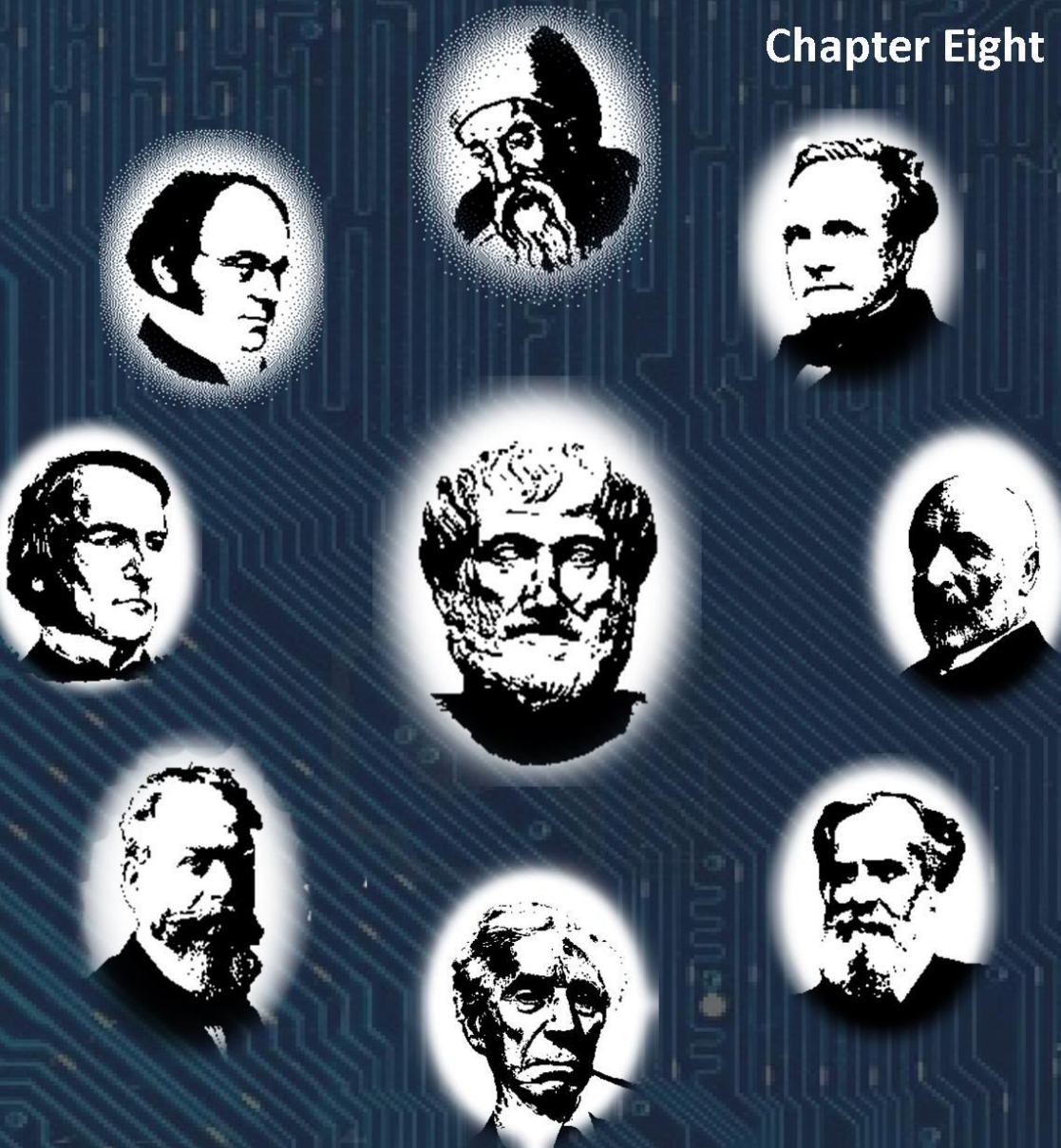


Chapter Eight



REASONING

elaine rich

alan kaylor cline

The Logicians on our cover are:

Euclid (? - ?)

Augustus De Morgan (1806 – 1871)

Charles Babbage (1791 – 1871)

George Boole (1815 – 1864)

Aristotle (384 BCE – 322 BCE)

George Cantor (1845 – 1918)

Gottlob Frege (1848 – 1925)

John Venn (1834 – 1923)

Bertand Russell (1872 – 1970)

REASONING

AN INTRODUCTION TO LOGIC, SETS, AND FUNCTIONS

CHAPTER 8 A RICHER CATALOGUE OF REASONING AND PROOF TECHNIQUES

Elaine Rich
Alan Kaylor Cline

The University of Texas at Austin

Image credits:

Baby emu: <http://www.telegraph.co.uk/earth/earthpicturegalleries/5948601/Animal-pictures-of-the-week-31-July-2009.html?image=17>

White peacock: © David Rich, 2014. www.RichImagesColorado.com

REEM-A: <http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=1212>

Coffee can and beans: © David Rich, 2014.

Man climbing stairs: © Lynda Trader, 2014.

Woman rock climber: © Lynda Trader, 2014.

Stack of paper plates on picnic table: © Lynda Trader, 2014.

Box of tissues: http://en.wikipedia.org/wiki/Facial_tissue

80th birthday: © Lynda Trader, 2014.

Colored M&Ms: © David Rich, 2014.

Archimedes in bathtub: © Lynda Trader, 2014.

Dante Alighieri: Portrait by Sandro Botticelli,
http://en.wikipedia.org/wiki/Dante_Alighieri#mediaviewer/File:Portrait_de_Dante.jpg

Four Color Problem: http://en.wikipedia.org/wiki/Four_color_theorem

19 foot tall man: © Lynda Trader, 2014.

Sunrise: <http://pics9.this-pic.com/key/sunrise%20clipart%20black%20and%20white>

Flock of birds: <http://pastorcraigsermonblog.blogspot.com/2010/10/for-several-years-i-lived-in-joseph.html>

Penguin: <http://www.downloadclipart.net/browse/7/emperor-penguin-clipart>

Ostrich: <http://animal-silhouette.com/47-food/064-food.html>

REASONING—AN INTRODUCTION TO LOGIC, SETS AND FUNCTIONS Copyright © 2014 by Elaine Rich and Alan Kaylor Cline. All rights reserved. Printed in the United States of America. No part of this book may be used or reproduced in any manner whatsoever without written permission except in the case of brief quotations embodied in critical articles or reviews. For information, address Elaine Rich, ear@cs.utexas.edu.

<http://www.cs.utexas.edu/learnlogic>

Library of Congress Cataloging-in-Publication Data

Rich, Elaine, 1950 -

Reasoning—An Introduction to Logic Sets and Functions / Elaine Rich.— 1st ed. p. cm.
ISBN x-xxx-xxxxx-x 1

Table of Contents

Real Proofs.....	1
Direct Proofs	6
Proof by Contradiction.....	16
Proof by Example or Counterexample.....	26
Proof by Construction.....	43
Divide and Conquer	48
Invariants.....	60
Mathematical Induction I.....	64
Mathematical Induction II.....	78
Mathematical Induction III	86
Stronger and Weaker Claims	107
Strategies for Discovering Proofs	113
Empirical Induction	116
Everyday Reasoning	122
Appendix.....	125

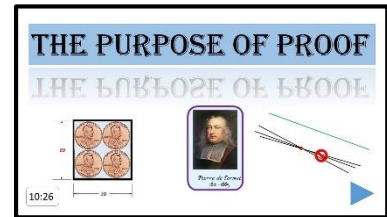
A Richer Catalogue of Reasoning and Proof Techniques

Real Proofs

What Are Proofs For?

Recall that the job of proof is to lead us to truth and insight. Let's watch this video again.

<https://www.youtube.com/watch?v=iiCqs6Vi3gw>



So far, in this course, we've focused on guaranteeing that our proofs:

- **Preserve truth.** We have laid out a set of inference rules that is both sound and complete. These rules allow us to derive all and only those statements that follow from our premises.

Of course, if we want to derive conclusions that are true, we must also:

- **Begin with truth.** This means that we must choose premises (axioms) that are true in the world we're working with. We have chosen to say very little about this because choosing premises is a very different sort of activity than proof construction is. It typically requires substantial domain expertise. And it may be controversial.

In fact, one of the beauties of the theory that we've been presenting is that we've been able to separate the noncontroversial, reasoning piece from the (very often) controversial premise-selection piece. So, while our goal continues to be the construction of sound arguments (i.e., ones that start with true premises and apply sound inference rules) that lead to conclusions that are true, we'll continue to focus on the argument construction part.

So far, nothing new. But, up until now, our proofs have been small and not very likely to tell us something we didn't already know. We need to change that.

We need to:

- Discuss strategies for finding nontrivial proofs in nontrivial problem domains.
- Describe a way to write such nontrivial proofs. We want to avoid getting so bogged down in the details that we miss the main reason(s) why our conclusion must be true.

In this chapter, we'll do both of those things.

What Do Real Proofs Look Like?

When we're reasoning about the world around us, our effective arguments never look like the proofs we've just been constructing.



<https://www.youtube.com/watch?v=29ZpYbY6eeU>

Imagine arguing that Mary must drive me to the store by saying, "Step 1. John or Mary must drive me to the store. Premise. Step 2. If John drives me to the store, he will be late for work. Premise." By the time we got to, "Step 6. Mary must drive me to the store. Disjunctive Syllogism from Steps 4 and 5," no one would be awake, much less following the reasoning.

When we're reasoning about less trivial problems, the need for a more concise language is even more clear.

Consider the following argument:

We need to improve the quality of our schools. Doing that costs money. The only way to get the money will be to raise taxes. But voters are generally unwilling to raise taxes unless they clearly understand what benefit they'll get if they do. So we need to launch a public awareness campaign.

Most people would agree that this argument is valid (i.e., the logic is correct). In most communities, though, there would likely be disagreement on whether it's sound (in other words, does it start with premises that are true). People may dispute the truth of one or more of the premises.

Notice that we can agree that the argument is valid, even though I've left out several steps, including some noncontroversial premises. For example, I haven't mentioned that the only way to raise taxes is for the voters to approve of doing so. Nor have I made it explicit that a public awareness campaign could change the minds of any voters.

The key is that, in a complex world, if I want to convince you of something, I have to make a short argument that is focused on those things that are both relevant and nonobvious. Rarely, in discussions of how to wash dishes, do we mention the effect that gravity would have on a glass if we let go of it.

The world of mathematicians and computer scientists is no different. Even the more formal proofs that are their bread and butter don't look like the ones we've just been writing:

- They don't have four columns; they're written in clear English.
- They don't generally use all the premises that are available (many of which may be irrelevant).
- They're often a lot shorter.

In this chapter, we'll make the transition to writing these kinds of proofs. As we do so, we must keep in mind that, if challenged, we must be able to fill in the details of any omitted steps. Thus, the request, "I don't see how you got from statement x to statement y . Please explain," is fair game. In fact, it is in response to this very question that we often realize that one person has assumed premises that the other person does not accept.

Me: So now we've shown that $xy = 2z$. Dividing both sides by y , we have that $x = 2z/y$.

You: Wait. How do you know that you can divide both sides by y ?

Me: Oops. I guess I'd have to know that $y \neq 0$. But I do know that. Let me add it as a premise.

Me: It's going to snow tomorrow. So everyone will be wearing boots.

You: How do you know about the boots?

Me: Well, I've assumed that everyone will check the weather and that they'll want to stay warm and that they have boots.

Big Idea

An English proof is a concise explanation of a valid argument. But, when you write an English proof, you must be prepared to defend every step if you're challenged to do so.

Problems

1. Evaluate each of the following arguments:

(Part 1) All students want to learn. The only way to learn is to spend time studying. So all students will want to spend time studying.

- a) The argument is sound (i.e., it's logically valid and its premises are true.)
- b) The argument is valid (i.e., the logic is correct) but its premises aren't all true.
- c) The premises are true but the argument isn't valid.
- d) It's total junk: at least one of the premises is false and the logic is wrong.

(Part 2)

- [1] $2 < 1$ Premise
- [2] $\text{successor}(1) = 2$ Premise
- [3] $\text{successor}(1) < 1$
- [4] $\exists x (\text{successor}(x) < x)$

- a) The argument is sound (i.e., it's logically valid and its premises are true.)
- b) The argument is valid (i.e., the logic is correct) but its premises aren't all true.
- c) The premises are true but the argument isn't valid.
- d) It's total junk: at least one of the premises is false and the logic is wrong.

