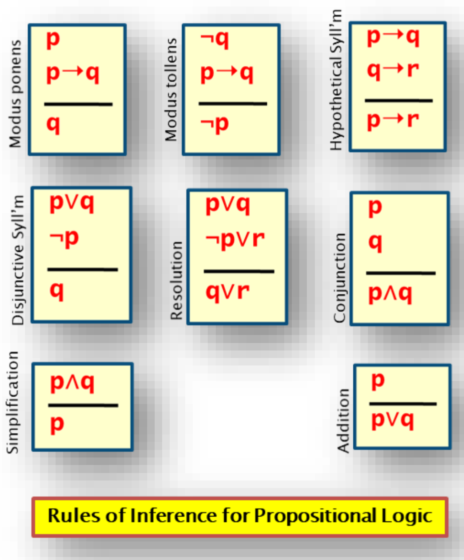
---

p *(disjunctive syllogism)* q *(p4)*

$p \wedge q$ *(Conjunction)* $p \wedge q \rightarrow s$ *(p1)*

---

s *(modus ponens)*



The power of such “deductive” reasoning

- Based on rules of inference which are simple, almost childishly obvious.

- But: given that they are rigorously applied, complex arguments can be built, which are far from obvious intuitively, but are provably, mathematically correct.

Topic Outline

- **Valid Arguments and Rules of Inference**
  - Valid Arguments
  - Inference Rules for Propositional Logic
  - Using Rules of Inference to Build Arguments
  - Rules of Inference for Quantified Statements (Predicate Logic)
  - Building Arguments for Quantified Statements

- **Proof Methods and Strategies**

Handling Quantified Statements

- Valid arguments for quantified statements are a sequence of statements.

- Each statement is either a premise or follows from previous statements by rules of inference which include:
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Quantified Statements → (new in this topic)

- The rules of inference for quantified statements are introduced in the next several slides

Universal Instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal Instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example:

Our domain consists of all dogs and Fido is a dog.

"All dogs are cuddly."

"Therefore, Fido is cuddly."

Universal Generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Used often implicitly in Mathematical Proofs.

Existential Instantiation (EI)

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

Existential Instantiation (EI)

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

Example:

“There is someone who got an A in the course.”
“Let’s call her *a* and say that *a* got an A”

Existential Generalization (EG)

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

Existential Generalization (EG)

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

Example:

"Michelle got an A in the class."
"Therefore, someone got an A in the class."

Rules of Inference for Quantified Statements: Summary

	Instantiation	Generalization
$\forall$	$\dfrac{\forall x P(x)}{\therefore P(c)}$ UI	$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$ UG
$\exists$	$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$ EI	$\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$ EG

Using Rules of Inference

	Instantiation	Generalization
$\forall$	$\dfrac{\forall x P(x)}{\therefore P(c)}$ UI	$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$ UG
$\exists$	$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$ EI	$\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$ EG

Example 1: Using the rules of inference, construct a valid argument to show that

“Jean has a GUID”

is a consequence of the premises:

“Everyone who is a student of GU has a GUID”

“Jean is a student of GU.”

	Instantiation	Generalization
$\forall$	$\dfrac{\forall x P(x)}{\therefore P(c)}$ UI	$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$ UG
$\exists$	$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$ EI	$\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$ EG

Using Rules of Inference

Example 1: Using the rules of inference, construct a valid argument to show that

"Jean has a GUID"

is a consequence of the premises:

"Everyone who is a student of GU has a GUID"

"Jean is a student of GU."

Solution:

Let **S(x)** denote "*x* is a student of GU" and

ID(x) denote "*x* has a GUID" and

Jean be a member of the domain of discourse U = students of GU

Valid Argument: ?

	Instantiation	Generalization
$\forall$	$\dfrac{\forall x P(x)}{\therefore P(c)}$ UI	$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$ UG
$\exists$	$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$ EI	$\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$ EG

Using Rules of Inference

Example 1: Using the rules of inference, construct a valid

argument to show that

"Jean has a GUID"

is a consequence of the premises:

"Everyone who is a student of GU has a GUID"

"Jean is a student of GU."

Solution:

Let S(x) denote "*x* is a student of GU" and

ID(x) denote "*x* has a GUID" and

Jean be a member of the domain of discourse U = students of GU

Valid Argument:

1. $\forall x\,(S(x) \rightarrow ID(x))$	Premise; Everyone who is a student of GU has a GUID
2. $S(J) \rightarrow ID(J)$	UI from (1); If Jean is a student of GU, then she has a GUID
3. $S(J)$	Premise; Jean is a student of GU
4. $ID(J)$	Modes Ponens using 2 and 3: **Jean has a GUID**

Using Rules of Inference – on your own

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion

"Someone who passed the first exam has not read the book."

follows from the premises

"A student in this class has not read the book."

