Methods of Proof

The Vicky Pollard Proof Technique

Prove that when n is even n^2 is even.

Assume n is 0, then n^2 is 0, and that is even

Assume n is 2, then n^2 is 4, and that is even

Assume n is 4, then n^2 is 16, and that is even

Assume n is 6, then n^2 is 36, and that is even

Assume n is -2, then n^2 is [illegible] even also!

Therefore when n is even n^2 is even!

What's wrong with that?

It's got to be a logical, convincing argument!

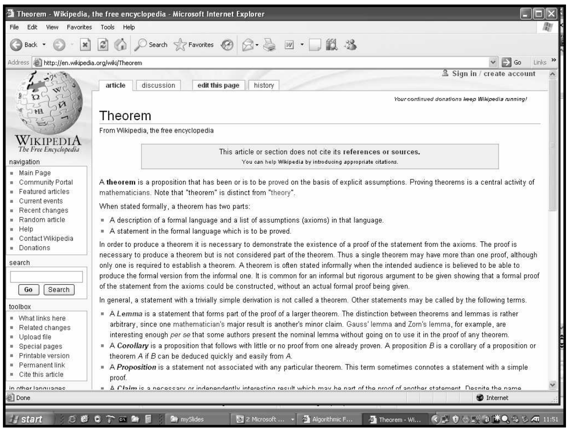
Direct Proof

$$p \to q$$

- (1) assume that p is true
- (2) use
  - rules of inference
  - theorems already proved
  - to show q is true

What's a theorem then?

A theorem is a statement that can be shown to be true


Theorem - Wikipedia, the free encyclopedia - Microsoft Internet Explorer
http://en.wikipedia.org/wiki/Theorem
Sign in / create account
article
discussion
edit this page
history
Your continued donations keep Wikipedia running!
Internet
11:51

Theorem

From Wikipedia, the free encyclopedia

This article or section does not cite its **references or sources.**
You can help Wikipedia by introducing appropriate citations.

A **theorem** is a proposition that has been or is to be proved on the basis of explicit assumptions. Proving theorems is a central activity of mathematicians. Note that "theorem" is distinct from "theory".

When stated formally, a theorem has two parts:

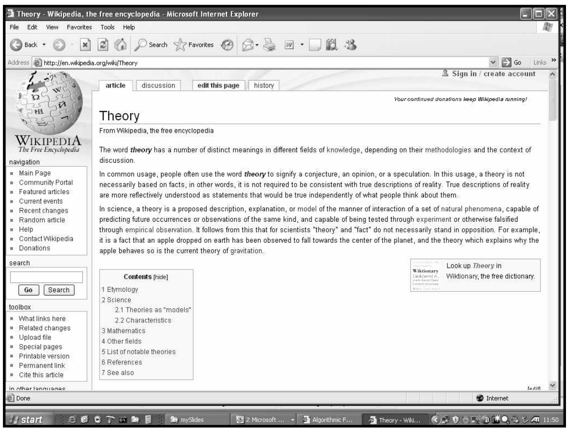
- A description of a formal language and a list of assumptions (axioms) in that language.
- A statement in the formal language which is to be proved.

In order to produce a theorem it is necessary to demonstrate the existence of a proof of the statement from the axioms. The proof is necessary to produce a theorem but is not considered part of the theorem. Thus a single theorem may have more than one proof, although only one is required to establish a theorem. A theorem is often stated informally when the intended audience is believed to be able to produce the formal version from the informal one. It is common for an informal but rigorous argument to be given showing that a formal proof of the statement from the axioms could be constructed, without an actual formal proof being given.

In general, a statement with a trivially simple derivation is not called a theorem. Other statements may be called by the following terms.

- A ***Lemma*** is a statement that forms part of the proof of a larger theorem. The distinction between theorems and lemmas is rather arbitrary, since one mathematician's major result is another's minor claim. Gauss' lemma and Zorn's lemma, for example, are interesting enough *per se* that some authors present the nominal lemma without going on to use it in the proof of any theorem.
- A ***Corollary*** is a proposition that follows with little or no proof from one already proven. A proposition *B* is a corollary of a proposition or theorem *A* if *B* can be deduced quickly and easily from *A*.
- A ***Proposition*** is a statement not associated with any particular theorem. This term sometimes connotes a statement with a simple proof.
- A ***Claim*** is a necessary or independently interesting result which may be part of the proof of another statement. Despite the name

So, what's a theory?