(Part 3)

- [1] $(x > 0) \rightarrow (x+1 > 0)$ Premise
- [2] $\frac{1}{2} > 0$ Premise
- [3] $-\frac{1}{2} + 1 > 0$ Substituting into [2] since $\frac{1}{2} = -\frac{1}{2} + 1$
- [4] $-\frac{1}{2} > 0$ Letting [3] match the right hand side of [1] to derive the left hand side.

- a) The argument is sound (i.e., it's logically valid and its premises are true.)
- b) The argument is valid (i.e., the logic is correct) but its premises aren't all true.
- c) The premises are true but the argument isn't valid.
- d) It's total junk: at least one of the premises is false and the logic is wrong.

Problems

2. Define the following symbols:

J: John must drive me to the store.
M: Mary must drive me to the store.
K: Kelly must drive me to the store.
L: John will be late for work.
MDL: Mary must have a driver's license.
JDL: John must have a driver's license.
KDL: Kelly must have a driver's license.
SK: Kelly is my sister.
SM: Mary is my sister.

Now suppose that we have the following premises:

[1] $J \vee M \vee K$ John or Mary or Kelly must drive me to the store.
[2] $J \rightarrow L$ If John drives me to the store, he will be late for work.
[3] $\neg L$ John cannot be late for work.
[4] $M \rightarrow MDL$ If Mary must drive me to the store, she must have a driver's license.
[5] $K \rightarrow KDL$ If Kelly must drive me to the store, she must have a driver's license.
[6] *SM* Mary is my sister.
[7] *SK* Kelly is my sister.

Consider the following arguments:

- I. If John drives, he'll be late for work, but that can't happen. Since one of John, Mary, or Kelly has to drive, it will have to be Mary or Kelly. So one of my sisters must drive me to the store.
- II. If John drives, he'll be late for work, but that can't happen. So one of my sisters must drive me to the store. Since John isn't my sister, he can't drive me.
- III. If John drives, he'll be late for work, but that can't happen. So one of my sisters must have a driver's license.
- IV. If John drives, he'll be late for work, but that can't happen. Which is good because John doesn't have a driver's license.

Which (one or more) of them is/are valid (assuming that it's okay to leave out any number of steps that could be filled in if necessary)?

Direct Proofs

Introduction

In a direct proof, we walk forward from the premises to the desired conclusion, typically relying heavily on modus ponens. We'll leave out some steps along the way if we believe that a reader of our proof can easily fill them in. In particular, we almost always leave out explicit mention of existential/universal instantiation/generalization.

Problems

1. Consider the following proof of the existence of a white mammal (yes, you saw it as the *White Mammal* example):

[1]	$\forall x (Bear(x) \rightarrow Mammal(x))$	Premise	
[2]	$\exists x (Bear(x) \wedge White(x))$	Premise	
[3]	$Bear(c^*) \wedge White(c^*)$	Existential Instantiation	[2]
[4]	$Bear(c^*)$	Simplification	[3]
[5]	$White(c^*)$	Simplification	[3]
[6]	$Bear(c^*) \rightarrow Mammal(c^*)$	Universal Instantiation	[1]
[7]	$Mammal(c^*)$	Modus Ponens	[4], [6]
[8]	$Mammal(c^*) \wedge White(c^*)$	Conjunction	[5], [7]
[9]	$\exists x (Mammal(x) \wedge White(x))$	Existential Generalization	[8]

Which (one or more) of the following possible English proofs of the same claim (assuming the same premises) is/are valid?

- I. We know that there's a white bear. Since all bears are mammals, our white bear is thus a white mammal.
- II. Since all bears are mammals, the white bear we know exists must also be a white mammal.
- III. There must be a white mammal because there is a white bear, which is also a mammal.

2. Consider the following proof (from one of our videos) of the existence of someone who can participate in our drug test: Assign the following names to basic statements:

$W(x)$:	True if x is a W oman.
$U(x, y)$	True if person x U ses medication y .
$P(x)$	True if x may P articipate in our drug test.

[1]	$\exists p (\exists q (W(p) \wedge U(p, q)))$	Premise	
[2]	$\exists q (W(a^*) \wedge U(a^*, q))$	Existential Instantiation	[1]
[3]	$W(a^*) \wedge U(a^*, b^*)$	Existential Instantiation	[2]
[4]	$\forall x (\forall y ((W(x) \wedge U(x, y)) \rightarrow P(x)))$	Premise	
[5]	$(\forall y ((W(a^*) \wedge U(a^*, y)) \rightarrow P(a^*)))$	Universal Instantiation	[4]
[6]	$(W(a^*) \wedge U(a^*, b^*)) \rightarrow P(a^*)$	Universal Instantiation	[5]
[7]	$P(a^*)$	Modus Ponens	[3], [6]
[8]	$\exists z (P(z))$	Existential Generalization	[7]

Which (one or more) of the following possible English proofs of the same claim (assuming the same premises) is/are valid?

- I. If there's a woman who uses a medication, then she can be in our drug test. There is such a woman, so we've got someone who may participate in our test.
- II. There's a woman who uses a medication and anyone who does can be in our test. So we have that person as a participant.
- III. There must be someone who can participate in our drug test since there is a woman who takes a medication.

Simple Direct Proofs in Mathematics

The key to the correctness of our mathematical proofs will be that, as we move from one statement to the next, we will rely on theorems that we (or someone else) have already proven to be correct. In all of the examples that we'll do here, we'll assume that we can use as theorems all of high school mathematics. For example, if we have that $x = y$, we can multiply both sides by the same quantity and they will still be equal.

When we write direct proofs in mathematics, we may write some English sentences. We may also write sequences of formulas when our theorems tell us that each formula must follow from one or more of its predecessors.

Let the universe be the integers. We will take as premises what we know from high school algebra. Prove:

$$\forall x (x^2 + 1 > 0)$$

Proof:

Since the square of any integer is nonnegative, we have:

$$x^2 \geq 0$$

We also have:

$$1 > 0$$

Adding these, we have:

$$x^2 + 1 > 0$$

Thus:

$$\forall x (x^2 + 1 > 0)$$

Notice that, while we didn't explicitly mention universal instantiation or generalization, we used them. We instantiated x , treated it as an "arbitrary value", and reasoned with it. Then (implicitly) generalized back to a statement about all x 's.

Problems

1. Let the universe be the integers. We want to prove:

$$\forall x ((x > 1) \rightarrow (x^2 > x))$$

Try to write a proof of this claim. Then answer the question.

Which of the following statements is true:

- a) It's not possible to prove the claim.
- b) It's possible to prove an even stronger claim, namely: $\forall x (x^2 > x)$. It's not necessary to restrict the claim to positive integers.
- c) It's possible to prove this claim but not the stronger one without the restriction ($x > 1$)

2. Let the universe be the non-zero integers. Consider the following "proof" that $1 = 0$. We'll number the lines just so we can refer to them (even though in simple English proofs we generally don't bother).

- [1] $x = x$.
- [2] Squaring both sides we get $x^2 = xx$.
- [3] Subtracting x^2 from both sides, we get $x^2 - x^2 = xx - x^2$.
- [4] Factoring both sides, we get $(x - x)(x + x) = x(x - x)$.
- [5] Dividing both sides by $x - x$, we get $x + x = x$.
- [6] Simplifying, we get $2x = x$.
- [7] Dividing by x , we get $2 = 1$.
- [8] Subtracting 1 from both sides, we get $1 = 0$.

At which step did our proof first become invalid?

Starting with Definitions

It is very common, in doing proofs in mathematics, to appeal to formal definitions of the objects that we're working with. This tends to cut down a lot on handwaving.

Prove:

[1] For all integers a, b , and c , if a is divisible by b and b is divisible by c , then a is divisible by c .

We can rewrite this in our logical notation if we want to. Sometimes it makes the claim clearer. So we can write:

[1'] $\forall a, b, c ((\text{Div}(a, b) \wedge \text{Div}(b, c)) \rightarrow \text{Div}(a, c))$

Recall that a is divisible by b if and only if $b \neq 0$ and:

there exists some integer n such that $a = b * n$.

(For example, 15 is divisible by 5 because $15 = 5 * 3$.) So we have that $(\text{Div}(a, b) \wedge \text{Div}(b, c))$ is equivalent to saying that b and c are nonzero and there exist integers n and m such that:

[2] $a = b * n$

[3] $b = c * m$

Substituting $c * m$ for b in [2], we get:

[4] $a = c * m * n$

Give the name k to $m * n$. Then we have:

[5] $a = c * k$

So we have that a is divisible by c (by using the same definition that we used to get started).

Problems

1. Prove that if a is an even integer and b is an odd integer, then $a+b$ is odd. (Hint: start with the definitions that we've already given for $Even(x)$ and $Div(x, y)$). Write a definition for $Odd(x)$. Then write your proof.)
2. Prove that for all odd integers a and b , ab is also odd. (Hint: Start with the definition of odd integer.)
3. Prove that the sum of any two rational numbers is also rational. Hint: Recall the definition of a rational number:

$$\forall x (Rational(x) \equiv (\exists y, z (Integer(y) \wedge Integer(z) \wedge (z \neq 0) \wedge (x = \frac{y}{z}))))$$

In other words, x is rational if and only if it is the quotient of two integers and the denominator is not 0.

Don't Do Proofs Backwards

A common error, in attempting to construct a direct proof, is to start from the conclusion and work backwards, rather than to start from the premises and work forwards. While it often helps to *search* for a proof by working backwards from the conclusion, a valid proof must *proceed* from premises to conclusion, not the other way.

We can see how going backwards can fail to produce a legitimate proof with a very simple example from Boolean logic. Give names to the following statements:

C: Cody wins the prize.
 J: Jody wins the prize.
 P: There will be a party.

Assume the following premises:

[1]	$\neg C \rightarrow \neg P$	If Cody doesn't win the prize, there will be no party.
[2]	$\neg P$	There will be no party.

We'd like to prove:

[3]	$\neg(C \vee J)$	Neither Cody nor Jody wins the prize.
-----	------------------	---------------------------------------

Suppose that we try to prove [3] by starting with it and reasoning backwards to the premises:

[3]	$\neg(C \vee J)$	Goal	
[4]	$\neg C \wedge \neg J$	De Morgan	[3]
[5]	$\neg C$	Simplification	[4]
[2]	$\neg P$	Modus Ponens	[1], [5]

So we've derived something that we know must be true since it's one of the premises.

But this isn't a proof. If our conclusion is true, so are our premises. But there's no new information there. The premises are true, regardless of the truth status of the conclusion.

But maybe, since we've found a chain of reasoning that connects the conclusion to the premises (albeit backwards), we can transform what we've written into a valid proof. Let's start from the premises and go the other way. What happens?

[2]	$\neg P$	Premise
-----	----------	---------

We're stuck right away. We can't apply Modus Ponens backwards to derive $\neg C$. And by the way, if we had made it past this step, the reasoning that derived [5] also cannot be reversed. If we know $P \wedge Q$, we can use Simplification to derive P . But, based just on P , we cannot prove anything about Q , and in particular we cannot prove $P \wedge Q$. So this "proof" used two irreversible rules.

We shouldn't be surprised that we can't reverse this proof. From our premises, it isn't possible to conclude anything about either Cody or Jody winning the prize, much less some stronger claim about both of them.

The problem we just saw is that, while logical identities can be used in either direction, there are inference rules that are one way streets. If we try to use them backwards they will take us right into proof Never Never Land.

If, on the other hand, we have used only reversible rules, then it's possible to convert an invalid, backwards "proof" into a valid actual proof simply by reversing it. Remember, though, that if you're tempted to try to find a proof by working backwards and you're lucky enough to find a reversible one, you must actually do the reversal before claiming that you have a proof.

Prove that, for every positive real number x , $x + \frac{4}{x} \geq 4$.

Proposed "proof":

- [1] Let x be a positive real number and suppose that $x + \frac{4}{x} \geq 4$.
- [2] Multiplying by x , we get $x^2 + 4 \geq 4x$.
- [3] Subtracting $4x$ from both sides, we get $x^2 - 4x + 4 \geq 0$.
- [4] Factoring that, we get $(x - 2)^2 \geq 0$.

Now we observe that [4] must be true, since the square of any real number is nonnegative.

The problem here is that what we have is a proof of the following: If it's true that, for every positive real number x , $x + \frac{4}{x} \geq 4$, then some other thing [4] is also true. But that other thing is always true, independent of the truth of the claim we're interested in. So our proof hasn't actually yielded anything new. Most importantly, what we don't have is a proof of our claim. We assumed it was true; we didn't prove it true.