"Everyone in this class passed the first exam."

Solution: Let $C(x)$ denote "x is in this class," $B(x)$ denote "x has read the book," and $P(x)$ denote "x passed the first exam."

First we translate the premises and conclusion into symbolic form.

$$\begin{array}{l} \exists x(C(x) \land \neg B(x)) \\ \forall x(C(x) \rightarrow P(x)) \\ \hline \therefore \ \exists x(P(x) \land \neg B(x)) \end{array}$$

Continued on next slide →

Using Rules of Inference

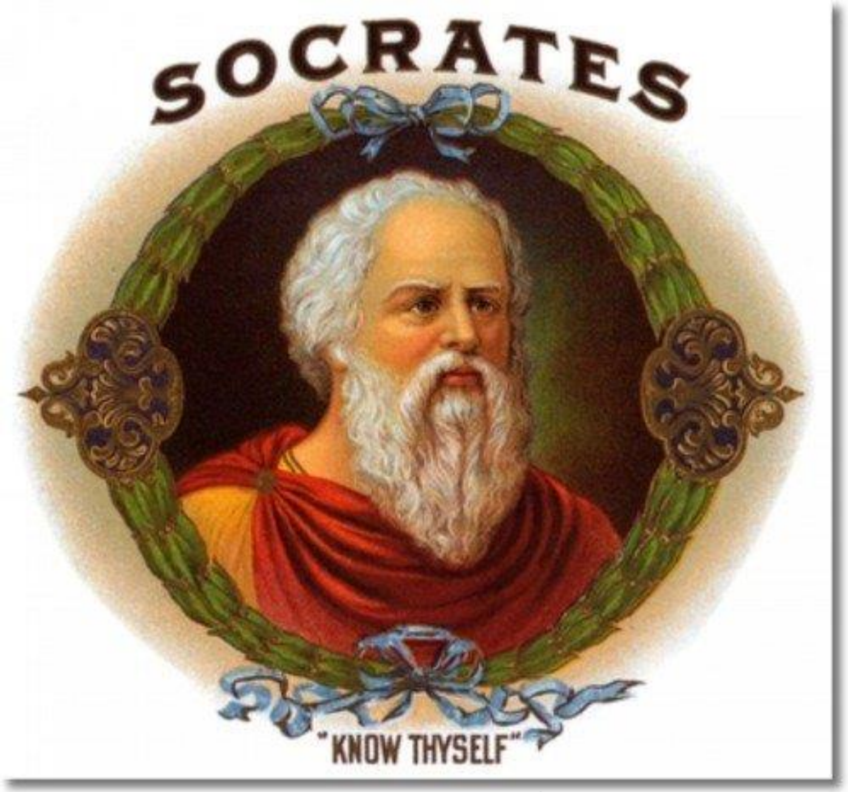
Valid Argument:

Step	**Reason**
1. $\exists x(C(x) \land \neg B(x))$	Premise
2. $C(a) \land \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \land \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$	EG from (8)

Returning to the Socrates Example

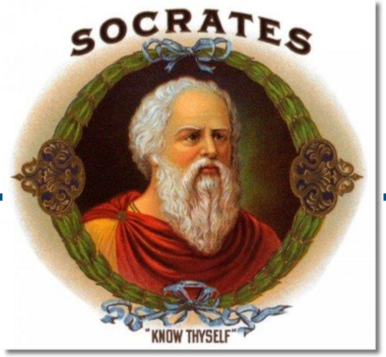
All men are mortal
Socrates is a man

Therefore, Socrates is mortal



(I drank poison with my own hands. Is there no peace for me?)

