Proof Techniques
Lecture 4

COSC 242 – Algorithms and Data Structures

Today’s outline

1. What is a proof?
2. Direct Proof
3. Proof by Contradiction
4. Proof by Induction

Today’s outline

1. What is a proof?
2. Direct Proof
3. Proof by Contradiction
4. Proof by Induction

In truth, why do we need proofs?

As we saw in Lecture 3, plots of n are insufficient. We needed a mathematical notation to describe upper bounds on runtime, $\mathrm{O}(\mathrm{n})$.

This notation is concise and helpful. But that doesn't mean all equations using asymptotic notation are *true*.

To know that a runtime adheres a given equation, we have to *prove* that it's true. To do that, we need to use a mathematical proof.

What is a proof?

A **proof** is a convincing argument expressed in the language of mathematics that a statement is **true**[1].

In math, a **statement** is sentence that is either true or false.

Statement examples

Two parallel lines in a plane have the same slope (True)

1 = 0 (False)

True or False?

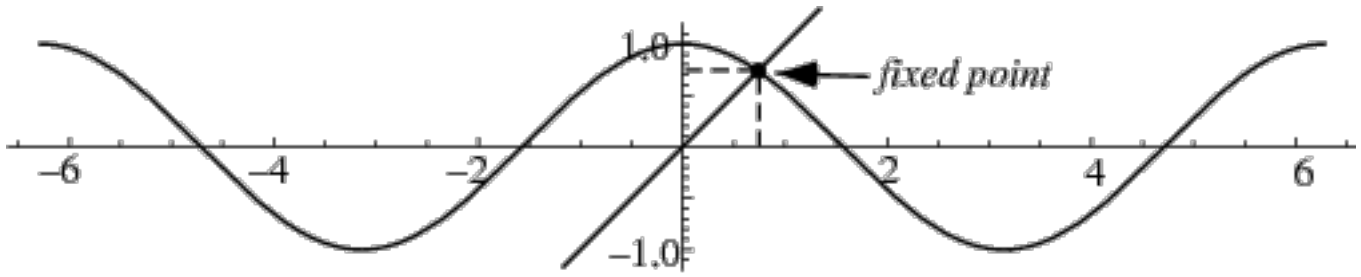
But what about this statement:

There is an angle t such that $\cos(t) = t$

True!

This statement is true. This time we can prove visually:

There is an angle t such that $\cos(t) = t$



[2]

The value is called the Dottie number, which you can read about here
[2] - https://mathworld.wolfram.com/DottieNumber.html

Conditional statements

Given two statements, each of which may be either True or False, a common problem is to show that the following **conditional statement**, also called an **implication**, is true[1]:

If A is true, then B is true.

This can be shortened to "If A, then B", or "A **implies** B".

Implication

This implication contains three separate statements[1]:

1. Statement A, which we call the **hypothesis**
2. Statement B, which we call the **conclusion**
3. Statement "A implies B"

Note, some texts may write this as $P \implies Q$

Truth table

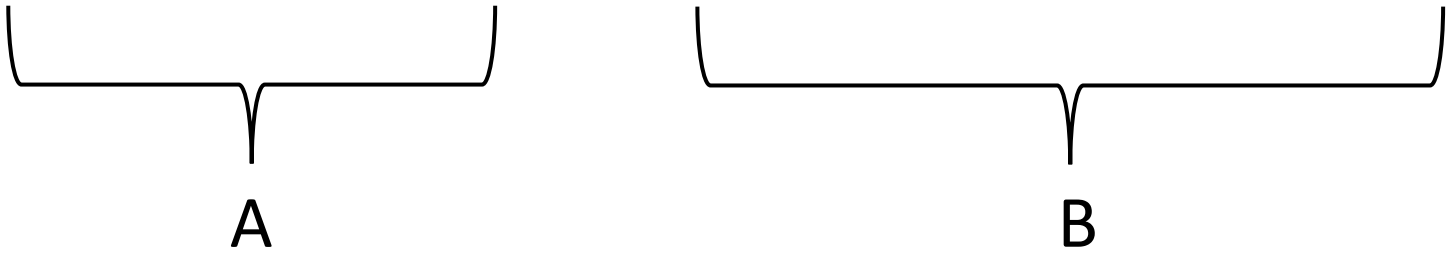
Given that both the hypothesis (A) and the conclusion (B), could each be either True or False, we have four cases to consider[1]:

1. A is True and B is True
2. A is True and B is False
3. A is False and B is True
4. A is False and B is False

$\mathbf{A}$	$\mathbf{B}$	$\mathbf{A \Rightarrow B}$
True	True	True
True	False	False
False	True	True
False	False	True

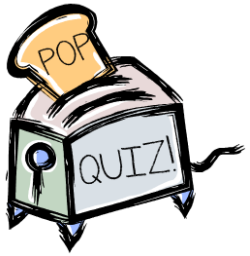
Example of truth

“If you study hard, then you will get a good grade”



A	**B**	**A ⇒ B**
Studied hard	Got good grade	True
Studied hard	Did not get good grade	False
Did not study	Got a good grade	True
Did not study	Did not get a good grade	True

Pop quiz 1



Is the following statement true of false?

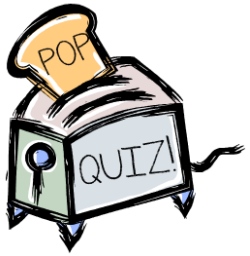
if 1 < 2, then 4 < 3

Answers

True

False

Pop quiz 2



Is the following statement true of false?

if 2 < 1, then 3 < 4

Answers

True

False

Identifying the hypothesis & conclusion

The first step in doing a proof is identifying the **hypothesis A**, and the **conclusion B**.

Everything you are assuming to be True is the hypothesis.

Everything you are trying to prove is the conclusion.

Examples

The sum of the first n positive numbers is n(n+1)/2

Hypothesis: n is a positive integer

Conclusion: The sum of the first n positive integers is n(n+1)/2

The quadratic equation $ax^2 + bx + c = 0$ has two real roots provided that $b^2 - 4ac > 0$, where a ≠ 0, b, and c are given real numbers.

Hypothesis: a, b, and c are given real numbers with a ≠ 0 and $b^2 - 4ac > 0$

Conclusion: The quadratic equation $ax^2+bx+c = 0$ has two real roots.

Proof types

There are many types of mathematical proofs.

In COSC242 we're only going to consider three types:

Direct proof – A logical explanation

Proof by contradiction – Disprove a counterexample

Proof by induction – Prove the base, then prove n+1

Today’s outline

1. What is a proof?
2. Direct Proof
3. Proof by Contradiction
4. Proof by Induction

Direct proof

A direct proof is more of a “logical explanation”. It is sometimes called an argument by deduction.

It involves taking known facts, and using them to show other facts, without making further assumptions.

Typically, this involves algebra or known mathematical relationships, such as those used in simple geometry proofs.

Example

Prove:

$$(x + y)^2 = x^2 + 2xy + y^2$$

Proof:

Using the distributive property, that is, a(b+c) = ab+ac:

$$(x + y)^2$$
$$= (x + y)(x + y)$$
$$= x(x + y) + y(x + y)$$
$$= xx + xy + yx + yy$$
$$= x^2 + 2xy + y^2$$

Which proves the left hand side of the equality, equals the right hand side. ■

Direct proof

A direct proof is oftentimes the simplest proof method available.

When applicable, it’s the best method to use.

However, it’s use is somewhat limited. To prove equations involve asymptotic notation, we will need to learn some more powerful proving techniques.

Reading proofs

You may have noticed that funny little ■ symbol at the end of our proof.

This symbol, or some equivalent, is usually used to signal the end of the proof.

Sometimes the letters “Q.E.D.” are used, which is an acronym for the Latin words “*quod erat demonstrandum*”, which translates to “*what was to be shown*”. [link]

Today’s outline

1. What is a proof?
2. Direct Proof
3. Proof by Contradiction
4. Proof by Induction

Proof by contradiction

In proof by contradiction, our goal is to prove that the statement is True, by showing that it cannot be False.

To do this, we first *assume* that our hypothesis *A* is True, and that our conclusion *B* is False. We then show why this cannot happen.

This proof technique is valuable when the statement *NOT B* gives you useful information.

Proof by contradiction

Assume A is true

Assume ¬B is true

Use A and ¬B to demonstrate a contradiction

Proof by contradiction

This proof technique is valuable when the statement *NOT B* gives you useful information.

If statement B is one of two possible alternatives (binary), then the contradiction method can often be effective.

By assuming *NOT B*, that means the other cases must happen, which should helpful lead to a contradiction.

Example

Prove:

There is no largest integer.

Proof:

1. Assume the contrary, that there *is* a largest integer.
   Call it *B*.
2. Show this assumption leads to a contradiction.
   C = B + 1. Here C is an integer that is the sum of two integers.
   Also, C > B, which means B is not the largest integer.
   Thus, we have proved there is no largest integer.