But we have discovered a chain of reasoning between something that is already known to be true [4] and the claim that we want to prove [1]. And, in this case, every step that we performed is, in fact, reversible. So here's a valid proof of our claim:

- [1] Since the square of every real number is nonnegative, we have, in particular:
 $(x - 2)^2 \geq 0$.
- [2] Expanding that, we have $x^2 - 4x + 4 \geq 0$.
- [3] Adding $4x$ to both sides, we have $x^2 + 4 \geq 4x$.
- [3] Assume that x is positive. Then we can divide by it, which yields $x + \frac{4}{x} \geq 4$.
- [4] Thus, for every positive real number x , $x + \frac{4}{x} \geq 4$.

Notice that the assumption that we need in order to carry out step [3] becomes a condition (a guard) on the claim that we can ultimately make.

Problems

1. Assume the following premises:

- [1] P
- [2] $P \rightarrow R$
- [3] $R \rightarrow \neg Q$

We want to prove: $\neg(P \rightarrow Q)$

Consider the following proposed proof:

[4]	$\neg(P \rightarrow Q)$		
[5]	$\neg(\neg P \vee Q)$	Conditional Disjunction	[4]
[6]	$P \wedge \neg Q$	De Morgan	[5]
[1]	P	Simplification	[6]

Which of the following statements is true:

- a) This proof is correct.
- b) This proof isn't correct. But the claim is true and it's possible to write a correct proof by reversing the order of the steps of this one.
- c) This proof isn't correct. But the claim is true and it's possible to write a correct proof by reversing the order of some of the steps of this one and then adding additional steps
- d) This proof isn't correct although the claim is true. But nothing in this proof will help us find a correct proof since no steps are reversible.
- e) This proof isn't correct and the claim isn't true.

2. Consider the claim that, for any nonnegative reals a and b :

$$[1] \quad \frac{a+b}{2} \geq \sqrt{ab}$$

Consider the following proposed proof of [1]:

$$[1] \quad \frac{a+b}{2} \geq \sqrt{ab} \quad \text{Squaring both sides, we get:}$$

$$[2] \quad \left(\frac{a+b}{2}\right)^2 \geq ab$$

$$[3] \quad \frac{(a+b)^2}{4} \geq ab$$

$$[4] \quad (a+b)^2 \geq 4ab$$

$$[5] \quad a^2 + 2ab + b^2 \geq 4ab$$

$$[6] \quad a^2 - 2ab + b^2 \geq 0$$

$$[7] \quad (a-b)^2 \geq 0$$

[7] must be true since the square of any real number is nonnegative. Q. E. D.

Which of the following statements is true:

- a) This proof is correct.
- b) This proof isn't correct. But the claim is true and it's possible to write a correct proof by reversing the order of the steps of this one.
- c) This proof isn't correct although the claim is true. But it isn't possible to write a correct proof just by reversing the order of the steps of this one. There is exactly one irreversible step.
- d) This proof isn't correct although the claim is true. But it isn't possible to write a correct proof just by reversing the order of the steps of this one. There are at least two irreversible steps.
- e) This proof isn't correct and the claim isn't true.

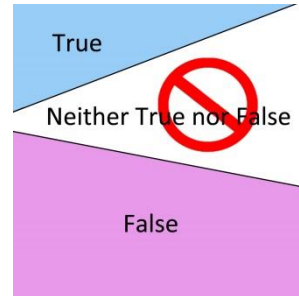
Proof by Contradiction

How Does a Proof by Contradiction Work?

Recall the Law of the Excluded Middle:

$$p \vee \neg p.$$

In other words, for any statement p , either it's true or false. Either it or its negation must be true. There's nothing "in the middle".



So suppose that I want to prove p . I'll start by assuming $\neg p$. Suppose that, from that, I can derive *False* (or any contradiction, since every contradiction evaluates to *False*). But I know that one of p or $\neg p$ must be true. And I've just shown that it's not $\neg p$. Thus it must be p . I'm done.

Suppose we want to prove that $\sqrt{2}$ is irrational. (Recall that a number is irrational if it cannot be expressed as the ratio of two integers.) The most straightforward way to prove this claim is to assume that it were rational. (In other words, that it could be expressed as the ratio of two integers, say as x/y). From that, we can derive a contradiction. Since (by the Law of the Excluded Middle) $\sqrt{2}$ must either be rational or not rational and we've just shown that it can't be rational, it must be irrational. We'll present the details of this proof soon.

Proofs by contradiction are also sometimes called *indirect proofs*.

Reductio ad Absurdum

The Proof by Contradiction technique that we just described is a special case of a more general reasoning strategy called *reductio ad absurdum*. (Translate this literally as, “reduce to absurdity”.) We can use this more general strategy in everyday rhetoric as well as in mathematics.

The earth can't be flat; if it were, people would be falling off the edges.

But people aren't falling off the edges. The conclusion doesn't match our experience. It feels absurd.

We have to hire more inspectors. If we don't, contaminated food will make it to the supermarkets.

But we can't accept that. So we must do something to make the contaminated food conclusion false.

The square root of 2 is irrational. If it were rational, we'd have a mathematical contradiction.

We can't accept such a contradiction, since, from False, we could then derive anything and mathematics would no longer be a useful tool.

When we use *reductio ad absurdum* arguments in everyday reasoning, we depend on our listeners sharing our premises, at least enough so that they agree with us that some conclusion is clearly false or clearly unacceptable.

When we use this strategy (generally then called *proof by contradiction*) in mathematics, we assume that we have started with some agreed upon set of axioms. So we simply reason until we find a logical contradiction, i.e., some expression that evaluates to False.

In the next several problems, we'll present everyday arguments that we'll evaluate. Then we'll consider some examples from mathematics

Problems

1. Label each of the following arguments as one of:

- a) Convincing to most people.
- b) Not convincing since the ascribed conclusion (we'll lose our market share) isn't particularly bad or absurd.
- c) Not convincing because there's at least one assumption that isn't justified.

(Part 1) We have to lower our prices. If we don't, we'll lose our market share because our competitors already slashed their prices.

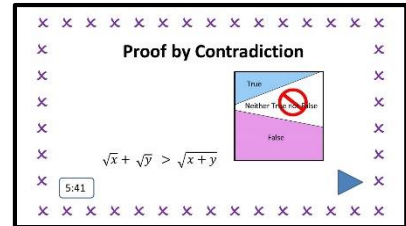
(Part 2) We have to pave over the front lawn. If we don't, the weeds will come back in the spring.

(Part 3) That door must be metal. If it weren't, all those magnets would have fallen off.

(Part 4) That new soda, Flash Gulp, must be low calorie. If it weren't, the glamorous actresses who advertise it would be fat.

Proof by Contradiction

Suppose that we want to prove some claim P . To use a proof by contradiction, we assume the negation of P and show that, by doing so, we derive a contradiction.



https://www.youtube.com/watch?v=M02_6Rp4yCU

In more detail: As usual, we assume that we are given some set of premises p_1 through p_n . Then (to simplify the rest of this discussion) let:

$$C = p_1 \wedge p_2 \wedge \dots \wedge p_n$$

We want to prove that, from C , we can derive P .

Here is the structure of a proof by contradiction of P :

[1]	C	Premises	
[2]	$\neg P$	(Conditional) Premise (Assuming the negation of our claim)	
...		(Reasoning, using C and $\neg P$, as appropriate)	
[k]	$\neg C$	(Using some rule that derives this final step)	
[k+1]	$\neg P \rightarrow \neg C$	Conditional Discharge	[2], [k]
[k+2]	$C \rightarrow P$	Contrapositive	[k+1]
[k+3]	P	Modus Ponens	[1], [k+2]

Note that the key to this proof is step [k]. We've shown that, given $\neg P$, at least one of our premises would have to be false. But we have asserted that they are all true.

So, in the last three steps of the proof, we show that, since the negation of P leads to a contradiction, P itself must be true.

$\sqrt{2}$ is Irrational

Let's now look at examples of the use of proof by contradiction (also called indirect proof) in mathematics.

Recall that a number is rational just in case it can be described as the ratio of two integers. In other words, it has the form $\frac{a}{b}$ for some integers a and nonzero b .

We can use a proof by contradiction to show that $\sqrt{2}$ is not rational. Suppose, to the contrary, that it were. Then there would exist integers a and nonzero b , such that:

$$[1] \quad \sqrt{2} = \frac{a}{b}$$

If a and b share any common factors, divide those factors out until a and b are relatively prime (i.e., they share no common factors). Another way to say this is that we reduce $\frac{a}{b}$ as much as possible. Squaring both sides of [1], we get:

$$[2] \quad 2 = \frac{a^2}{b^2} \quad \text{Multiplying by } b^2, \text{ we get:}$$

$$[3] \quad 2b^2 = a^2$$

So a^2 is even and it can only be so if a itself is even. (We'll prove that a^2 even implies a even in a couple of pages. Take it as a theorem for now.) Thus, there exists a k such that:

$$[4] \quad a = 2k.$$

Substituting $2k$ for a in [3], we get:

$$[5] \quad 2b^2 = (2k)^2 = 4k^2 \quad \text{Dividing by 2, we get:}$$

$$[6] \quad b^2 = 2k^2$$

So b^2 is even and thus b is even. So a and b are both even and thus both have 2 as a factor. But this cannot be so since we'd reduced $\frac{a}{b}$ until there were no common factors. Contradiction.

Problems

1. Try to cut and paste the proof we just did of the irrationality of $\sqrt{2}$ to show that $\sqrt{4}$ is also irrational. What happens?

- a) Everything is fine through [2] but [3] is different and we can't argue that a is even.
- b) Everything is fine through [5] but [6] is different and we can't argue that b is even.
- c) It works.

There is No Largest Prime Number

We'll now prove another important result using a proof by contradiction. We'll prove that there exists no largest prime number.

Consider the claim that there is no largest prime number. Following Euclid, we prove this claim by assuming, to the contrary, that the set P of prime numbers does contain some largest element. So there exists some value of n such that there are exactly n prime numbers and

$$P = \{p_1, p_2, p_3, \dots, p_n\}.$$

Let q be the product of all of those primes, plus 1. So we have:

$$q = (p_1 p_2 p_3 \dots p_n) + 1.$$

Since q is greater than each p_i , it is not on the list of primes. So it must be composite. In that case, it must have at least one prime factor, which must then be an element of P . Suppose that factor is p_k , for some $k \leq n$. Then q must have at least one other factor, some integer i such that:

$$\begin{aligned} q &= ip_k && \text{But } q \text{ was defined to be } (p_1 p_2 p_3 \dots p_n) + 1. \text{ So we have:} \\ (p_1 p_2 p_3 \dots p_n) + 1 &= ip_k && \text{Subtracting } ip_k \text{ and 1 from both sides, we get:} \\ (p_1 p_2 p_3 \dots p_n) - ip_k &= -1. \end{aligned}$$

Now observe that p_k evenly divides both terms on the left since it is prime and so must be in the set $\{p_1, p_2, p_3, \dots, p_n\}$. Factoring it out, we get the following (where we list all the primes up to p_k , then we skip it, and list all the ones after it):

$$\begin{aligned} p_k(p_1 p_2 p_{k-1} p_{k+1} \dots p_n - i) &= -1. && \text{Dividing by } (p_1 p_2 p_{k-1} p_{k+1} \dots p_n - i), \text{ we get:} \\ p_k &= \frac{-1}{p_1 p_2 p_{k-1} p_{k+1} \dots p_n - i} \end{aligned}$$

But, since the denominator $(p_1 p_2 p_{k-1} p_{k+1} \dots p_n - i)$ is an integer, this means that $|p_k| < 1$ (for the same reason that $\frac{1}{2}$ and $\frac{1}{4}$ are less than 1). But that cannot be true since p_k is prime and thus greater than 1. Contradiction. Recall that p_k was chosen to be some *arbitrary* prime factor of q . We now know that that *arbitrary* value is not in fact a prime number. So no other value can be a prime factor of q either. (Notice the way we have used Existential Instantiation and Generalization.) So q is not composite. Since q is greater than 1 and not composite, it must be prime, contradicting the assumption that all primes are in the set $\{p_1, p_2, p_3, \dots, p_n\}$.

Notice that the proof we just did, in addition to being a proof by contradiction, is **constructive**. It exhibits a specific example that contradicts the initial assumption. We'll soon see more uses of this proof by construction technique.