Returning to the Socrates Example



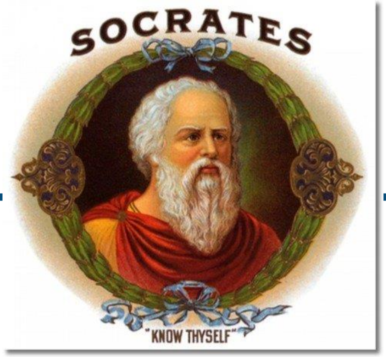
All men are mortal
Socrates is a man

Therefore, Socrates is mortal

$$\forall x(Man(x) \rightarrow Mortal(x))$$

$$Man(Socrates)$$

Returning to the Socrates Example



All men are mortal
Socrates is a man

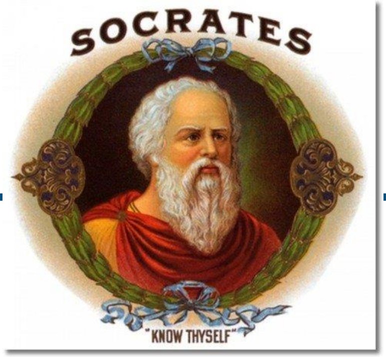
Therefore, Socrates is mortal

$$\forall x(Man(x) \to Mortal(x))$$

$$Man(Socrates)$$

$$\therefore \quad Mortal(Socrates)$$

Solution for Socrates Example



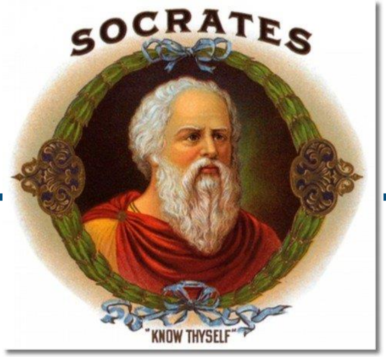
All men are mortal
Socrates is a man

Therefore, Socrates is mortal

$$\begin{array}{ll} & \forall x(Man(x) \rightarrow Mortal(x)) \\ & Man(Socrates) \\ \hline \therefore & Mortal(Socrates) \end{array}$$

Valid Argument

Solution for Socrates Example



All men are mortal
Socrates is a man

Therefore, Socrates is mortal

$$\forall x(Man(x) \rightarrow Mortal(x))$$

$$Man(Socrates)$$

$$\therefore \quad Mortal(Socrates)$$

Valid Argument

Step	**Reason**
1. $\forall x(Man(x) \rightarrow Mortal(x))$	Premise
2. $Man(Socrates) \rightarrow Mortal(Socrates)$	UI from (1)
3. $Man(Socrates)$	Premise
4. $Mortal(Socrates)$	MP from (2) and (3)

Universal Modus Ponens

Universal Modus Ponens combines universal instantiation and modus ponens into one rule.

$$\begin{array}{l} \forall x(P(x) \to Q(x)) \\ P(a), \text{where } a \text{ is a particular} \\ \qquad \text{element in the domain} \\ \hline \therefore Q(a) \end{array}$$

This rule could be used in the Socrates example.

PROOF METHODS AND STRATEGIES

Rules of inference & methods of proof

- Valid Arguments and Rules of Inference

- Proof Methods and Strategies

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.

- In math, CS, and other disciplines, informal proofs which are generally shorter, are mostly used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - Easier to understand and to explain to people.
  - But it is also easier to introduce errors.

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.

- In math, CS, and other disciplines, informal proofs which are generally shorter, are mostly used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - Easier to understand and to explain to people.
  - But it is also easier to introduce errors.

- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent

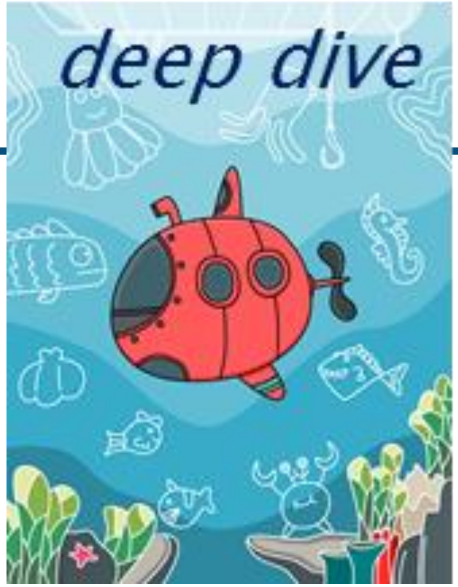
Theorem & Conjecture

- **Theorem**: A statement (proposition) that has been proven to be true, using
  - other theorems
  - *axioms* (propositions which are given as true)*
  - rules of inference

- A *conjecture* is a statement that is being proposed to be true.
  - Once a proof of a conjecture is found, it becomes a theorem.
  - A conjecture may also turn out to be false!

- Premises and Axioms are a similar, but not the same concept. Have a look at this for a good explanation
  https://qr.ae/prNo34

Theorem & Conjecture



- Theorem: A statement that has been proven to be true, using
  - other theorems
  - *axioms* (statements which are given as true)*
  - rules of inference

- A *conjecture* is a statement that is being proposed to be true.
  - Once a proof of a conjecture is found, it becomes a theorem.
  - It may turn out to be false!