Theory - Wikipedia, the free encyclopedia - Microsoft Internet Explorer
http://en.wikipedia.org/wiki/Theory
Sign in / create account
article
discussion
edit this page
history
Your continued donations keep Wikipedia running!
Internet
11:50

Theory

From Wikipedia, the free encyclopedia

The word ***theory*** has a number of distinct meanings in different fields of knowledge, depending on their methodologies and the context of discussion.

In common usage, people often use the word ***theory*** to signify a conjecture, an opinion, or a speculation. In this usage, a theory is not necessarily based on facts, in other words, it is not required to be consistent with true descriptions of reality. True descriptions of reality are more reflectively understood as statements that would be true independently of what people think about them.

In science, a theory is a proposed description, explanation, or model of the manner of interaction of a set of natural phenomena, capable of predicting future occurrences or observations of the same kind, and capable of being tested through experiment or otherwise falsified through empirical observation. It follows from this that for scientists "theory" and "fact" do not necessarily stand in opposition. For example, it is a fact that an apple dropped on earth has been observed to fall towards the center of the planet, and the theory which explains why the apple behaves so is the current theory of gravitation.

Look up *Theory* in Wiktionary, the free dictionary.

Contents [hide]

Direct Proof

The square of an even number is even

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

- (1) assume even(n)
- (2) n = 2k
- (3) $n^2 = 4k^2 = 2(2k^2)$ which is even
- Q.E.D

Quod erat demonstrandum

That which was to be proved

Indirect Proof

$$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$$

- (0) show that contrapositive is true
- (1) assume that q is false
- (2) use
  - rules of inference
  - theorems already proved
  - to show p is false
- (4) "Since the negation of the conclusion of the implication (¬q) implies that the hypothesis is false (¬p), the original implication is true"

Indirect Proof

If n is an integer and 3n + 2 is even then n is even

$$even(3n+2) \rightarrow even(n)$$
$$odd(n) \rightarrow odd(3n+2)$$

- (1) assume odd(n)
- (2) n = 2k + 1
- (3) 3n + 2
  - = 3(2k + 1) + 2
  - = 6k + 3 + 2
  - = 6k + 5
  - = 6k + 4 + 1
  - = 2(3k + 2) + 1
  - which is odd
- QED

Indirect Proof

If n^2 is even then n is even

$$even(n^2) \to even(n)$$

$$odd(n) \to odd(n^2)$$

assume odd(n)
$\therefore$ n = 2k + 1
$\therefore$ $n^2 = (2k + 1)^2$
$= 4k^2 + 4k + 1$
$= 2(2k^2 + 2) + 1$
which is odd

- QED

Could we prove this directly?

If n^2 is even then n is even

$$even(n^2) \to even(n)$$

assume even(n^2)
$\therefore$ $n^2 = 2k$
$\therefore$ n = …

- QED

Q: Why use an indirect proof?
A: It might be the easy option

Direct Proof again

What's wrong with this?

If n^2 is even then n is even

$$even(n^2) \to even(n)$$

- Suppose that n^2 is even.
- Then $2k = n^2$ for some integer k.
- Let n = 2m for some integer m
- Therefore n is even
- QED

Where did we get "n = 2m" from?
This is circular reasoning, assuming true what we have to prove!

Indirect Proof

It's an argument. Present it well

Theorem: If n^2 is even then n is even

Proof:
We prove this indirectly, i.e. we show that if a number is odd then when we square it we get an odd result. Assume n is odd, and can be represented as 2k + 1, where k is an integer. Then n squared is $4k^2 + 4k + 1$, and we can express that as $4(k^2 + 1) + 1$., and this is an even number plus 1, i.e. an odd number. Therefore, when n^2 is even n is even. QED

Proving *if and only if*

To prove p ↔ q

prove p → q
and
prove q → p

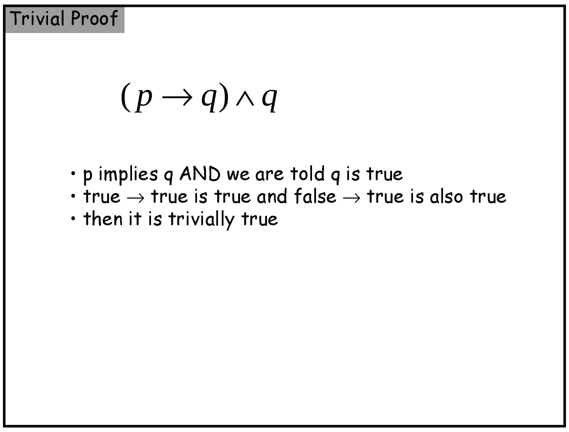
The proof is in 2 **parts**!!