Problems

1. Prove that there exists no largest composite (nonprime) positive integer. (Hint: Start out the same way we just did to prove that there is no largest prime. But this proof is much simpler.)

Proving an Implication Using Contradiction

Suppose that we want to prove a claim of the form: $p \rightarrow q$

Sometimes the easiest way to do that is by contradiction. We assume its negation ($\neg(p \rightarrow q)$) and derive a contradiction.

The form $\neg(p \rightarrow q)$ isn't very easy to work with. Let's massage it a bit:

[1]	$\neg(p \rightarrow q)$		
[2]	$\neg(\neg p \vee q)$	Disjunctive Syllogism	[1]
[3]	$\neg\neg p \wedge \neg q$	De Morgan	[2]
[4]	$p \wedge \neg q$	Double Negation	[3]

Now it's clearer what we should do: Assume both p and $\neg q$. Derive a contradiction. Of course, we could resolve that contradiction by giving up p . But we won't. We'll stick to p . That means that q must be true. In other words $p \rightarrow q$.

In this example, we'll assume the axioms of plane geometry, including that, through any two distinct points, there is exactly one straight line.

Prove that, if two distinct straight lines intersect, then they do so at only one point.

The proof is by contradiction. Assume that two lines L_1 and L_2 are distinct and that they intersect at two or more different points. Call two of those points p and r . Then those two points are on both L_1 and L_2 . But there is exactly one straight line through those two points. This contradicts the hypothesis that L_1 and L_2 are distinct.

Problems

1. Definition: A **perfect** number is a positive integer that is the sum of all of its proper divisors (i.e., all its divisors, including 1, except itself). (Example: the proper divisors of 15 are 1, 3, and 5.)

Which of the following numbers as/are perfect: 6, 12, 17?

2. Prove that no perfect number is prime.

The Contrapositive (and Modus Tollens)

Now suppose that we know that some implication of this form is true:

$$p \rightarrow q$$

Then its contrapositive must also be true and we have:

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

So, if we know $\neg q$, the contrapositive gives us a straightforward way to derive $\neg p$ using Modus Ponens. Of course, an alternative is to use the original form ($p \rightarrow q$) and Modus Tollens, but that's not always quite so obvious a thing to do.

Suppose that we have that all college students are literate. Then we can prove that Morgan isn't a college student if we can show that Morgan isn't literate.

Another way to think of a contrapositive proof is that it is a proof by contradiction. We are given $p \rightarrow q$. We want to prove:

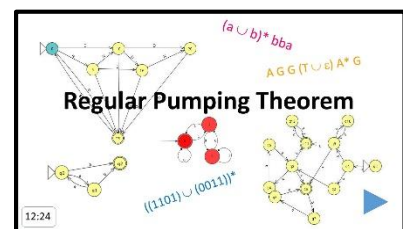
$$\neg p$$

We assume its contradiction, p . We can immediately derive q . If we can then reason and derive $\neg q$, we have found a contradiction that proves $\neg p$.

Using the Contrapositive: The Regular Pumping Theorem

In this video, we'll see an example of this approach.

The Pumping Theorem for regular languages is an important theorem in formal language theory. You can ignore its details. It is an interesting example of a significant and nontrivial contrapositive proof. Note that it requires that we negate an expression with four nested quantifiers.



<https://www.youtube.com/watch?v=Ih2onWfBrxk>

When Should We Try a Proof by Contradiction?

Given something that we want to prove, how do we know to try a proof by contradiction (an indirect proof)? One way is to try to write a direct proof and discover that we're not making much progress.

Suppose that we want to prove:

[1] For all integers n , if n^2 is even, then n is also even.

Sometimes it's enlightening to write our claim in our formal logical notation. We can do that here:

[1'] $\forall n (Even(n^2) \rightarrow Even(n))$

We might first try to prove this claim directly. From the definition of *Even*, we have, since we can assume that n^2 is even, that there exists some integer k such that:

[2] $n^2 = 2k$

We're interested in n . So we take the square root of both sides and we get:

[3] $n = \sqrt{2k}$

But now we're sort of stuck.

When we get stuck like this, it often makes sense to try an indirect proof.

We'll assume that the implication is false, namely that, for some n , n^2 is even but n is not even. In other words, n is odd, so there exists some integer k such that:

[4] $n = 2k + 1$

Squaring both sides, we have:

[5] $n^2 = (2k + 1)(2k + 1)$

Doing some simple algebra, we have:

[6]
$$\begin{aligned} n^2 &= 4k^2 + 2k + 2k + 1 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

But a number is odd just in case it is 1 more than some number that is divisible by 2. So we have that n^2 is odd. But that contradicts our starting premise that n^2 was even. Thus the assumption that n is not even must be false. So n is even.

Problems

1. Let n be any positive integer. Prove that, if n is a perfect square, $n + 2$ is not a perfect square.

Proof by Example or Counterexample

The Key Ideas

Existential Claims: Suppose that we want to prove that there exists *some object* with some desired property. We've seen that sometimes we can do that by combining premises with inference rules to derive a claim of the form $\exists x (P(x))$.

But sometimes we can do something even simpler:

We can prove that something exists by exhibiting it.

Prove: $\exists x (\text{Prime}(x) \wedge (x > 20))$

Proof: 23

Of course, it's not quite that simple. We do have to show that the example we've provided does meet the requirements of the claim we're trying to prove. Continuing with our example:

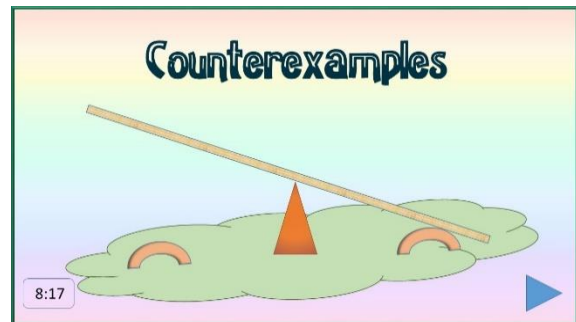
Since we are taking as theorems the claim of basic mathematics, we have that $23 > 20$. And we can show that 23 is prime by showing that it is not evenly divisible by any positive integer that is less than it. (This works because there is a finite number of such integers. So we can simply try all of them.)

Universal Claims: We've already seen examples of the use of both direct and indirect (by contradiction) proof to prove claims of this sort.

But sometimes we can do something even simpler:

We can prove that a universal claim is *false* by exhibiting a single counterexample.

<https://www.youtube.com/watch?v=oJGraKc1Sjc>



Consider the claim: $\forall x ((x > 1000) \rightarrow \text{Composite}(x))$. Maybe we think this is likely because large numbers have a lot of potential factors.

Proof that the claim is false: 1013, which we can show is prime by showing that it is not evenly divisible by any integer less than it.

Consider the claim: All birds can fly.

Proof that the claim is false:

Emus are birds.

Emus cannot fly.

Many nonflying emus have been observed
(including this baby one).



Problems

1. Consider the following claim:

There exists a quadratic equation with a single root.

- a) This claim is true and can be proved by a single example.
- b) This claim is true but cannot be proved so with a single example.
- c) This claim is false and can be shown so by a single counterexample.
- d) This claim is false but cannot be proved so with a single counterexample.

2. Consider the following claim:

$$\forall x \left(\frac{x}{3} < x-3 \right)$$

- a) This claim is true and can be proved by a single example.
- b) This claim is true but cannot be proved so with a single example.
- c) This claim is false and can be shown so by a single counterexample.
- d) This claim is false but cannot be proved so with a single counterexample.

Prime Fermat Numbers

Over the course of the history of mathematics, counterexamples have played a key role in blowing away claims that were made, but not proved, by some great mathematicians.

Recall from Chapter 6 that a Fermat number is an integer that can be expressed as $2^{2^n} + 1$, for some nonnegative integer n . The first seven Fermat numbers are 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617.

Fermat made the following conjecture about Fermat numbers (although he didn't call them that):

All Fermat numbers are prime.

But he only computed the first five (up to 65537). All it took was a single counterexample to prove him wrong. Leonhard Euler computed the sixth Fermat number (4294967297) and showed that it is composite.

On the basis of what we now know about these numbers, here's a new claim:

All Fermat numbers after the first 5 are composite.

No one has yet succeeded in proving this claim. Nor has it been disproved (which could also be done with a single counterexample).

Nifty Aside

Visit <http://www.prothsearch.net/fermat.html> for the effort to check larger and larger Fermat numbers to see whether they can be factored.

Proof by Example

Let's return to the problem of proving that something exists.

Approach 1: Sometimes it's possible to do a nonconstructive proof by traditional forward reasoning.

Suppose that we want to prove that there exists someone who is Sandy's mother. We have two premises:

[1]	$\forall x (Person(x) \rightarrow \exists y (MotherOf(y, x)))$	All people have mothers.
[2]	$Person(Sandy)$	Sandy is a person.

We need two steps to complete our proof:

[3]	$Person(Sandy) \rightarrow \exists y (MotherOf(y, Sandy))$	Universal Instantiation [1]	
[4]	$\exists y (MotherOf(y, Sandy))$	Modus Ponens	[2],
[3]			

So we know that Sandy has a mother, although we have no idea who that mother is.

But sometimes we may not be able to see how to make that approach work. When that happens, we can try what we'll call a constructive approach: we actually build (show) the required object.

Approach 2: We may be able to prove that something exists simply by finding and exhibiting the required object. In this case, the hard part is usually to find the object. Once it's found, actually writing the proof is often trivial.

Suppose that Chris is Sandy's mother. We could then prove that Sandy has a mother simply by exhibiting Chris.

Prove that there exist even numbers.

Proof: 2 is an even number. Now we have to show that it really is. By definition, a number is even if it is divisible by 2, which 2 is: $2 = 2 * 1$.

Prove that there exist two prime numbers whose sum is prime.

Proof: There are many examples that work. But we'll show a simple one: $2 + 3 = 5$.

Approach 3: Suppose that we want to prove not just the existence of one individual (e. g., one prime number or one buffalo). Instead, we want to show that *every* prime number has a successor or that, for *every* buffalo, there exists a head (for sure, not the same head for every buffalo). Now what we might do is to describe an algorithm that, when given an individual object, finds the required associated one. We'll talk about this more later in a separate section on proof by construction.

Problems

1. Prove that there exists a multidigit prime all of whose digits are the same.

Nifty Aside

(Hint: Visit <http://mathforsmartypants.com/resources/primecheck.php> for a nice primality checking app.)

Find an example that proves this claim.

2. Recall Goldbach's conjecture:

Every even integer greater than 2 can be expressed as the sum of two primes.

By the way, recall that 1 is not a prime. The smallest prime is 2.

Can even integers be expressed as the sum of two primes *in more than one way*? Try to prove this claim:

There exists an even integer greater than 2 that can be expressed *in two different ways* as the sum of two primes (where $a+b$ and $b+a$ don't count as different).

Which of the following is true:

- a) There is no such even integer.
- b) There is an integer less than 10 that proves the claim.
- c) There is an integer greater than 20 that proves the claim.

3. Define: An integer n is a **perfect square** if there exists some integer k such that $n = k^2$. For example, 100 is a perfect square because it is equal to 10^2 .

Prove that there exist distinct positive integers m , n , and r such that each is a perfect square and $m = n + r$. (Hint: When you need to look for integers, it's often a good idea to start small. If you try that and it doesn't work, a good next strategy is to write a program to do the looking. But you won't have to do that for this problem.)

Proof by Counterexample

Suppose that we are considering a universal claim. So we might have something like one of these expressions:

- [1] $\forall x (P(x))$
- [2] $\forall x (\exists y (P(x, y)))$
- [3] $(\exists x (Q(x))) \rightarrow (\forall y (P(y)))$

To prove that such a claim is true, it is necessary to prove that it holds for all values of all the universally quantified variables (drawn from the universe that we are discussing).

But to prove that such a claim is false, it suffices to find a single counterexample. The existence of even one such counterexample means that the claim cannot be true for *all* values.

Assume the universe of positive integers. Consider the following claim:

- [1] $\forall n (\text{Prime}(3^n + 2))$

Suppose that we don't have a clue how to prove the claim. In fact, we don't even know whether it is true. One thing we could try is to examine it for several values of n to see if we can find a pattern. Doing that, we get:

$n = 1$	$3^1 + 2 = 5$	Prime	
$n = 2$	$3^2 + 2 = 11$	Prime	
$n = 3$	$3^3 + 2 = 29$	Prime	
$n = 4$	$3^4 + 2 = 83$	Prime	All prime so far, but no clue why, so keep going.
$n = 5$	$3^5 + 2 = 245$	Not Prime	

We're done. We have proved that [1] is false.