Goldbach Conjecture - Numberphile
https://www.youtube.com/watch?v=MxiTG96QOxw

* Premises and Axioms are a similar, but not the same concept. Have a look at this for a good explanation.
https://www.quora.com/What-is-the-difference-between-an-axiom-and-a-premise

Proving Theorems

Proving Theorems

- Many theorems have the form:

$$\forall x(P(x) \rightarrow Q(x))$$

- To prove them, we show that where *c* is an arbitrary element of the domain,

$$P(c) \rightarrow Q(c)$$

- By **universal generalization,** the truth of the original formula follows.

$$\begin{array}{l} P(c) \text{ for an arbitrary } c \\ \hline \therefore \forall x P(x) \end{array}$$

- So, we generally we are trying to prove something of the form:

$$p \rightarrow q$$

Methods of Proof

A proof must be a logical, convincing **argument**

Varying degrees of formality

From some premises **P** prove some conclusion **Q**

- i.e. show that $P \rightarrow Q$ is **true** or $\forall x \in X.(P(x) \rightarrow Q(x))$ is **true**

Direct and Indirect proofs

Direct proof: based on the implication $P \rightarrow Q$

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

Direct and Indirect proofs

Direct proof: based on the implication $P \rightarrow Q$

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

Indirect proof: based on contrapositive $P \rightarrow Q \equiv \neg Q \rightarrow \neg P$

1. assume that **Q** is **false** (**¬Q is true**)
2. show **P** is **false** (**¬P is true**) using
   - rules of inference
   - theorems already proved

Direct and indirect proofs: with Quantifiers

Direct proof: based on the implication $\forall x \in X.(P(x) \rightarrow Q(x))$

1. assume $P(x)$ is **true** for arbitrary $x \in X$
2. show $Q(x)$ is **true** using
   - rules of inference
   - theorems already proved

Indirect proof: based on contrapositive

$$\forall x \in X.(P(x) \rightarrow Q(x)) \equiv \forall x \in X.(\neg Q(x) \rightarrow \neg P(x))$$

1. assume that $Q(x)$ is **false** ($\neg Q(x)$ **is true**) for arbitrary $x \in X$
2. show $P(x)$ is **false** ($\neg P(x)$ **is true**) using
   - rules of inference
   - theorems already proved

Direct proof – Example

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n=2 \cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n=2 \cdot k+1)$
- $\neg$**even**(n) = **odd**(n)
- $\neg$**odd**(n) = **even**(n)

Direct proof – Example

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k+1)$
- $\neg$**even**(n) = **odd**(n)
- $\neg$**odd**(n) = **even**(n)

Prove that the square of an even number is even.

$$\forall n \in \mathbb{Z}.(\text{even}(n) \rightarrow \text{even}(n^2))$$

Direct proof:

Direct proof – Example

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n=2 \cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n=2 \cdot k+1)$
- ¬**even**(n) = **odd**(n)
- ¬**odd**(n) = **even**(n)

Prove that the square of an even number is even.

$$\forall n \in \mathbb{Z}.(\mathrm{even}(n) \rightarrow \mathrm{even}(n^2))$$

Direct proof:

- consider an arbitrary $n \in \mathbb{Z}$ and assume **even**(n)

Direct proof – Example

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k+1)$
- ¬**even**(n) = **odd**(n)
- ¬**odd**(n) = **even**(n)

Prove that the square of an even number is even.

$$\forall n \in \mathbb{Z}.(\mathbf{even}(n) \rightarrow \mathbf{even}(n^2))$$

Direct proof:

- consider an arbitrary $n \in \mathbb{Z}$ and assume **even**(n)
- therefore $n = 2\cdot k$ for some $k \in \mathbb{Z}$

Direct proof – Example

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k+1)$
- $\neg$**even**(n) = **odd**(n)
- $\neg$**odd**(n) = **even**(n)

Prove that the square of an even number is even.

$$\forall n \in \mathbb{Z}.(\mathbf{even}(n) \rightarrow \mathbf{even}(n^2))$$

Direct proof:

- consider an arbitrary $n \in \mathbb{Z}$ and assume **even**(n)
- therefore $n = 2\cdot k$ for some $k \in \mathbb{Z}$
- hence $n^2 = (2\cdot k)^2 = 4\cdot k^2 = 2\cdot(2\cdot k^2)$

Direct proof – Example

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n = 2 \cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n = 2 \cdot k + 1)$
- ¬**even**(n) = **odd**(n)
- ¬**odd**(n) = **even**(n)

Prove that the square of an even number is even.

$$\forall n \in \mathbb{Z}.(\mathrm{even}(n) \rightarrow \mathrm{even}(n^2))$$

Direct proof:

- consider an arbitrary $n \in \mathbb{Z}$ and assume **even**(n)
- therefore $n = 2 \cdot k$ for some $k \in \mathbb{Z}$
- hence $n^2 = (2 \cdot k)^2 = 4 \cdot k^2 = 2 \cdot (2 \cdot k^2)$
- which is by definition even as required

Direct proof – Example

1. assume **P** is **true**
2. show **Q** is **true** using
   - rules of inference
   - theorems already proved

First some definitions and properties we assume (have proved):