Class challenge 1

Prove:

For all real numbers x and y, if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$

Hint steps:

1. Identify A and B. Then,
2. State ¬B. Then,
3. Using algebra, show that the contradiction cannot happen.

Proof by Contradiction with Big-Oh

Suppose you are asked: Is $\mathrm{n} = \boldsymbol{\Theta}(\mathrm{n}^2)$?

Recall:

$O\big(g(n)\big) =$ {f(n): there exists positive constants, c and n_0, such that: $0 \leq f(n) \leq c \cdot g(n)$ for all $n \geq n_0$}

And, in asymptotic notation, we use '=' to mean that our function is within the set of functions.

Proof by Contradiction with Big-Oh

Thus, taking $0 \leq f(n) \leq c \cdot g(n)$, it is easy to see that $n = O(n^2)$.

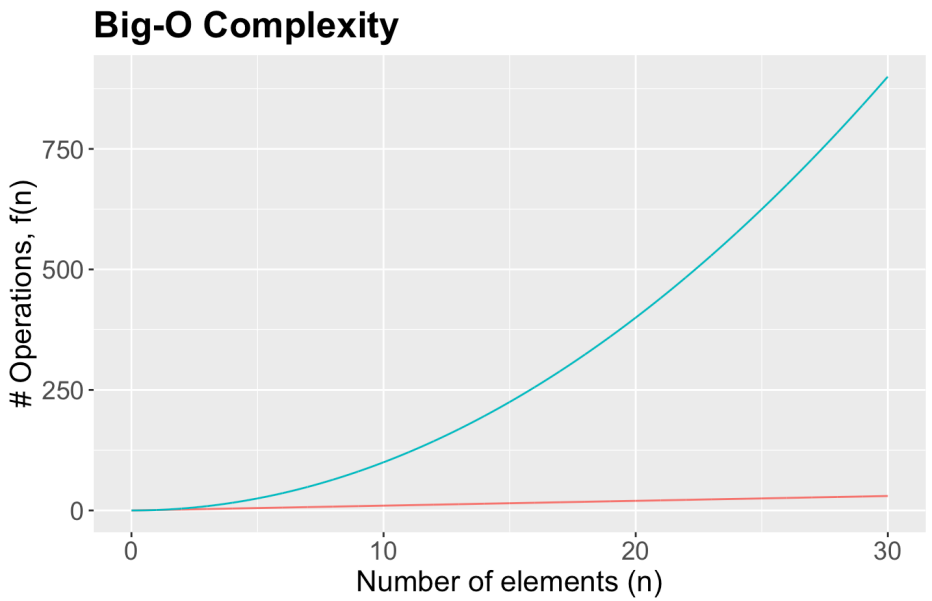
Just take $c = n_0 = 1$. That is, $1 \leq 1*1^2$

This is a simple case. But what about $n^2 = O(n)$?

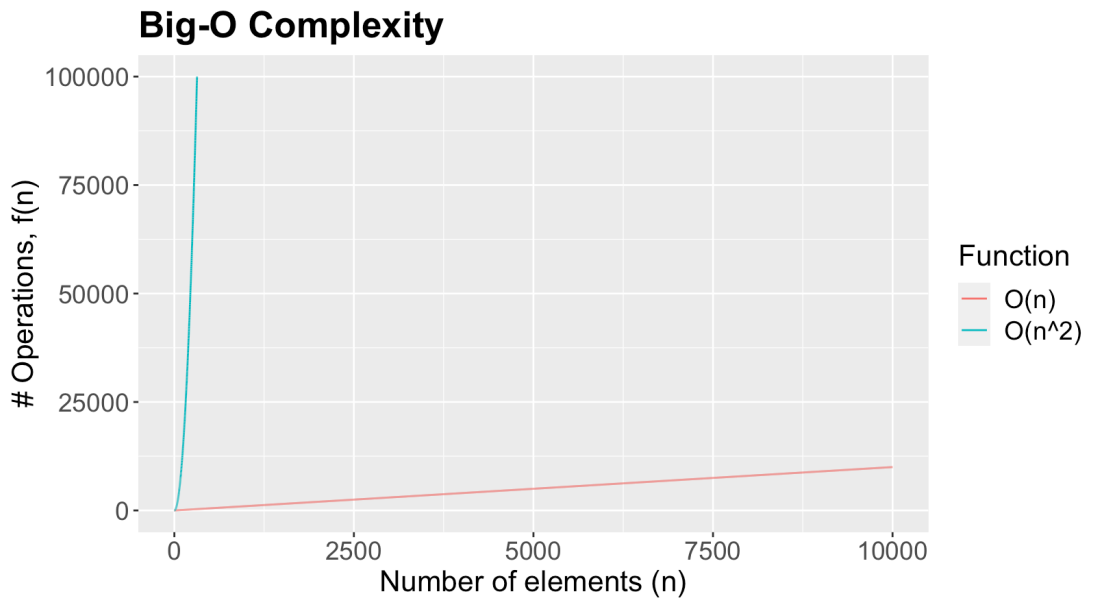
Proof by contradiction: $n^2 = O(n)$?