Proving *if and only if*

n is odd if and only if n^2 is odd

To prove p ↔ q
prove p → q & prove q → p

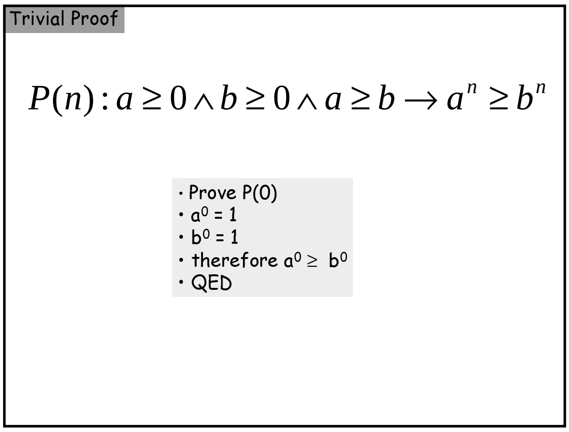
- prove odd(n) → odd(n^2)
  if n is odd then n = 2k + 1
  $n^2 = 4k^2 + 4k + 1$, which is $2(2k^2 + 2k) + 1$
  and this is an odd number
- prove odd(n^2) → odd(n)
  use an indirect proof, i.e. even(n) → even(n^2)
  we have already proved this (slide 3)
- Since we have shown that p → q & q → p we have shown that the theorem is true



Trivial Proof

$$(p \to q) \wedge q$$

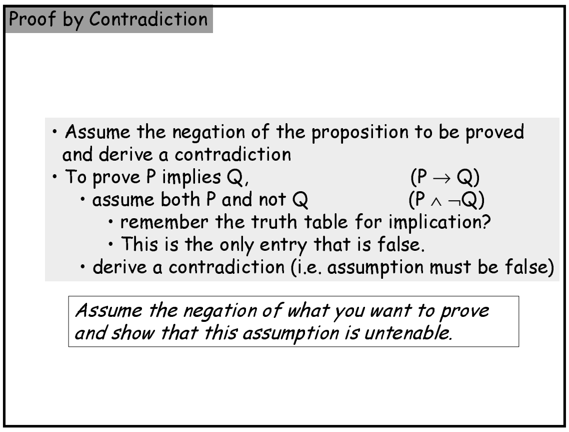
- p implies q AND we are told q is true
- true → true is true and false → true is also true
- then it is trivially true



Trivial Proof

$$P(n): a \geq 0 \wedge b \geq 0 \wedge a \geq b \to a^n \geq b^n$$

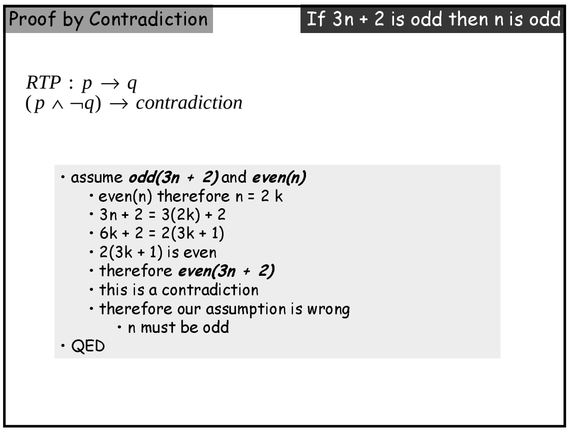
- Prove P(0)
- $a^0 = 1$
- $b^0 = 1$
- therefore $a^0 \geq b^0$
- QED



Proof by Contradiction

- Assume the negation of the proposition to be proved and derive a contradiction
- To prove P implies Q, (P → Q)
  - assume both P and not Q (P ∧ ¬Q)
    - remember the truth table for implication?
    - This is the only entry that is false.
  - derive a contradiction (i.e. assumption must be false)

Assume the negation of what you want to prove and show that this assumption is untenable.