- **even**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k)$
- **odd**(n) : $\exists k \in \mathbb{Z}.(n=2\cdot k+1)$
- $\neg$**even**(n) = **odd**(n)
- $\neg$**odd**(n) = **even**(n)

Prove that the square of an even number is even.

$$\forall n \in \mathbb{Z}.(\mathbf{even}(n) \rightarrow \mathbf{even}(n^2))$$

Direct proof:

- consider an arbitrary $n \in \mathbb{Z}$ and assume **even**(n)
- therefore $n = 2\cdot k$ for some $k \in \mathbb{Z}$
- hence $n^2 = (2\cdot k)^2 = 4\cdot k^2 = 2\cdot(2\cdot k^2)$
- which is by definition even as required

Indirect proof – Example

1. assume that **Q** is **false** (**¬Q is true**)
2. show **P** is **false** (**¬P is true**) using
   - rules of inference
   - theorems already proved

Indirect proof – Example

1. assume that **Q** is **false** (**¬Q is true**)
2. show **P** is **false** (**¬P is true**) using
   - rules of inference
   - theorems already proved

Prove: If n^2 is even, then n is even,

- $\forall n \in \mathbb{Z}.(\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$ what we need to prove

  $\equiv \forall n \in \mathbb{Z}.(\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ equivalent contrapositive, which we will aim to prove here

  $\equiv \forall n \in \mathbb{Z}.(\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ inverse of even is odd (property already assumed/proved)

Indirect proof – Example

1. assume that **Q** is **false** (**¬Q is true**)
2. show **P** is **false** (**¬P is true**) using
   - rules of inference
   - theorems already proved

If n^2 is even, then n is even

- $\forall n \in \mathbb{Z}.(\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$ what we need to prove
- $\equiv \forall n \in \mathbb{Z}.(\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ equivalent contrapositive, which we will aim to prove here
- $\equiv \forall n \in \mathbb{Z}.(\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ inverse of even is odd (property already assumed/proved)

Indirect proof:

- consider arbitrary $n \in \mathbb{Z}$ and assume $\mathbf{odd}(n)$

Indirect proof – Example

1. assume that **Q** is **false** (**¬Q is true**)
2. show **P** is **false** (**¬P is true**) using
   - rules of inference
   - theorems already proved

If n^2 is even, then n is even

- $\forall n \in \mathbb{Z}.(\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$

  $\equiv \forall n \in \mathbb{Z}.(\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ contrapositive

  $\equiv \forall n \in \mathbb{Z}.(\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ property already assumed/proved

Indirect proof:

- consider arbitrary $n \in \mathbb{Z}$ and assume $\mathbf{odd}(n)$ [i.e., $\neg\mathbf{even}(n)$]
- then there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k+1$ *(definition of odd numbers)*

Indirect proof – Example

1. assume that **Q** is **false** (**¬Q is true**)
2. show **P** is **false** (**¬P is true**) using
   - rules of inference
   - theorems already proved

If n^2 is even, then n is even

- $\forall n \in \mathbb{Z}. (\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$

  $\equiv \forall n \in \mathbb{Z}. (\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ contrapositive

  $\equiv \forall n \in \mathbb{Z}. (\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ property already assumed/proved

Indirect proof:

- consider arbitrary $n \in \mathbb{Z}$ and assume $\mathbf{odd}(n)$
- then there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k+1$ *(definition of odd numbers)*
- therefore $n^2 = (2 \cdot k+1)^2$

  $= 4 \cdot k^2 + 4 \cdot k + 1$ expanding

  $= \underbrace{\underbrace{2 \cdot (2 \cdot k^2 + 2 \cdot k)}_{\text{even}} + 1}_{\text{odd}}$ which is odd as required

Indirect proof – Example

1. assume that **Q** is **false** (**¬Q** is **true**)
2. show **P** is **false** (**¬P** is **true**) using
   - rules of inference
   - theorems already proved

If n^2 is even, then n is even

- $\forall n\in\mathbb{Z}.(\mathbf{even}(n^2)\rightarrow\mathbf{even}(n))$

  $\equiv \forall n\in\mathbb{Z}.(\neg\mathbf{even}(n)\rightarrow\neg\mathbf{even}(n^2))$ contrapositive

  $\equiv \forall n\in\mathbb{Z}.(\mathbf{odd}(n)\rightarrow\mathbf{odd}(n^2))$ property already assumed/proved

Indirect proof:

- consider arbitrary $n\in\mathbb{Z}$ and assume $\mathbf{odd}(n)$
- then there exists $k\in\mathbb{Z}$ such that $n = 2\cdot k+1$ *(definition of odd numbers)*
- therefore $n^2 = (2\cdot k+1)^2$

  $= 4\cdot k^2 + 4\cdot k + 1$ expanding

  $= \underbrace{\underbrace{2\cdot(2\cdot k^2 + 2\cdot k)}_{\text{even}} + 1}_{\text{odd}}$ which is odd as required

Indirect proof – Why use it?