First, use your intuition: n^2 has a sharp upward curve, whereas n is a straight line with a gradient of 1.

So surely n^2 can't scale up as well as n?



Zooming out… →



Proof by contradiction: $n^2 = O(n)$?

But we showed in L03 that plots are not enough.

Therefore, to be convinced that $n^2 \neq O(n)$, or rather, $n^2 = O(n)$ cannot hold, we need to prove it.

To do this, we will use **proof by contradiction**.

This is a good case for contradiction as there are two possibilities: $n^2 = O(n)$ OR $n^2 \neq O(n)$.

The former is likely untenable. So we will take $n^2 \neq O(n)$…

Proof by contradiction: $\mathrm{n}^2 = \mathrm{O}(\mathrm{n})$?

Lets try and prove $\mathrm{n}^2 = \mathrm{O}(\mathrm{n})$ cannot hold through by contradiction.

Then c, n_0 would have to exist such that $\mathrm{n}^2 \leq \mathrm{c} \cdot \mathrm{n}$ for all $\mathrm{n} \geq \mathrm{n}_0$

1. **Statement A (hypothesis)**: c, n, n_0 are real numbers ($\mathrm{c}, \mathrm{n}, n_0 \in \mathbb{R}$), such that $n > 0$, $c > 0$, and $n \geq n_0$
2. **Statement B (conclusion)**: $\mathrm{n}^2 = \mathrm{O}(\mathrm{n})$

Lets find a case that proves ¬B = False.

Proof by contradiction: $\mathrm{n}^2 = \mathrm{O}(\mathrm{n})$?

Rewriting our equation into standard notation:

1. $n^2 \leq c \cdot n$
2. $\frac{n^2}{n} \leq c$
3. $n \leq c$

We stated that c is a fixed value, while n can vary freely. So lets set n = c+1

4. $c + 1 \leq c$ → False

Conclusion: Our contradiction ¬B, or $\mathrm{n}^2 = \mathrm{O}(\mathrm{n})$, is shown to be False. Therefore, $\mathrm{n}^2 \neq \mathrm{O}(\mathrm{n})$, must be True. ■

Summary

Proofs by contradiction are useful for proving that something is not the case. They always have the same structure:

1. Assume the opposite of what you want to prove.
2. Use the rules of logic or math to arrive at a statement that can't be true (an absurdity, or a paradox).
3. If you've applied the rules correctly, then the only thing that could be wrong must be the assumption at the start. Therefore the opposite of the assumption must be true.

Today’s outline

1. What is a proof?
2. Direct Proof
3. Proof by Contradiction
4. Proof by Induction

Can we always use contradiction?

Proof by contradiction is great at proving something is **not True**, and when our choice is a binary one.

But it's harder to prove when something is the case.

For example, consider the set $\mathrm{X} \in \mathbb{R}$, where

X = {3, 12, 33, 72, …}

Where X is given by $f(n) = n^3 + 2n$

Are all the elements of X divisible by 3?

Start with contradiction

Lets begin by rewriting our equation:

$n^3 + 2n = 3m$ for some integer m

1. **Statement A (hypothesis)**: n, m are real numbers ($\mathrm{n}, m \in \mathbb{R}$), such that $n > 0, m > 0$
2. **Statement B (conclusion)**: $n^3 + 2n = 3m$

Lets find a case that proves ¬B = False.

Start with contradiction

$n^3 + 2n \neq 3m$

$\frac{n^3+2n}{3} \neq m$, where m is a real, positive integer

Starting with n = 1

$\frac{1^3+2*1}{3} = 1$ … Nope, that's valid. Lets try n = 2

$\frac{2^3+2*2}{3} = 4$ … Nope, that's valid too. Lets try ….