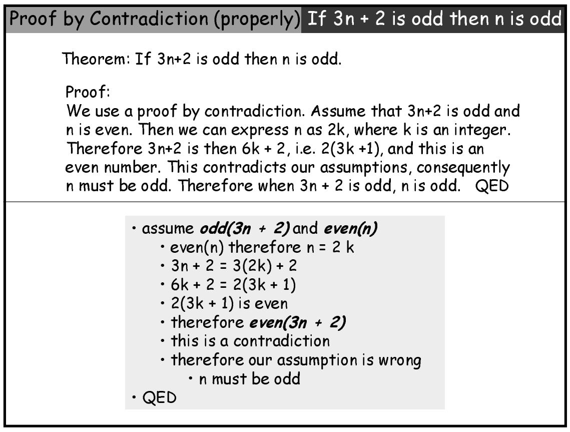


Proof by Contradiction

If 3n + 2 is odd then n is odd

$RTP : p \to q$
$(p \wedge \neg q) \to contradiction$

- assume ***odd(3n + 2)*** and ***even(n)***
  - even(n) therefore n = 2 k
  - 3n + 2 = 3(2k) + 2
  - 6k + 2 = 2(3k + 1)
  - 2(3k + 1) is even
  - therefore ***even(3n + 2)***
  - this is a contradiction
  - therefore our assumption is wrong
    - n must be odd
- QED



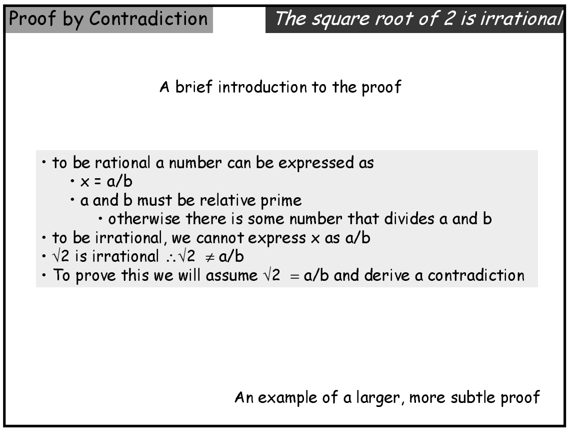
Proof by Contradiction (properly)

If 3n + 2 is odd then n is odd

Theorem: If 3n+2 is odd then n is odd.

Proof:
We use a proof by contradiction. Assume that 3n+2 is odd and n is even. Then we can express n as 2k, where k is an integer. Therefore 3n+2 is then 6k + 2, i.e. 2(3k +1), and this is an even number. This contradicts our assumptions, consequently n must be odd. Therefore when 3n + 2 is odd, n is odd.   QED

- assume ***odd(3n + 2)*** and ***even(n)***
  - even(n) therefore n = 2 k
  - 3n + 2 = 3(2k) + 2
  - 6k + 2 = 2(3k + 1)
  - 2(3k + 1) is even
  - therefore ***even(3n + 2)***
  - this is a contradiction
  - therefore our assumption is wrong
    - n must be odd
- QED



Proof by Contradiction

The square root of 2 is irrational

A brief introduction to the proof

- to be rational a number can be expressed as
  - x = a/b
  - a and b must be relative prime
    - otherwise there is some number that divides a and b
- to be irrational, we cannot express x as a/b
- $\sqrt{2}$ is irrational $\therefore \sqrt{2} \neq a/b$
- To prove this we will assume $\sqrt{2} = a/b$ and derive a contradiction

An example of a larger, more subtle proof

Proof by Contradiction

The square root of 2 is irrational

- assume √2 is rational (and show this leads to a contradiction)
  - ∴ √2 = a/b
  - ∴ a and b are integers
  - ∴ relativePrime(a,b)   i.e. gcd(a,b) = 1
- 2 = $(a^2)/(b^2)$
  - ∴ $2b^2 = a^2$
  - ∴ even(a^2)
- we have already proved
  - even(n^2) → even(n)

∴ *even(a)*

∴ a = 2c

∴ $2b^2 = a^2 = 4c^2$

∴ $b^2 = 2c^2$

∴ *even(b)*

- *but gcd(a,b) = 1*
  - ∴ a and b cannot both be even
- Our assumption must be false, and root √2 is irrational
- QED

Proof by Cases

To prove this

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

Know that

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \Leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

- To prove P → Q
  - find a set of propositions P1, P2, …, Pn
  - (P1 or P2 or … or Pn) → Q
  - prove