If $\mathbf{n^2}$ is even, then **n** is even

- $\forall n \in \mathbb{Z}.(\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$

  $\equiv \forall n \in \mathbb{Z}.(\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ contrapositive

  $\equiv \forall n \in \mathbb{Z}.(\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ property already assumed/proved

Could we have proved this directly?

Indirect proof – Why use it?

If n^2 is even, then n is even

- $\forall n \in \mathbb{Z}.(\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$

  $\equiv \forall n \in \mathbb{Z}.(\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ contrapositive

  $\equiv \forall n \in \mathbb{Z}.(\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ property already assumed/proved

Could we have proved this directly?

- consider arbitrary $n \in \mathbb{Z}$ and assume $\mathbf{even}(n^2)$
- $n^2 = 2 \cdot k$
- $n = ?$

Indirect proof – Why use it?

If $\mathbf{n^2}$ is even, then $\mathbf{n}$ is even

- $\forall n \in \mathbb{Z}. (\mathbf{even}(n^2) \rightarrow \mathbf{even}(n))$

  $\equiv \forall n \in \mathbb{Z}. (\neg\mathbf{even}(n) \rightarrow \neg\mathbf{even}(n^2))$ contrapositive

  $\equiv \forall n \in \mathbb{Z}. (\mathbf{odd}(n) \rightarrow \mathbf{odd}(n^2))$ property already assumed/proved

Could we have proved this directly

- consider arbitrary $n \in \mathbb{Z}$ and assume $\mathbf{even}(n^2)$
- $n^2 = 2 \cdot k$
- $n = ?$

Question: why use an indirect proof?

Answer: it might lead to a far easier proof (the dual can also be true)

Proving “if and only if”

To prove $P \leftrightarrow Q$ prove $P \rightarrow Q$ and prove $Q \rightarrow P$

Proving "if and only if"

To prove $P \leftrightarrow Q$ prove $P \rightarrow Q$ and prove $Q \rightarrow P$

Theorem: n is even if and only if n^2 is even

Proof.

first we prove $even(n) \rightarrow even(n^2)$ using a direct proof (done)

second we prove $even(n^2) \rightarrow even(n)$ using an indirect proof (done)

since we have shown that

$even(n) \rightarrow even(n^2)$ and

$even(n^2) \rightarrow even(n)$ hold,

the theorem $even(n^2) \leftrightarrow even(n)$ follows

∎

Proof by contradiction

Assume the negation of what you want to prove and show that this assumption is untenable (leads to a contradiction)

- a proof by contradiction that R holds, assumes R is **`false`**
  and show that is untenable (*cannot hold; leads to a contradiction*)

Proof by contradiction

Assume the negation of what you want to prove and show that this assumption is untenable (leads to a contradiction)

Example: to prove P implies Q (i.e. $P \rightarrow Q$)

- assume property is **false** i.e. *P and not Q* hold (i.e. $P \wedge \neg Q$)
  - recall in truth table for $P \rightarrow Q$ only **false** entry is when P and not Q hold. So, the negation of $P \rightarrow Q$ is $P \wedge \neg Q$
- derive a contradiction
- conclude assumption must be **false**

p	q	p→q
0	0	1
0	1	1
1	**0**	**0**
1	1	1

Proof by contradiction

Assume the negation of what you want to prove and show that this assumption is untenable (leads to a contradiction)

Example: to prove P implies Q (i.e. $P \rightarrow Q$)

- assume property is **false** i.e. *P and not Q* hold (i.e. $P \wedge \neg Q$)
  - recall in truth table for $P \rightarrow Q$ only **false** entry is when P and not Q hold. So, the negation of $P \rightarrow Q$ is $P \wedge \neg Q$
- derive a contradiction
- conclude assumption must be **false**

p	q	p→q
0	0	1
0	1	1
1	**0**	**0**
1	1	1

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

– Say $P(n) = odd(3 \cdot n+2)$, $Q(n) = odd(n)$

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- Say $P(n) = odd(3 \cdot n+2)$, $Q(n) = odd(n)$
- to prove by contradiction $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \land \neg Q(n)$
- Then we will show that $P(n) \land \neg Q(n)$ leads to a contradiction
- i.e. we show $\textbf{odd}(3 \cdot n+2) \ \land \ \neg\textbf{odd}(n)$ leads to a contradiction
- or equivalently, show that $\textbf{odd}(3 \cdot n+2) \ \land \ \textbf{even}(n)$ leads to a contradiction