Single counterexamples also disprove everyday kinds of claims.

Recall our **Contagious Disgruntledness** example. We have a group of people among whom grumpiness is highly contagious. If even one person gets disgruntled, the bad vibes will quickly spread to the whole group. So we wrote:

- [1] $(\exists x (\text{Disgruntled}(x))) \rightarrow (\forall z (\text{Disgruntled}(z)))$

How could we prove that this claim is false? The conclusion of the implication is only guaranteed if there exists at least one disgruntled person. But, if there does, then everyone else must be disgruntled too. So, we could prove this claim false if we could both find one disgruntled person (or, alternatively, prove the claim that such a person exists) and then find even one other person who isn't disgruntled. So, for example, we can prove that [1] is false if we have two more claims:

- [2] $\text{Disgruntled}(\text{Grouchy})$
- [3] $\neg \text{Disgruntled}(\text{Sunshine})$

Big Idea

A single example says nothing about the truth of a universal claim. Yet a single counterexample says everything about the falsity of such a claim.

Assume the universe of positive integers. Define n factorial (written $n!$) as:

$$[1] \quad n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1$$

For example, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

Now consider the following claim:

$$[2] \quad \forall n \text{ (Even}(n!))$$

Consider the following "proof" of [2]: Let $n = 4$. Then $n! = 24$, which is even.

NOT A PROOF. We attempted to prove a universal claim with a single example.

But now consider the following proof that [2] is false: Let $n = 1$. Then $n! = 1$, which is odd.

PROOF: In this case, a single counterexample suffices to show that [2] is false.

(By the way, $n = 1$ is the only counterexample to this claim. You might try to prove:

$$[3] \quad \forall n ((n > 1) \rightarrow \text{Even}(n!))$$

Here is a proof:

$$\text{If } n > 1, \text{ then } n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$$

Thus $n!$ has 2 as a factor and thus is even.)

Problems

1. Hypothesis: It matters to be tall. More specifically, all US Presidents have been at least 6' tall. Prove or disprove this claim.

2. Let our universe of discourse be the positive integers. Consider the following claim:

$$[1] \quad \forall x ((\exists y (y \geq x)) \rightarrow (\exists z (\neg(z \geq x))))$$

(In English, this says:

Every positive integer has the property that, if there exists some integer that is equal to or greater than it then there also exists an integer that is less (i. e., not greater than or equal) than it.)

We'd like to try to prove either that [1] is true or that it's false. We've decided to look for counterexamples. Do it. Which of these statements is true:

- a) There is exactly one counterexample that shows that [1] is false.
- b) There are exactly two counterexamples, either of which would suffice to show that [1] is false.
- c) There is an infinite number of counterexamples, any one of which would suffice to show that [1] is false.
- d) There are no counterexamples. [1] is true.

3. Let our universe of discourse be the positive integers. Consider the following claim:

$$[1] \quad \forall n (\text{Prime}(3^n + 1))$$

We'd like to try to prove either that [1] is true or that it's false. We've decided to look for counterexamples. Do it. Hint: Make a spreadsheet with one column for values of n and one column for the expression $3^n + 1$.

Which of these statements is true:

- a) There is exactly one counterexample that shows that [1] is false.
- b) There are exactly two counterexamples, either of which would suffice to show that [1] is false.
- c) There are at least three counterexamples, any one of which would suffice to show that [1] is false.
- d) There are no counterexamples. [1] is true.

4. Let our universe of discourse be the positive integers. Prove or disprove:

$$[1] \quad \text{For all } r, m, n, \text{ if } r \text{ divides } mn, \text{ then either } r \text{ divides } m \text{ or } r \text{ divides } n.$$

Mersenne Numbers

We'll give one more example of a famous disproof by counterexample.

A *Mersenne number* is a number that can be expressed in the form $2^n - 1$, for some positive integer n . Here's a table of the first several Mersenne numbers:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2^n-1	1	3	7	15	31	63	127	255	511	1023	2047	4095	8191	16383

Now let's focus on those Mersenne numbers that happen also to be prime. We'll call these numbers *Mersenne primes*. (The name comes from the 17th century monk, Marin Mersenne, who studied them.)

Problem

1. Here's the Mersenne numbers table again:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2^n-1	1	3	7	15	31	63	127	255	511	1023	2047	4095	8191	16383

Which of the Mersenne numbers shown in this table are prime?

Mersenne Numbers

Here's the Mersenne numbers table again, this time with all the prime numbers shown in red:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2^n-1	1	3	7	15	31	63	127	255	511	1023	2047	4095	8191	16383

Consider two statements:

1. If n is prime, then 2^n-1 is prime.
2. If 2^n-1 is prime, then n is prime. (Alternatively, if n is not prime, then 2^n-1 is not prime.)

Think about them. Do they appear to be true?

Problem

1. Here's the Mersenne numbers table again, this time with all the prime numbers shown in red:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2^n-1	1	3	7	15	31	63	127	255	511	1023	2047	4095	8191	16383

Just on the basis of the examples shown in the table above, what can you say about these two statements:

(Part 1) Statement 1 (If n is prime, then 2^n-1 is prime.):

- a) Could be true or it could be false. Either case would be consistent with the examples in the table.
- b) Must be true (i.e., the examples in the table prove that it must be true.)
- c) Is not true. The table contains a counterexample to the universal claim.

(Part 2) Statement 2 (If 2^n-1 is prime, then n is prime.):

- a) Could be true or it could be false. Either case would be consistent with the examples in the table.
- b) Must be true (i.e., the examples in the table prove that it must be true.)
- c) Is not true. The table contains a counterexample to the universal claim.

Mersenne Primes

Hundreds of years ago, some mathematicians believed that statement 1 above (i. e., if n is prime, then 2^n-1 is prime) was true. Then, in 1536, Hudalricus Regius refuted the claim by showing (as we just did) a single counterexample: $2^{11}-1 = 2047$ is not prime.

But that was not the end of false conjectures about these numbers. The eponymous monk, Marin Mersenne, in 1644, made the claim that Mersenne numbers are prime if $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257 , but are composite for all other positive integers $n \leq 257$. Mersenne's claim was shown to be false by counterexample, over two hundred years later, when it was discovered that $2^{61}-1$ is also prime. Later discoveries showed other ways in which Mersenne was wrong. The correct list of values of $n \leq 257$ such that 2^n-1 is prime is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ and 127 .

48 Mersenne primes are now known. It's conjectured that there are infinitely many of them. Proving this will require more than just a longer list of them, however.

The story of these numbers is an excellent example of what proof by example/counterexample can do and what it cannot do:

- A universal claim *can* be refuted by a single counterexample.
- A universal claim *cannot* be proved even by a long list of examples.

Nifty Aside

To find out more about Mersenne numbers, visit <http://primes.utm.edu/mersenne/>.

Problems

1. Consider the claim:

$$[1] \quad \forall x (Prime(x) \rightarrow \neg Prime(x + 1))$$

Which of the following statements is true:

- a) [1] can be proved with a single example.
- b) [1] is true but cannot be proved with a single example.
- c) [1] can be proven to be false with a single counterexample.
- d) [1] is false but cannot be proven so with a single counterexample.

2. Consider the claim:

[1] Every sequence of 10 consecutive integers contains at least one prime number.

For example, the sequence 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 actually contains 4 primes (11, 13, 17, 19)

Which of the following statements is true:

- a) [1] can be proved with a single example.
- b) [1] is true but cannot be proved with a single example.
- c) [1] can be proven to be false with a single counterexample.
- d) [1] is false but cannot be proven so with a single counterexample.

Program (In)correctness and Proof by Counterexample

When we write code, we'd like to be able to prove that it's correct. What we mean by that is that, *in all circumstances*, it does what it is supposed to do. Unfortunately, this is often difficult. We typically can't do it by exhaustively enumerating all possible circumstances: there may be millions (or more) of them. Fortunately, there are other techniques that can be used, at least in some cases.

Sadly, it is sometimes easier to prove that a program is incorrect. All it takes is one counterexample. Finding this counterexample is often the job of the testing department. Of course, if they fail to find a counterexample, we're still not sure that there are no bugs. All we know is that we haven't found any yet.

Suppose that we are running an animal clinic. We have two technicians, Chris and Kelly, and each morning we want to split the animals between them in such a way that they each have the same number of animals to tend to that day.

Consider the following program (written in an easy to read pseudocode). Assume that `animal_list` is the list of animals to be tended.

1. Initialize both Chris's and Kelly's list to the empty list.
2. For odd values of i , starting at 1, and going to $\text{length}(\text{animal_list}) - 1$ do this:
 - 1.1. Assign the i^{th} animal to Chris.
 - 1.2. Assign the $(i+1)^{\text{st}}$ animal to Kelly.
3. Output the two lists.

Try simulating this program on a couple of possible `animal_lists`. On the basis of your experiments, do you think that this program works (i.e., all animals get assigned and both Chris and Kelly have the same number of animals to tend to):

- a) All of the time.
- b) Some but not all of the time. In this case, give an example where it does work and one where it does not.
- c) Never.

Problems

1. Suppose that we have a list of sales that have occurred during each month this year. We want to go through and tally how many sales occurred on each day. So, for example, we might output a table like this, which we'll call SUMMARY:

1	34
2	52
3	17



Consider the following program for doing this for the month of February. (The program is written in a hopefully easy to read pseudocode):

1. Initialize SUMMARY, an array that contains 28 rows: Set the values in the first column (corresponding to the date) to the sequence of integers 1, 2, ..., 28. Set all values in the second column to 0.
2. Walk through the list of sales records. For each one do this:
 - 1.1. Extract the date of the sale.
 - 1.2. Add 1 to that date's count in SUMMARY.
3. Output SUMMARY.

Try hand simulating this program. Which of the following is true of it:

- a) It works all the time.
- b) It works some but not all of the time. In this case, you should be able to give an example where it does work and one where it does not.
- c) It never works.

2. Suppose that we have a list of heights of all of the girls in the chess club. Call the list HEIGHTS. We want to compute the average height of the girls.

Consider the following pseudocode program for doing that:

1. Initialize SUM to 0.
2. Initialize NUMBEROFGIRLS to 0.
3. For each element of HEIGHTS do this:
 - 1.1. Add that element of HEIGHTS to SUM.
 - 1.2. Add 1 to NUMBEROFGIRLS.
4. Set AVERAGE to $SUM/NUMBEROFGIRLS$.

Try hand simulating this program. Which of the following is true of it:

- a) It works all the time.
- b) It works some but not all of the time. In this case, you should be able to give an example where it does work and one where it does not.
- c) It never works.

Quantifier Exchange and Proof by Example/Counterexample

Recall our rules for quantifier exchange. When we “push” *not* through \exists , we get \forall . So what may appear to be an existentially quantified claim may actually be a universally quantified one (or vice versa). That then changes our job from finding a single example/counterexample to finding a general proof (or vice versa).

Consider:

$$[1] \quad \neg \exists x (MuskOx(x) \wedge ColorOf(Purple, x))$$

That looks like an existence claim (i.e., that there exist no purple musk oxen). Can I prove it with one example?

Suppose that I exhibit one brown musk ox. Does that validate my claim? No.

Let's do quantifier exchange. We get:

$$[2] \quad \forall x (\neg (MuskOx(x) \wedge ColorOf(Purple, x)))$$

Using De Morgan, we get:

$$[3] \quad \forall x (\neg MuskOx(x) \vee \neg ColorOf(Purple, x))$$

Now it's clearer that I can't support my claim with a single example. In fact, how many musk oxen would I have to find before I can be sure of my claim? Answer: all of them. I could refute it, however, with the existence of a single purple musk ox.

Our original statement looked like an existence claim that could perhaps have been verified by finding one existence proof. But now it's clear that we have a universal claim.



Problems

1. Consider the claim, “No parents like rap music”. Which of the following statements is true:

- a) It could be proved by exhibiting one parent who likes rap music.
- b) It could be proved by exhibiting one parent who doesn't like rap music.
- c) It could be disproved by exhibiting one parent who likes rap music.
- d) It could be disproved by exhibiting one parent who doesn't like rap music.
- e) None of these.