Obviously this can go on forever, which tells us something

Proof by Induction

Proof by induction is a very powerful method that can be used to prove a wide variety of theorems.

The technique also provides a useful way for thinking about algorithm design - it encourages you to think about solving a problem by building up from simpler sub-problems.

It is closely related to recursion, and allows us to demonstrate an infinite number of facts in a finite amount of space.

When to use induction

You should consider using induction when B has the form:

For every integer $n \geq 1$, “something happens”.

Where the **“something happens” is P(n)**, that depends on the integer n.

Formally, it’s used to prove statements of the form:

$$(\forall n \in \mathbb{N})\big(P(n)\big)$$

Why could induction be helpful?

Recall

1. $\Theta\big(g(n)\big) =$ {f(n): there exists positive constants, c_1, c_2, and n_0, such that: $0 \leq c_1 \cdot g(n) \leq f(n) \leq c_n \cdot g(n)$ for all $n \geq n_0$}
2. $c, n, g(n), f(n) \in \mathbb{N}$.
3. Induction use: For every integer $n \geq 1$, “something happens”.

Asymptotic notation deals exclusively with integers between 0 and ∞, where “something happens”. Thus, induction may be a powerful technique in determining the runtime of algorithms.

An example with Proof by induction

Lets start by using induction to prove a classic example, the sum of a finite arithmetic series[1].

For all integers n ≥ 1, $\underbrace{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}}_{P(n)}$, where $\sum_{k=1}^{n} k = 1 + \cdots + n$

One way to prove this is by creating an infinite list of statements, one for each value of n, starting at n = 1, and then prove each one separately.

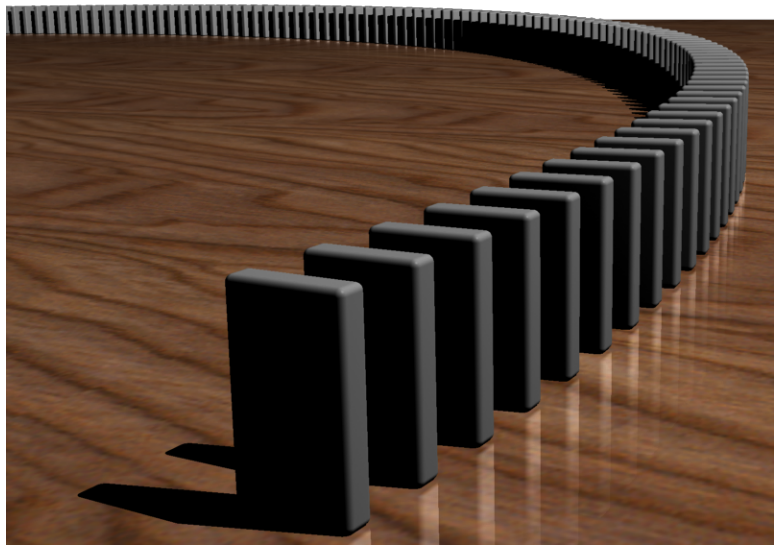
Proof by induction

This manual approach works fine for the first few n, but how do we solve for statement number ‘n’?

Something happens	Equation	Sum
$P(1)$	$\frac{1(1+1)}{2}$	1 = 1
$P(2)$	$\frac{2(2+1)}{2}$	1 + 2 = 3
$P(3)$	$\frac{3(3+1)}{2}$	1 + 2 + 3 = 6
	$\vdots$	
$P(n)$	$\frac{n(n+1)}{2}$	
$P(n+1)$	$\frac{(n+1)\big((n+1)+1\big)}{2}$	$\frac{(n+1)(n+2)}{2}$