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \wedge \neg Q(n)$
- Then we will show that $P(n) \wedge \neg Q(n)$ leads to a contradiction
  - *where $P(n)$ denote **odd**$(3 \cdot n+2)$ and $Q(n)$ denote **odd**(n)*
- i.e. we show **odd**$(3 \cdot n+2)$ $\wedge$ $\neg$**odd**(n) leads to a contradiction
- or equivalently, show that odd$(3 \cdot n+2) \wedge$ even(n) leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**$(3 \cdot n+2)$ and **even**(n)

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \wedge \neg Q(n)$
- Then we will show that $P(n) \wedge \neg Q(n)$ leads to a contradiction
  - *where $P(n)$ denote **odd**$(3 \cdot n+2)$ and $Q(n)$ denote **odd**(n)*
- i.e. we show **odd**$(3 \cdot n+2)$ $\wedge$ $\neg$**odd**(n) leads to a contradiction
- or equivalently, show that odd$(3 \cdot n+2) \wedge$ even(n) leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**$(3 \cdot n+2)$ and **even**(n)
- since **even**(n) there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k$
-

Proof by contradiction – Example

Theorem: if 3·n+2 is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \wedge \neg Q(n)$
- Then we will show that $P(n) \wedge \neg Q(n)$ leads to a contradiction
  - *where P(n) denote **odd**(3·n+2) and Q(n) denote **odd**(n)*
- i.e. we show **odd**(3·n+2) $\wedge$ ¬**odd**(n) leads to a contradiction
- or equivalently, show that odd(3·n+2) $\wedge$ even(n) leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**(3·n+2) and **even**(n)
- since **even**(n) there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k$
- hence $3 \cdot n+2 = 3 \cdot (2 \cdot k)+2 = 6 \cdot k+2 = 2 \cdot (3 \cdot k+1)$ which is even
-

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \wedge \neg Q(n)$
- Then we will show that $P(n) \wedge \neg Q(n)$ leads to a contradiction
  - *where $P(n)$ denote **odd**$(3 \cdot n+2)$ and $Q(n)$ denote **odd**(n)*
- i.e. we show **odd**$(3 \cdot n+2) \wedge \neg$**odd**$(n)$ leads to a contradiction
- or equivalently, show that odd$(3 \cdot n+2) \wedge$ even(n) leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**$(3 \cdot n+2)$ and **even**(n)
- since **even**(n) there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k$
- hence $3 \cdot n+2 = 3 \cdot (2 \cdot k)+2 = 6 \cdot k+2 = 2 \cdot (3 \cdot k+1)$ which is even
- that is **even**$(3 \cdot n+2)$ holds
-

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \wedge \neg Q(n)$
- Then we will show that $P(n) \wedge \neg Q(n)$ leads to a contradiction
  - *where $P(n)$ denote $odd(3 \cdot n+2)$ and $Q(n)$ denote $odd(n)$*
- i.e. we show $odd(3 \cdot n+2) \wedge \neg odd(n)$ leads to a contradiction
- or equivalently, show that $odd(3 \cdot n+2) \wedge even(n)$ leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**$(3 \cdot n+2)$ and **even**(n)
- since **even**(n) there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k$
- hence $3 \cdot n+2 = 3 \cdot (2 \cdot k)+2 = 6 \cdot k+2 = 2 \cdot (3 \cdot k+1)$ which is even
- that is **even**$(3 \cdot n+2)$ holds
- but from the assumption we have **odd**$(3 \cdot n+2)$ yielding a contradiction
-

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \land \neg Q(n)$
- Then we will show that $P(n) \land \neg Q(n)$ leads to a contradiction
  - *where $P(n)$ denote **odd**$(3 \cdot n+2)$ and $Q(n)$ denote **odd**(n)*
- i.e. we show **odd**$(3 \cdot n+2) \;\land\; \neg$**odd**$(n)$ leads to a contradiction
- or equivalently, show that odd$(3 \cdot n+2) \land$ even(n) leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**$(3 \cdot n+2)$ and **even**(n)
- since **even**(n) there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k$
- hence $3 \cdot n+2 = 3 \cdot (2 \cdot k)+2 = 6 \cdot k+2 = 2 \cdot (3 \cdot k+1)$ which is even
- that is **even**$(3 \cdot n+2)$ holds
- but from the assumption we have **odd**$(3 \cdot n+2)$ yielding a contradiction
- therefore our assumption is untenable and the theorem holds

Proof by contradiction – Example

Theorem: if $3 \cdot n+2$ is odd, then n is odd

- will prove by contradiction
- to prove $P(n) \rightarrow Q(n)$ will first presume it is false, i.e. $P(n) \wedge \neg Q(n)$
- Then we will show that $P(n) \wedge \neg Q(n)$ leads to a contradiction
  - *where $P(n)$ denote **odd**$(3 \cdot n+2)$ and $Q(n)$ denote **odd**(n)*
- i.e. we show **odd**$(3 \cdot n+2)$ $\wedge$ $\neg$**odd**(n) leads to a contradiction
- or equivalently, show that odd$(3 \cdot n+2) \wedge$ even(n) leads to a contradiction

Proof.