    P1 -> Q and
    P2 -> Q and
    …   and
    Pn -> Q

We look exhaustively for all cases and prove each one

Proof by Cases

Factoid: the 4-colour theorem had > 1000 cases

Proof by Cases

For every non-zero integer x, x^2 is greater than zero

- There are 2 cases to consider,
  - x > 0
  - x < 0
- x > 0 then clearly x^2 is greater than zero
- x < 0
  - the product of two negative integers is positive
  - consequently x^2 is again greater than zero
- QED

Proof by Cases

The square of an integer, not divisible by 5 , leaves a remainder of 1 or 4 when divided by 5

- There are 4 cases to consider
  - n = 5k + 1
    - ∴ $n^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1$
  - n = 5k + 2
    - ∴ $n^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4$
  - n = 5k + 3
    - ∴ $n^2 = 25k^2 + 30k + 9 = 5(5k^2 + 6k + 1) + 4$
  - n = 5k + 4
    - ∴ $n^2 = 25k^2 + 40k + 16 = 5(5k^2 + 8k + 3) + 1$

∴ the remainders are 1 or 4

- QED

Vacuous Proof

When P is false P implies Q is true
If we can prove P is false we are done!

$$P(n): n > 4 \rightarrow n^3 < 3^n$$

- prove P(3)
  - if 3 > 4 then …
  - if false then …
- Since the hypothesis in this implication is false
  - the implication is vacuously true
- QED

Existence Proof

- Prove, or disprove something, by presenting an instance.
- 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

Disprove the assertion *"All odd numbers are prime"*

Number nine

Existence Proof

Is n^2 - n + 41 prime when n is positive?

- let n = 41
- n^2 - n + 41 = 41.41 - 41 + 41
  = 41.41
  which is composite
- therefore n^2 - n + 41 is not always prime
- QED

Existence Proof

Show that there are n consecutive composite integers for any +ve n

What does that mean?

- for example, let n = 5
- consider the following sequence of 5 numbers
  - 722 divisible by 2
  - 723 divisible by 3
  - 724 divisible by 4
  - 725 divisible by 5
  - 726 divisible by 6
- the above consecutive numbers are all composite

Existence Proof

Show that there are n consecutive composite integers for any +ve n

let x = (n + 1)! + 1
x = 1.2.3.4 … n.(n+1) + 1

- x + 1 = 2 + (n + 1)! = 2(1 + (n + 1)!/2)
- x + 2 = 3 + (n + 1)! = 3(1 + (n + 1)!/3)
- x + 3 = 4 + (n + 1)! = 4(1 + (n + 1)!/4)
- …
- x + i = (i + 1) + (n + 1)! = (i + 1)(1 + (n + 1)!/(i + 1))

We have constructed n consecutive composite integers
QED

Existence Proof

Are there an infinite number of primes?

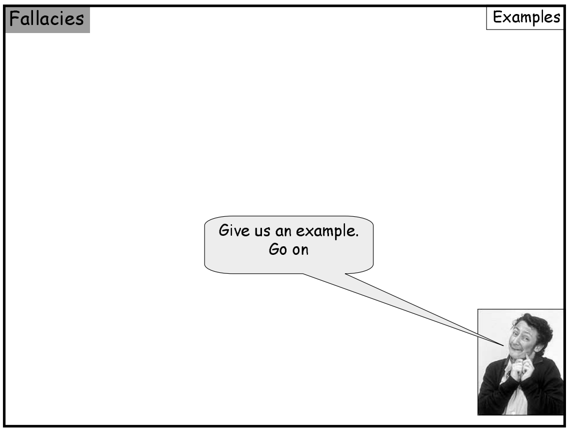
- Reformulate this as
  - "For any n, is there a prime greater than n?"
- compute a new number x = n! + 1
  - x = 1.2.3.4.5.6…n-1.n + 1
- x is not divisible by any number in the range 2 to n
  - we always get remainder 1
- the FTA states x is a product of primes
  - x has a prime divisor
  - x's smallest prime divisor is greater than n
- Consequently for any n there is a prime greater than n