2. Suppose that I exhibit a 250 lb hot dog. Which (one or more) of the following claims have I proved:

- I. $\neg \forall x (Hotdog(x) \rightarrow (weight(x) < 50))$
- II. $\forall x (Hotdog(x) \rightarrow \neg (weight(x) < 50))$
- III. $\exists x (Hotdog(x) \wedge \neg (weight(x) < 50))$



3. Assume that we have as a premise that peacocks are birds. Now suppose that I exhibit a white peacock. Which (one or more) of the following claims have I proved:

- I. $\forall x (Peacock(x) \rightarrow HasMultiColoredFeathers(x))$
- II. $\neg \forall (Bird(x) \rightarrow HasMultiColoredFeathers(x))$
- III. $\exists x (Peacock(x) \wedge \neg HasMultiColoredFeathers(x))$



Is It Really Impossible to Prove a Negative?

You've probably heard the adage:

It's impossible to prove a negative.

We now know that that's ridiculous.

But it certainly is true that *some* negative claims are indeed very hard to prove.

Consider the claim: There is no life in the universe except on Earth.

To prove this, we'd have to examine the entire universe (and be certain that our examination techniques are foolproof) or we'd have to be able to reason from a sufficiently exact model of the universe that we'd believe our conclusion.

So it's nearly certain that we'll never be able to prove this claim.

But some negative claims are straightforwardly provable. This often happens when those claims can be rewritten as positive ones using operators like Quantifier Exchange and De Morgan.

Let's reconsider the question of whether all birds can fly. Now we'll assert this specific negative claim:

$$[1] \quad \neg \forall x (Bird(x) \rightarrow CanFly(x))$$

This claim is easy to prove. Applying quantifier exchange to [1], we get:

$$[2] \quad \exists x \neg (Bird(x) \rightarrow CanFly(x))$$

Applying Conditional Disjunction to [2], we get:

$$[3] \quad \exists x \neg (\neg Bird(x) \vee CanFly(x))$$

Applying De Morgan and Double Negation to [3], we get:

$$[4] \quad \exists x (Bird(x) \wedge \neg CanFly(x))$$

To prove [4], it suffices to exhibit our baby emu who cannot fly.



Problems

1. Prove or disprove the following negative claim:

$$[1] \quad \neg \forall x (Even(x) \rightarrow Even(x+1))$$

Proof by Construction

The Key Idea – When One Value Depends on Another

So far, we've been able to prove (or disprove) claims by simply exhibiting a single example. But when an existential quantifier occurs inside the scope of another quantifier, it's possible (in fact likely) that the required example depends on the value of the variable that is bound by the outside quantifier.

Consider:

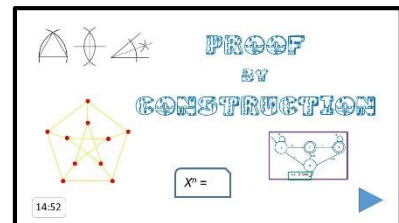
$$\forall x (\exists y (\text{MotherOf}(y, x)))$$

Note that this claim is true although there is no single y who is the mother of everyone.

In such cases, what we need to do is to describe a procedure that, when given a value of one variable, finds an appropriate value for the dependent variable. We must of course also argue that our procedure is correct.

So a proof by construction generally has the structure:

1. Describe the construction that produces the required value.
2. Prove that the resulting value actually does have the necessary properties.



<https://www.youtube.com/watch?v=90Uh0u9mpsw>

Sometimes we do the two parts in that order. Sometimes our argument for the correctness of the construction is part of our definition of the construction itself.

In the examples that follow, assume the standard axioms of arithmetic. Also assume that we can compute any standard arithmetic functions like addition and multiplication.

Consider the domain of integers. Prove: $\forall x (\exists y (y > x^2))$.

The proof is by construction. Given any value x , the following procedure computes a value y that satisfies the claim:

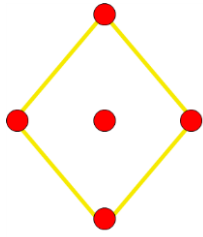
$$y = x^2 + 1$$

The value of y that is computed in this way must satisfy the claim: Since the domain is the integers, we have that $x^2 \geq x$. By adding 1, we guarantee that $x^2 > x$.

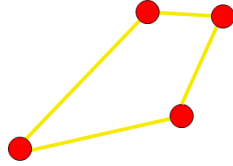
Notice that we can think of proof by example and counterexample as special cases of proof by construction: We have a simple procedure that takes no input and simply returns the one required object.

Problems

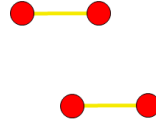
1. Indicate, for each of the following graphs, whether or not it is regular:



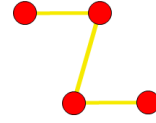
(a)



(b)

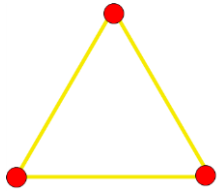


(c)

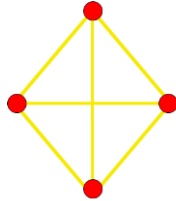


(d)

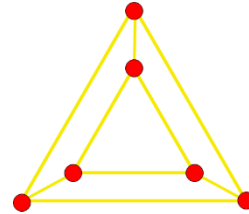
2. Indicate, for each of the following graphs, whether or not it is cubic:



(a)



(b)



(c)

3. Prove by construction that, for every fixed length character string, there exists a longer one.

The Usefulness of Constructive Proofs

Constructive proofs are often more useful than direct ones because they yield actual values that we can use.

We've already seen one example of this.

Prove that, for every prime number, there exists a larger one. In our proof that there is no largest prime (back in our discussion of proof by contradiction), we showed not only that such a larger one must exist, but we gave an algorithm for computing it: Define the sequence p_i of prime numbers, where $p_1 = 2$, $p_2 = 3$, and so forth. Now consider the n^{th} prime number, which we can write as p_n . Then q , as computed here, must be a prime number greater than p_n :

$$q = (p_1 p_2 p_3 \dots p_n) + 1.$$

In our proof by contradiction that there is no largest prime, we showed why q must, in fact, be prime.

Now let's look at another example.

Prove that every quadratic equation with real coefficients has at least one root.

First, notice that, while we didn't say so explicitly, this claim has the form of an existential quantifier inside a universal one:

\forall quadratic equations (\exists root)

The proof is by construction: Any quadratic equation can be written as: $y = ax^2 + bx + c$, where a is not 0.

Then the root(s) are given by the quadratic formula: $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

To complete the proof, we must show that this formula is correct:

Let: $x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$ and $x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$ These are the two roots.

Notice that $a(x - x_1)(x - x_2) = 0$ has solutions x_1 and x_2 . Notice also:

$$\begin{aligned} a(x - x_1)(x - x_2) &= a(x^2 - (x_1 + x_2)x + x_1x_2) \\ &= ax^2 - a(x_1 + x_2)x + ax_1x_2 \\ &= ax^2 - a\left(\frac{-b}{a}\right)x + a\left(\frac{b^2 - (b^2 - 4ac)}{4a^2}\right) \\ &= ax^2 + bx + c \end{aligned}$$

Thus x_1 and x_2 are also solutions to $ax^2 + bx + c$.

So we know not only that roots exist. We know what they are.

Prove that, for every positive integer n there exists a sequence of n consecutive positive integers containing no primes. For example, if n is 3, such a sequence would be 8, 9, 10. Another such sequence is 24, 25, 26. Again, notice the form of this claim:

$$\forall n (\exists \text{ sequence of consecutive positive nonprime integers of length } n)$$

We'll prove this claim by construction, which has the advantage of giving us an example of the desired sequence for any value of n .

How should we start designing our construction? The first thing we notice is that we need numbers that are composite. That means that every one of them must have some nontrivial (not itself or 1) factor. And that has to be true not just of the first one but of all the others that we get by adding 1, 2, etc. to it. Recall that $n!$ (n factorial) is defined to be $1 \cdot 2 \cdot 3 \dots n$. We observe that $n!$ has a lot of factors. And, in particular, every positive integer less than or equal to n is a factor. This might be a good place to start.

The sequence that we need is the sequence of n integers starting with $(n+1)! + 2$. To see why this works, observe:

Call the first element of the sequence x . Then we have:

$$x = (n+1)! + 2$$

The rest of the numbers in the sequence will then be $x + 1$, then $x + 2$, and so forth up to $x + (n - 1)$. That's n of them. To set the stage for the rest of the sequence, let's think of the first one as $x + 0$:

$$\begin{array}{rcll} x + 0 & = & (n+1)! + 2 + 0 & \text{Then we also have:} \\ x + 1 & = & (n+1)! + 2 + 1 & \\ & \dots & & \\ x + (n - 1) & = & (n+1)! + 2 + (n - 1) & \end{array}$$

More generally, for every value of i between 0 and $(n - 1)$, we have:

$$\begin{array}{rcl} [1] \quad x + i & = & (n+1)! + (2 + i) \\ & = & (n+1)! + (i + 2) \end{array}$$

Now, since i is less than n , $i + 1$ must be less than or equal to n and $i + 2$ must be less than or equal to $(n+1)$. So $i + 2$ is one of the factors of $(n+1)!$. Let's rewrite $(n+1)!$ so that we list the factors up to $i + 2$, then $i + 2$, then the remaining ones. That gives us:

$$[2] \quad x + i = (1 \cdot 2 \cdot \dots \cdot i \cdot (i + 1) \cdot (i + 2) \cdot \dots \cdot n \cdot (n + 1)) + (i + 2)$$

(Don't worry about what happens if i were, say, 2. We'll still include it only once in the expansion above. We've shown 2 explicitly here just to make it clear what's going on.)

Notice that the right hand side of [2] is the sum of two quantities, both of which have $(i + 2)$ as a factor. So we can factor it out, which produces:

$$[3] \quad x + i = (i + 2) \cdot ((1 \cdot 2 \cdot \dots \cdot i \cdot (i + 1)) + \dots n \cdot (n + 1)) + 1$$

Now we see that $x + i$ must be composite because it has two factors, neither of which is 1. (Since i starts at 0, $i + 2$ must be at least 2. In fact, that's why we had to add 2 to $(n+1)!$ to get the first value in our sequence.)

Problems

1. Indicate, for each of the following problems, whether it would be a good idea to try a proof by construction. Note: Sometimes a simple proof by single example is thought of as a proof by construction. Don't count it as that for this purpose.

- a) Prove that the only prime between 1000 and 1010 is 1009.
- b) Prove that every even integer can be written as the sum of two even integers.
- c) Prove that there is no longest English sentence.
- d) Prove that there exists a power of 2 whose decimal representation contains the digit 9.

2. Given any two numbers a and b , prove that, if $a < b$, then there exists some real number c such that:

$$a < c < b$$

Hint: Do the proof by construction. In this case, it probably makes sense to start by writing a formula for c . Then all that remains is to show that the formula is correct.

Divide and Conquer

Introduction

It often makes sense to divide complex problems into two or more simpler/smaller ones. We call this approach *divide and conquer*.

Divide and conquer can be a useful technique in constructing proofs.

Suppose that we are asked to prove: $P \rightarrow (Q \wedge R)$

We can divide it into two parts: We can prove that $P \rightarrow Q$ and, separately, possibly using different techniques, prove that $P \rightarrow R$.

We use divide and conquer all the time when we write nontrivial programs.

Consider the chess-playing robot REEM-A. REEM-A has cameras. It can see the board and observe the moves made by its opponent. It has a problem-solving engine that knows how to play winning chess. And it has actuators that enable it to move its own piece (and push the timer) once it has chosen a move.

To design REEM-A, it makes sense to break the problem down into at least these three pieces:

1. Scan the physical board and build an internal representation of which pieces are where.
2. Analyze the current board configuration and choose a next move.
3. Move the chosen piece to the correct location and then push the timer.

Very different algorithms (techniques) can then be used to solve each of those (slightly) smaller problems.



Problems

1. Suppose that we want to prove that Tracy can get a job. We have the following premises (involving the ability to graduate first):

- [1] $\forall x (Graduate(x) \rightarrow Job(x))$
- [2] $\forall x ((FinancialOK(x) \wedge ReqsOK(x)) \rightarrow Graduate(x))$
- [3] $\forall x ((LibOK(x) \wedge TuitionOK(x) \wedge FeesOK(x) \wedge AthlOK(x)) \rightarrow FinancialOK(x))$
- [4] $\forall x ((\neg Borrowed(x) \vee AllPaid(x)) \rightarrow LibOK(x))$
- [5] $\forall x ((StudentPaid(x) \vee ScholarshipPaid(x)) \rightarrow TuitionOK(x))$
- [6] $\forall x ((AthPaid(x) \vee \neg AthCard(x)) \rightarrow AthlOK(x))$
- [7] $\forall x ((Science(x) \wedge Rhetoric(x) \wedge Math(x) \wedge Social(x) \wedge Major(x)) \rightarrow ReqsOK(x))$
- [8] $\forall x (EnglishMajReqs(x) \rightarrow Major(x))$
- [9] $\forall x (CSMajReqs(x) \rightarrow Major(x))$

.....