How induction works

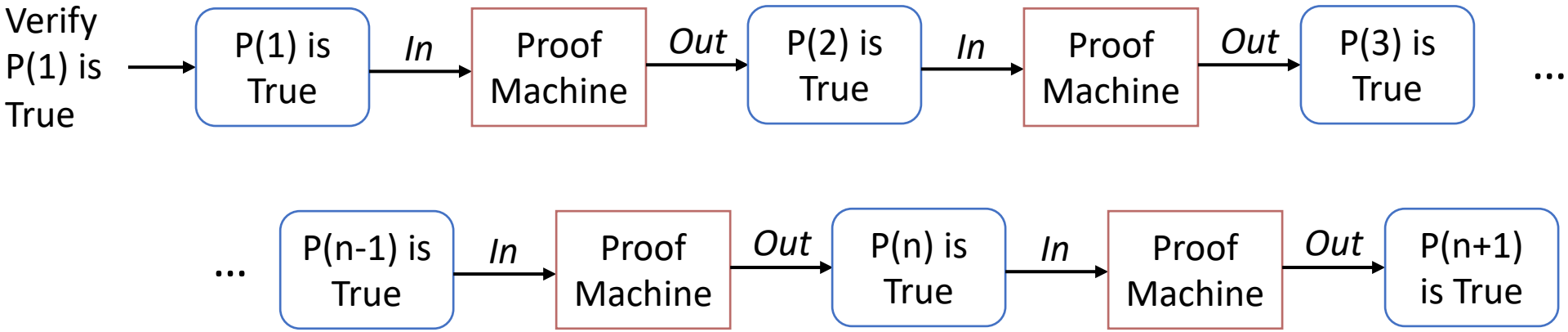
Domino effect: Induction is often informally compared to dominoes toppling over. When we push the first domino, all consecutive ones will fall; as one falls and hits the next, it too falls, and so on to infinity.



Induction “machine”

Solow compares induction to a little machine [1].

The machine works by verifying $P(1)$ is True, which is easy to do. The machine uses the fact that $P(1)$ is True, and automatically proves that $P(2)$ is True, and so on.



Induction “machine”

As we can see, when the machine gets to prove $P(n+1)$ is True, it has already shown that $P(n)$ is True.

With induction, we assume that $P(n)$ is True. This assumption is called the **Induction Hypothesis**.

Our job is then to prove that $P(n+1)$ is also True.

Steps of Induction

1. Base case: Verify that $P(1)$ is True.
2. Induction step: Use the assumption that $P(n)$ is True, to prove that $P(n+1)$ is True.

The hypothesis in Step 2, that our statement holds for a particular n, is called the **induction hypothesis**.

To prove the inductive step, we assume the induction hypothesis for n, and then use this assumption to prove that the statement holds for $\mathrm{n}+1$.

Helpful resources on proofs

The textbook does not cover mathematical proofs. Instead, you may find the following resources helpful:

Free resources

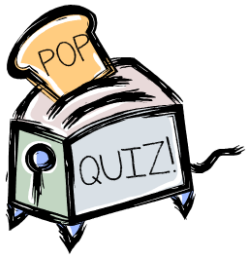
- Data Structures & Algorithm Analysis, C. A. Shaffer, 2013, Dover. [link]
- Mathematical Reasoning: Writing and Proof, T. Sundstrom, 2020, Grand Valley State University. [link]
- Proofs and Mathematical Reasoning, A. Stefanowicz, 2014, University of Birmingham. [link]
- American Institute of Mathematics. [link]

Paid resources

- How to read and do proofs, D. Solow, 2013, Wiley.

Solutions

Pop quiz 1



Is the following statement true of false?

if 1 < 2, then 4 < 3

A = True B = False $A \Rightarrow B = \text{False}$

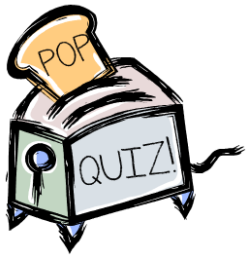
A	B	A ⇒ B
True	True	True
True	False	False
False	True	True
False	False	True

Answers

True

False ✓

Pop quiz 2



Is the following statement true of false?

if 2 < 1, then 3 < 4

A = False B = True $A \Rightarrow B = \text{True}$

Answers

True ✓

False

A	B	A ⇒ B
True	True	True
True	False	False
False	True	True
False	False	True

Class challenge 1

1. A is x and y are real numbers ($x, y \in \mathbb{R}$), such that $x \neq y$, $x > 0$, and $y > 0$.
2. B is '> 2'. So ¬B is '≤ 2'

$$xy\left(\frac{x}{y}+\frac{y}{x}\right) \leq 2xy$$
$$x^2 + y^2 \leq 2xy$$
$$x^2 - 2xy + y^2 \leq 0$$
$$(x-y)(x-y) \leq 0$$
$$(x-y)^2 \leq 0$$

Since both $x > 0$ and $y > 0$, and $x \neq y$, and that the square of any number must be positive, there are no numbers x & y that satisfy the contradiction. Therefore, the statement must be true. ■

References and attributions

1. How to read and do proofs, Solow, 2013, Wiley.
2. https://mathworld.wolfram.com/DottieNumber.html
3. https://www.khanacademy.org/math/algebra-home/alg-series-and-induction/alg-induction/v/proof-by-induction

Attributions