Fallacies

Bad proofs: Rosen 1.5 page 69

$[(p \to q) \wedge q] \to p$ Fallacy of affirming the conclusion

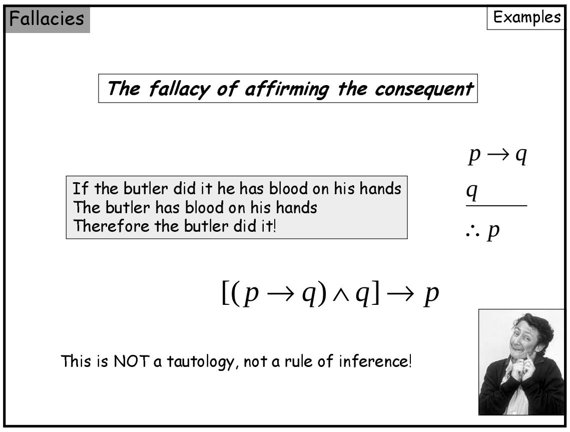
$[(p \to q) \wedge \neg p] \to \neg q$ Fallacy of denying the hypothesis



Fallacies

Examples

Give us an example.
Go on



Fallacies

Examples

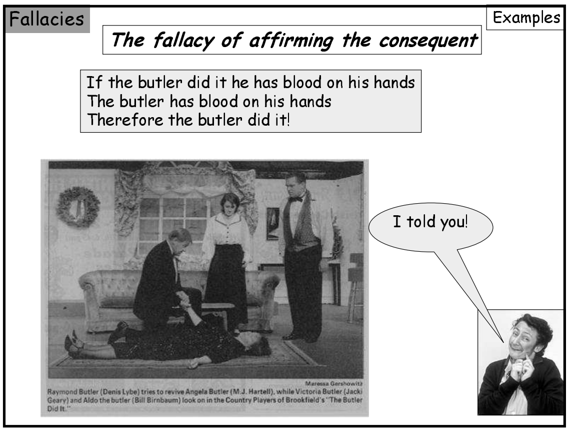
The fallacy of affirming the consequent

If the butler did it he has blood on his hands
The butler has blood on his hands
Therefore the butler did it!

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

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

This is NOT a tautology, not a rule of inference!



Fallacies

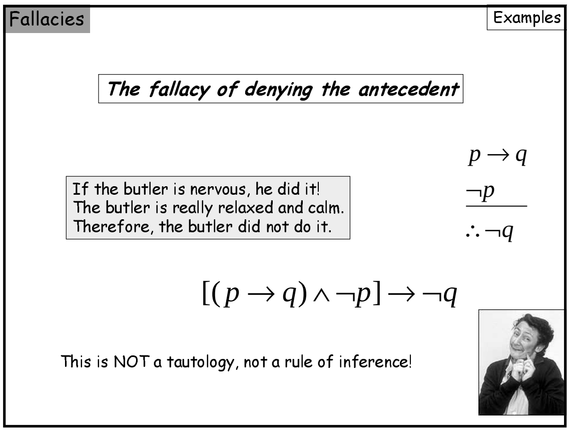
Examples

The fallacy of affirming the consequent

If the butler did it he has blood on his hands
The butler has blood on his hands
Therefore the butler did it!

Maressa Gershowitz

Raymond Butler (Denis Lybe) tries to revive Angela Butler (M.J. Hartell), while Victoria Butler (Jacki Geary) and Aldo the butler (Bill Birnbaum) look on in the Country Players of Brookfield's "The Butler Did It."



Fallacies

Examples

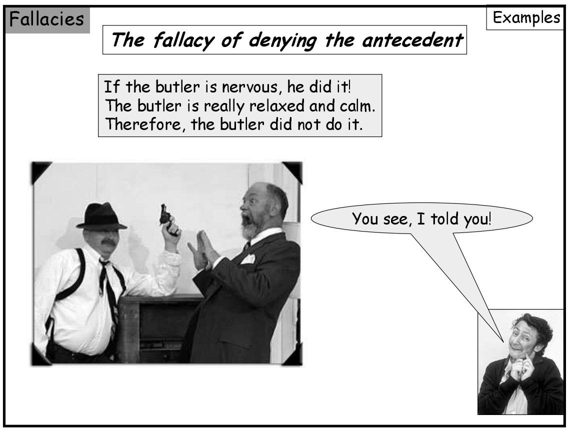
The fallacy of denying the antecedent

If the butler is nervous, he did it!
The butler is really relaxed and calm.
Therefore, the butler did not do it.

$$\begin{array}{l} p \to q \\ \underline{\neg p \quad\quad} \\ \therefore \neg q \end{array}$$

$$[(p \to q) \land \neg p] \to \neg q$$

This is NOT a tautology, not a rule of inference!