There are likely hundreds of rules that could play a part in determining whether we can prove our goal:

Job(Tracy)

Imagine trying to find a proof by reasoning backward from our goal. Very early in this process, there's a chance to apply the Divide and Conquer strategy. There will be other opportunities as well. Which premise first (assuming reasoning backwards from the goal) suggests the use of Divide and Conquer?

Use of Lemmas

A common way to exploit the divide and conquer idea when we're trying to write proofs is to exploit lemmas. We prove smaller, intermediate results and then use them as though they were additional premises. The benefit of this approach is that it may help to avoid the combinatorial explosion that can occur when we're working with too many premises at once.

Recall that we did exactly this in one of our extensions to the *Who Drives Me* example.

We used these propositional variable names for the basic statements:

J : John must drive me to the store.
 M : Mary must drive me to the store.
 L : John will be late for work.
 G : Mary must buy gas.
 D : Mary must have money.

We assumed these premises:

[1] $J \vee M$ John or Mary must drive me to the store.
[2] $J \rightarrow L$ If John drives me to the store, he will be late for work.
[3] $\neg L$ John cannot be late for work.
[4] $M \rightarrow G$ If Mary must drive me to the store, she must buy gas.
[5] $G \rightarrow D$ If Mary must buy gas, she must have money.

We wanted to prove:

[6] D Mary must have money.

We could have started from scratch to prove that the premises imply the conclusion. In other words, we could have proven:

[7] $((J \vee M) \wedge (J \rightarrow L) \wedge (\neg L) \wedge (M \rightarrow G) \wedge (G \rightarrow D)) \rightarrow D$

But then we noticed that we'd already proven:

[8] M Mary must drive me to the store.

We can use [8] as a lemma. If we do that, we can ignore premises [1] – [3]. We can simply prove:

[9] $(M \wedge (M \rightarrow G) \wedge (G \rightarrow D)) \rightarrow D$

Simpler.

Throughout this course we've been using lemmas in a big way. We've been assuming all the standard facts about arithmetic and algebra.

We've also used as mathematical lemmas claims that we have proved in other places.

For example, recall that in our proof that $\sqrt{2}$ is irrational, we exploited the following claim that we proved elsewhere:

For all integers n , if n^2 is even, then n is also even.

Problems

1. Prove that if a quadratic equation with real coefficients has exactly one root then that root must be real. (Hint: Use the quadratic formula as lemma.)

Copy and Paste

Sometimes when we're working on a proof, we don't have exactly the theorem or lemma that we need. But we may have one that's very similar. When that happens, we may be able to start our new proof by cutting and pasting the proof that we've already got for the related theorem. Sometimes it works exactly as it is. More often, we need to tweak it. But at least we had a place to start from.

Suppose that we want to prove that everyone has a (possibly no longer living) great grandmother. (By the way, it's not important that you follow every line of this excruciating proof. The point of this example is that there has to be a better way to write proofs.)

Assume the following premises:

- [1] $\forall x (\exists y (\text{MotherOf}(y, x)))$
- [2] $\forall x (\exists y (\text{FatherOf}(y, x)))$
- [3] $\forall x (\forall y (\text{MotherOf}(y, x) \rightarrow \text{ParentOf}(y, x)))$
- [4] $\forall x (\forall y (\text{FatherOf}(y, x) \rightarrow \text{ParentOf}(y, x)))$
- [5] $\forall x (\forall y (\text{GreatGrandMotherOf}(y, x) \equiv (\exists z (\text{MotherOf}(y, z) \wedge \exists t (\text{ParentOf}(z, t) \wedge \text{ParentOf}(t, x))))))$ (Definition)
- [6] $\forall x (\forall y (\text{GreatGrandFatherOf}(y, x) \equiv (\exists z (\text{FatherOf}(y, z) \wedge \exists t (\text{ParentOf}(z, t) \wedge \text{ParentOf}(t, x))))))$ (Definition)

We need to prove:

$$\forall x (\exists y (\text{GreatGrandMotherOf}(y, x)))$$

Suppose that we wanted to do a detailed proof. Here's one. In case you want to follow the details, we'll add a key piece of information to every line that uses Instantiation or Generalization: Let p/x mean that, when we write the new line, we are substituting p for every instance of the variable x in the starting line. We're doing so many of these, that this may help make it clearer what is going on.

- | | | | | |
|------|---|---------------------------|-----------|----------|
| [7] | ($\exists y (\text{MotherOf}(y, p_1)$) | Universal Instantiation | p_1/x | [1] |
| [8] | $\text{MotherOf}(y_1^*, p_1)$ | Existential Instantiation | y_1^*/y | [7] |
| [9] | $\forall y (\text{MotherOf}(y, p_1) \rightarrow \text{ParentOf}(y, p_1))$ | Universal Instantiation | p_1/x | [3] |
| [10] | $\text{MotherOf}(y_1^*, p_1) \rightarrow \text{ParentOf}(y_1^*, p_1)$ | Universal Instantiation | y_1^*/y | [9] |
| [11] | $\text{ParentOf}(y_1^*, p_1)$ | Modus Ponens | | [8],[10] |
| [12] | $(\exists y (\text{MotherOf}(y, y_1^*))$ | Universal Instantiation | y_1^*/x | [1] |
| [13] | $\text{MotherOf}(y_2^*, y_1^*)$ | Existential Instantiation | y_2^*/y | [12] |
| [14] | $\text{ParentOf}(y_2^*, y_1^*)$ | Modus Ponens | | [8],[13] |
| [15] | $(\exists y (\text{MotherOf}(y, y_2^*))$ | Universal Instantiation | y_2^*/x | [1] |
| [16] | $\text{MotherOf}(y_3^*, y_2^*)$ | Existential Instantiation | y_3^*/y | [15] |

Notice that now we have that p_1 has parent y_1^* , y_1^* has parent y_2^* , and y_2^* has mother y_3^* . We're close. We need to use the definition of great grandmother [5]. But we only need it in one direction (the one that concludes great grandmotherhood), so let's split it out to make things easier:

[17]	$\forall x (\forall y ((\exists z (\text{MotherOf}(y, z) \wedge \exists t (\text{ParentOf}(z, t) \wedge \text{ParentOf}(t, x))) \rightarrow \text{GreatGrandMotherOf}(y, x)))$		[5]
[18]	$\forall y ((\exists z (\text{MotherOf}(y, z) \wedge \exists t (\text{ParentOf}(z, t) \wedge \text{ParentOf}(t, p_1))) \rightarrow \text{GreatGrandMotherOf}(y, p_1))$	Universal Instantiation p_1/x	[17]
[19]	$(\exists z (\text{MotherOf}(y_3^*, z) \wedge \exists t (\text{ParentOf}(z, t) \wedge \text{ParentOf}(t, p_1))) \rightarrow \text{GreatGrandMotherOf}(y_3^*, p_1)$	Universal Instantiation y_3^*/y	[18]
[20]	$\text{ParentOf}(y_2^*, y_1^*) \wedge \text{ParentOf}(y_1^*, p_1)$	Conjunction	[14], [11]
[21]	$\exists t (\text{ParentOf}(y_2^*, t) \wedge \text{ParentOf}(t, p_1))$	Existential Generalization t/ y_1^*	[20]
[22]	$(\text{MotherOf}(y_3^*, y_2^*) \wedge \exists t (\text{ParentOf}(y_2^*, t) \wedge \text{ParentOf}(t, p_1))$	Conjunction	[16], [21]
[23]	$(\exists z (\text{MotherOf}(y_3^*, z) \wedge \exists t (\text{ParentOf}(z, t) \wedge \text{ParentOf}(t, p_1)))$	Existential Generalization z/ y_2^*	[22]
[24]	$\text{GreatGrandMotherOf}(y_3^*, p_1)$	Modus Ponens	[23] [17]
[25]	$\exists y (\text{GreatGrandMotherOf}(y, p_1))$	Existential Instantiation y/y_3^*	[24]
[26]	$\forall x (\exists y (\text{GreatGrandMotherOf}(y, x)))$	Universal Generalization x/p_1	[25]

Q. E. D. (Whew!)

Now suppose that we want to prove that everyone has a great grandfather. We could start over. Our new proof would look a lot like the one we just did except that it would use the fact that everyone has a father [2] and the definition of great grandfather [6], instead of [1] and [5], as we have done. But it made us crazy to do this once. We'd certainly not want to do it again.

We cannot simply claim that we've already proved the new claim. We haven't. But there are some things we can do:

Cut and paste: Our new proof will be so similar to the one we've just done that we could simply cut and paste it and then make the few simple changes that are necessary. This technique actually works in many more significant domains as well. Don't forget about it.

The proof that we just did was messy. We don't want to spend a lot of time writing proofs like it. So let's remind ourselves of two other approaches that we've already discussed:

- We can prove lemmas (intermediate results) that we can reuse for new proofs.
- We can skip the four column format and write more natural proofs.

Let's consider both of these approaches to the great grandparents problem:

- Lemmas: We could, in doing the great grandmother proof, have proved that every person p has some parent y_1^* , who, in turn, has parent y_2^* . We could have given that claim a name as a lemma. Then we could have started the new proof and all we'd have had to add is that y_2^* has a father. Then we could have gone from there to p having a great grandfather.
- A more natural proof: And, of course, we could have skipped the four column proof entirely, thus avoiding having to make explicit mention of all of the instantiations and generalizations. We could, instead, have written something like:

Since everyone has a mother (and a father too, for that matter), everyone has a parent, who also has a parent, who also has a mother. That mother is a great grandmother of the original person.

Double Implication

Suppose that we want to prove a claim of the form:

$$P \equiv Q$$

In other words, P and Q share the same truth value.

Double implication statements of this sort often occur inside a universal quantifier. So we might have:

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

In other words, for any given x , either both P and Q are true of it or neither is.

The most straightforward way to prove equivalence claims of this sort is to rewrite $P \equiv Q$ as:

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

Now it's clear that we can do two (we hope) simpler proofs:

- Prove $(P \rightarrow Q)$.
- Prove $(Q \rightarrow P)$.

When we do those two proofs, we are free to use whatever techniques are appropriate (not necessarily the same ones for both directions).

Consider the claim:

$$[1] \quad \text{For any integer } x, (x + 2 \text{ is even}) \equiv (x^2 \text{ is even})$$

By the way, the intuition here is that both $x + 2$ and x^2 will be even if and only if x itself is even.

Prove that $(x + 2 \text{ is even}) \rightarrow (x^2 \text{ is even})$: Since $x + 2$ is even, we have that there exists an integer k such that:

$$\begin{aligned} x + 2 &= 2k \\ x &= 2k - 2 \\ &= 2(k - 1) \\ x^2 &= 2 \cdot 2(k - 1)^2 \end{aligned}$$

Since k is an integer, so is $k - 1$. So $(k - 1)^2$ is an integer and so is $2(k - 1)^2$. Thus x^2 is even.

Prove that $(x^2 \text{ is even}) \rightarrow (x + 2 \text{ is even})$: Let's try to do this in the same way we just did the first direction. We have that x^2 is even, so:

$$x^2 = 2k$$

We want to say something about x , so it's tempting to take the square root of both sides. We can do that, and we get:

$$x = \sqrt{2k}$$

But now we seem stuck. Our problem is that, in the first proof, we could square both sides and get integers. When we go the other direction and take the square root, we get something that we can't say much of anything about. We know that x is an integer (we're only talking about integers here). So, since $\sqrt{2}$ is not an integer, we know that k would have to have $\sqrt{2}$ as a factor. But this isn't getting us anywhere.

We're in a bind where we can't simply reverse what we did in proving the other direction. We appear stuck. When this happens, it's often a good idea to try a proof by contradiction (an indirect proof). It lets us, in a very restricted way, "reverse" our proof. Let's try it:

The proof is by contradiction. We are assuming that x^2 is even. Suppose that $x + 2$ were odd. Then there exists an integer j such that:

$$\begin{aligned}x + 2 &= 2j + 1 \\x &= 2j - 1 \\x^2 &= (2j - 1)^2 \\&= 4j^2 - 4j + 1 \\&= 2(2j^2 - 2j) + 1\end{aligned}$$

Now we can square both sides.