- the proof is by contradiction therefore assume **odd**$(3 \cdot n+2)$ and **even**(n)
- since **even**(n) there exists $k \in \mathbb{Z}$ such that $n = 2 \cdot k$
- hence $3 \cdot n+2 = 3 \cdot (2 \cdot k)+2 = 6 \cdot k+2 = 2 \cdot (3 \cdot k+1)$ which is even
- that is **even**$(3 \cdot n+2)$ holds
- but from the assumption we have **odd**$(3 \cdot n+2)$ yielding a contradiction
- therefore our assumption is untenable and the theorem holds

Trivial and Vacuous Proofs

- *Trivial Proof*: If we know q is true, then

  $p \rightarrow q$ is true as well.

"If it is raining then 1=1."

Trivial and Vacuous Proofs

- *Trivial Proof*: If we know q is true, then

  $p \rightarrow q$ is true as well.

"If it is raining then 1=1."

- *Vacuous Proof*: If we know p is false then

  $p \rightarrow q$ is true as well.

"If $2 + 2 = 5$ then I am from Mars"

Trivial and Vacuous Proofs

- *Trivial Proof*: If we know q is true, then

  $p \to q$ is true as well.

"If it is raining then $1=1$."

- *Vacuous Proof*: If we know p is false then

  $p \to q$ is true as well.

"If $2+2=5$ then I am from Mars"

[Even though these examples seem silly, both trivial and vacuous proofs are often used in *mathematical induction*]

Existence proof

Prove, or disprove something, by presenting an instance (a witness)

This can be done by

- producing an actual instance
- showing how to construct an instance
- showing it would be absurd if an instance did not exist

Example: disprove the assertion "all odd numbers are prime"

- just need to produce one witness, disproving this, i.e. 9 (or 15,…)

Existence proof

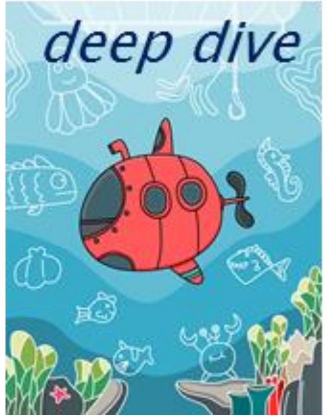
Prove, or disprove something, by presenting an instance (a witness)

This can be done by

- producing an actual instance
- showing how to construct an instance
- showing it would be absurd if an instance did not exist

Example: disprove the assertion “all odd numbers are prime”

- just need to produce one witness, disproving this, i.e. 9 (or 15,…)



Karl Popper's Falsification

https://www.youtube.com/watch?v=wf-sGqBsWv4

What not to do – Fallacies

A fallacy is an inference rule or other proof method that is not logically valid and therefore can yield a false conclusion

Fallacy of affirming the conclusion

- $P \to Q$ is **true**, and Q is **true**
- so P must be **true**?
- no, because **false**$\to$**true** yields **true**
- so $\neg P$ and Q can both be true together

If it's sunny, I'll take you to the beach
I have taken you to the beach.
So it must be sunny

X

Fallacy of denying the hypothesis

- $P \to Q$ is **true** and P is **false**
- so Q must be **false**?
- no, again because **false**$\to$**true** yields **true**

If it's sunny, I'll take you to the beach
It is not sunny
So I will not take you to the beach

X

References

1. Schneider, G. Michael, Judith Gersting, and Sara Baase. *Invitation to Computer Science : Java Version (2nd Edition).*
2. Goodrich, Michael T., Roberto Tamassia, and Michael H. Goldwasser. *Data structures and algorithms in **Java***. John Wiley & Sons (5th Edition onwards).
3. Goodrich, Michael T., Roberto Tamassia, and Michael H. Goldwasser. *Data structures and algorithms in **Python***.
4. Kent D. Lee, Steve Hubbard, *Data Structures and Algorithms with Python*, Springer, 2015.
5. Cormen, Thomas H., et al. *Introduction to algorithms*. MIT press, 2009
6. Sedgewick, Robert. *Algorithms in Java, Parts 1-4 (Fundamental Algorithms, Data Structures, Sorting, Searching)*. Addison Wesley, 2002.
7. *Discrete Mathematics & its Applications*, Kenneth H. Rosen (5th, 6th, 7th or 8th Edition) +companion website
8. Gerard O'Regan, *Concise Guide to Formal Methods*.
9. F Oggier, *Lecture Notes, Discrete Mathematics*.