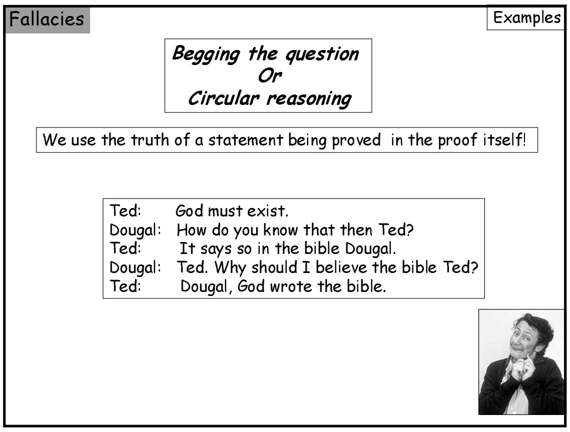
Fallacies

Examples

The fallacy of denying the antecedent

If the butler is nervous, he did it!
The butler is really relaxed and calm.
Therefore, the butler did not do it.

You see, I told you!



Fallacies

Examples

Begging the question
Or
Circular reasoning

We use the truth of a statement being proved in the proof itself!

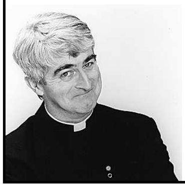
Ted: God must exist.
Dougal: How do you know that then Ted?
Ted: It says so in the bible Dougal.
Dougal: Ted. Why should I believe the bible Ted?
Ted: Dougal, God wrote the bible.

Fallacies

Examples

Begging the question
Or
Circular reasoning

Ted: God must exist.
Dougal: How do you know that then Ted?
Ted: It says so in the bible Dougal.
Dougal: Ted. Why should I believe the bible Ted?
Ted: Dougal, God wrote the bible.



Proofs. Who cares?

How would you prove that Iraq has no weapons of mass destruction?

Something like a proof by cases?
How many cases?
Any other technique?

How would you prove that IRAQ does have weapons of mass destruction?

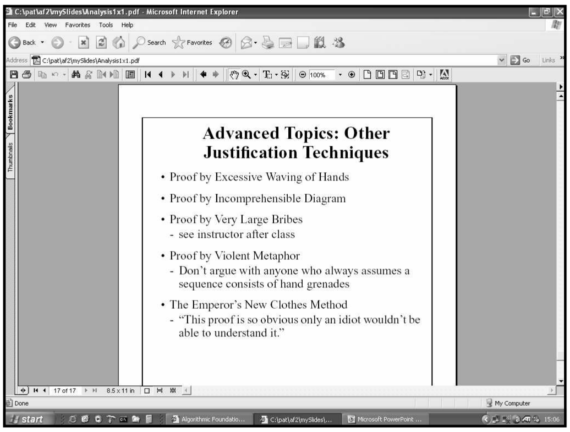
An existence proof?
Or something else?

Is it fair to assume someone is innocent until proved guilty?

Are there some things that cannot be proved?

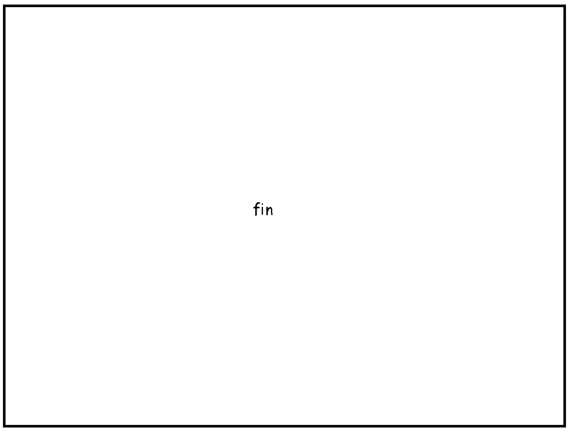
Proof techniques

- rules of inference
- fallacies
- direct proof
- indirect proof
- if and only if
- trivial proof
- proof by contradiction
- proof by cases
- vacuous proof
- existence proof



Advanced Topics: Other Justification Techniques

- Proof by Excessive Waving of Hands
- Proof by Incomprehensible Diagram
- Proof by Very Large Bribes
  - see instructor after class
- Proof by Violent Metaphor
  - Don't argue with anyone who always assumes a sequence consists of hand grenades
- The Emperor's New Clothes Method
  - "This proof is so obvious only an idiot wouldn't be able to understand it."



fin