Since j is an integer, so is j^2 . So is $2j^2$. So is $2j$. And thus, so is $(2j^2 - 2j)$. By letting $k = (2j^2 - 2j)$, we have that x^2 is $2k + 1$. But this means that x^2 is odd, which contradicts the assumption that x^2 is even. So our supposition that $x + 2$ is odd, must be false. $x + 2$ must be even.

Proof by Case Enumeration

A common way to exploit the divide and conquer idea to prove a general claim is to divide the universe into a set of distinct cases. Of course, we must make sure that every element of the universe is included in one of the cases. But, if we can do that, we can then reason separately about each different case. Once we've done that successfully, we have a proof that the claim is in fact universally true.

There's a whole class of puzzles called Knights and Knaves. In all of them, there's an island on which live two kinds of people, knights, who always tell the truth, and knaves, who always lie. We've already (back in the chapter on Boolean Logic Proofs) considered one example of this sort of puzzle. We called it Fork in the Road. Let's now consider another one.

Suppose that Peachy, an islander, makes the statement, "At least one of my friend Figgy and me is a knave." What are Peachy and Figgy?

We can divide our analysis into two cases:

- Peachy, the speaker is a knight. In that case, he must be telling the truth. Then there has to be a knave and it's not Peachy. So it must be Figgy. So we have that Peachy is a knight and Figgy is a knave.
- Peachy, the speaker is a knave. In that case, he must be lying. But then both he and Figgy would have to be knights, which can't be true since we already know that Peachy is a knave.

Thus the only choice is our first one: Peachy is a knight and Figgy is a knave.

Nifty Aside

If we're working with simple Boolean expressions, it doesn't matter whether *everyone* lies or *everyone* tells the truth, as long as we know which it is. If I know that you're lying, I just put a *not* in front of whatever you say in order to get the truth. Of course, if claims carry more information, it could be really annoying for me to have to ask enough questions to get the answer I want. For example, if I know that you will lie and I want to know how much your car cost, I don't want to have to get the (known to be false) answer, "25,000", and then ask again and get another (known to be false) answer, "25,001", and so forth, until I can eventually figure out what price you don't mention.

But the idea that one can know for sure that people are telling the truth is interesting. If you haven't seen it, you might want to watch the movie, *The Invention of Lying*.



Consider a tic-tac-toe grid with the squares labeled as in (A):

1	2	3
4	5	6
7	8	9

(A)

1	2	3
O	X	6
7	8	9

(B)

Suppose that X moves first to square 5 and that O moves next to square 4. Then we have a board as shown in (B).

Prove that X can choose a move such there is nothing O can do to prevent X from winning.

The proof is by case enumeration:

If X moves to 1, then there are five choices for O: 2, 3, 6, 7, 8, and 9. Consider them:

- If O moves to 2, 3, 6, 7, or 8, then X moves to 9 and wins.
- If O moves to 9, X moves to 2. Then O has the options of 3, 6, 7, or 8. Consider them:
 - If O moves to 3, 6, or 7, then X moves to 8 and wins.
 - If O moves to 8, then X moves to 3 and wins.

Nifty Aside

Of course, tic-tac-toe is a trivial game. It's easy to play by enumerating all the cases. But what about interesting games like chess? It turns out that, while people can't play winning chess by enumerating all the possible move sequences, computers can win by enumerating "enough" possible move sequences. For example, in 1997 IBM's Deep Blue beat the then reigning human chess champion Garry Kasparov. While Deep Blue has some other chess knowledge, its main approach was to look ahead enough moves to be able to decide what to do next.

Problems

1. Here's another knights and knaves problem: Suppose that Peachy, an islander, makes the statement, "My friend Figgy and I are both knaves." What are Peachy and Figgy?

- a) Peachy and Figgy are both knights.
- b) Peachy and Figgy are both knaves.
- c) Peachy is a knight and Figgy is a knave.
- d) Peachy is a knave and Figgy is a knight.

2. Suppose that the postage required to mail a letter is always at least 6¢. Prove that it is possible to apply any required postage to a letter given only 2¢ and 7¢ stamps.



3. Prove that any two consecutive integers have opposite parity (i.e., one is even and the other is odd).

4. Assume the universe of integers. Prove:

$$[1] \quad \forall n (Even(n^2 + n))$$

5. Assume the universe of positive integers. Prove:

$$[1] \quad \neg \exists n (n^2 = 5)$$

Assume the following theorems:

$$[2] \quad \forall n (n^2 \geq n)$$

$$[3] \quad \forall n, m ((n^2 > m^2) \equiv (n > m))$$

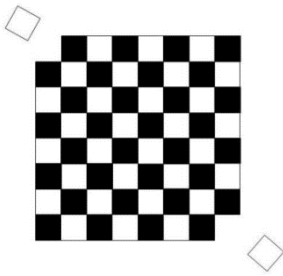
Hint: Use Proof by Contradiction. If [1] is false, what would have to be true?

Invariants

The Key Idea

When we solve a problem, we often take actions that change something. That's how we transform a "problem" into a "solution". Perhaps counterintuitively, we can often prove useful properties about our actions or our solution by relying on one or more key things that *don't change* as we solve the problem. We'll call these things that don't change *invariants*.

Consider a classic problem called the **mutilated checkerboard**.



Imagine that you are given a checkerboard that has been mutilated, as shown here. One square has been removed from each of two opposite corners.

Now consider the following question:



Can you cover the resulting mutilated board completely by placing nonoverlapping dominos on the squares? (Assume that each domino half exactly covers one checkerboard square.) Prove that your answer is correct.

What is your answer to this question? Hint: As you add dominos to the board, some things change. For example, the number of remaining empty squares decreases. You want to know whether it can decrease to 0. But is there some important property of the board that doesn't change?

Problems

1. Consider the following problem, which (following David Gries) we'll call the **coffee can problem**: We have a coffee can that contains some white beans and some black beans. We perform the following operation on the beans:

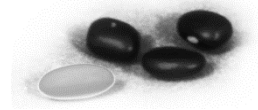
Until no further beans can be removed do:

1. Randomly choose two beans.
2. If the two beans are the same color, then throw both of them away and add a new black bean.
3. If the two beans are different colors, then throw away the black one and return the white one to the can.

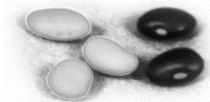
It is easy to show that this process must halt. After each step, the number of beans in the can decreases by one. When only one bean remains, no further beans can be removed.

But what can we say about the one remaining bean? Is it white or black?

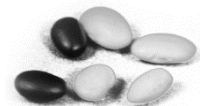
(Part 1) Suppose that the can starts with this collection of beans. What color is the remaining bean?



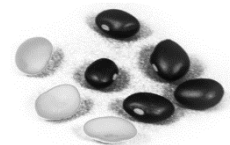
(Part 2) Suppose that the can starts with this collection of beans. What color is the remaining bean?



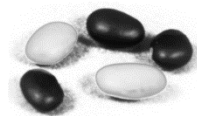
(Part 3) Suppose that the can starts with this collection of beans. What color is the remaining bean?



(Part 4) Suppose that the can starts with this collection of beans. What color is the remaining bean?



(Part 5) Suppose that the can starts with this collection of beans. What color is the remaining bean?



2. Now we'd like to generalize and make a statement about what color the last bean will be. To help us do that, a useful step will be to write down an explicit description of what can happen at each iteration. The rules are given above. Answer these questions to describe them:

If two white beans are chosen, then:

- How does the number of black beans change?
- How does the number of white beans change?

If two black beans are chosen, then:

- How does the number of black beans change?
- How does the number of white beans change?

If one black bean and one white bean are chosen, then:

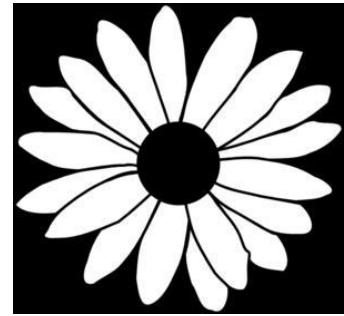
- How does the number of black beans change?
- How does the number of white beans change?

(Part 1) Now can you describe a pattern that lets you tell, for an arbitrary starting collection of beans, what color the last bean will be? Hint: Is there an invariant that helps? Look back at what happens in each of the three cases described above. Is there some important property that doesn't change?

(Part 2) Which one of the following is true:

- a) There is a useful invariant property of the number of white beans.
- b) There is a useful invariant property of the number of black beans.
- c) There is a useful invariant property that involves both the number of white and black beans.
- d) There is no useful invariant property.

2. Now consider the **Daisy Petal Game**. There are two players. When the game starts, there's a daisy with 18 petals. The players alternate turns. At his turn, a player may remove a single petal or a pair of adjacent petals (where adjacent means that the petals were adjacent in the original flower, before any petals were removed). The player who removes the last petal wins.



We want to answer the question, “Is there a guaranteed winning strategy?” And we want to prove that that answer is correct.

If you'd like to play the game to help you understand it, you can. Visit <http://www.novelgames.com/en/spgames/daisy/>

Let's start our analysis by considering a couple of simpler versions of the problem. Suppose that there are initially only 4 petals.

Should you elect to play first or second?

Now imagine that the petals are numbered 1 – 4 and consider:

- a. If your opponent moves first and takes petal 1, what should you do?
- b. If your opponent moves first and takes petals 1 and 2, what should you do?

Now suppose that there are initially 6 petals, numbered 1 – 6:

- a. If your opponent moves first and takes petal 1, what should you do?
- b. If your opponent moves first and takes petals 1 and 2, what should you do?

Now try it with a flower with 8 original petals. Can you see a pattern?

(Part 1) Which of the following is true? (Before you answer this, you should have in mind a winning strategy, if there is one, or an argument for why no such strategy exists.)

- a) There is a guaranteed winning strategy for the player who plays first.
- b) There is a guaranteed winning strategy for the player who plays second.
- c) There is no guaranteed winning strategy for either player.

(Part 2) Which of the following is true:

- a) There is a useful invariant property of just the number of remaining petals, regardless of which ones there are.
- b) There is a useful invariant property of the number of remaining petals but it also matters which ones they are.
- c) There is no useful invariant property.

See the Appendix for a discussion of our solution to this problem.

Mathematical Induction I

Summation Notation

Suppose that we want to talk about the sum of some sequence of values. One way to do that is to write something of the form:

$$v_1 + v_2 + v_3 + v_4 + \dots$$

For example, we could describe the sum of the first 100 positive integers as:

$$1 + 2 + 3 + 4 + 5 + \dots + 100$$

But what if it is not completely obvious to all of our readers exactly what the rest of the ... sequence is? Using this notation can be risky.

So we need a clearer, more formal notation. The one that we'll use exploits Σ (Sigma). To use Σ , we must specify:

- A name for a placeholder variable that we can use to describe values,
- The starting value for that variable,
- The ending value for that variable, and
- A description of the values to be added.

We specify these things by writing a statement of this form:

$$\sum_{\text{variable}=\text{starting value}}^{\text{ending value}} \text{some expression involving variable}$$

We'll read such an expression as, "The sum, as <variable> goes from <starting value> to <ending value> of <expression>". Of course, when we actually do this, we don't write or say "variable" or "starting value" or "ending value" or "expression". We substitute specific values. Note that the starting and ending values themselves are explicitly included.

For example, we can describe the sum of the first 100 positive integers as:

$$\sum_{i=1}^{100} i$$

Read this expression as, "The sum, as i goes from 1 to 100 of i ." So it's $1 + 2 + \dots + 99 + 100$.

The expressions that we write for both starting value and ending value can be written in a general form, in terms of other variables whose values we plan to fill in later.

For example, here's a general description of the sum of the first n positive integers:

$$\sum_{i=1}^n i$$

The sum is performed on the values in the range, starting value ... ending value. But we can add constraints so that not all values in that range are included.

For example, here's a description of the sum of just the *odd* integers, starting at 1 and going up to 10:

$$\sum_{\substack{i=1 \\ i \text{ odd}}}^{10} i$$

In other words, $1 + 3 + 5 + 7 + 9 = 25$.

The expression that we sum can be arbitrarily complex.

For example, here's a description of the sum of the first n values that are one less than some integer power of 2:

$$\sum_{i=1}^n (2^i - 1)$$

In other words $(2^1 - 1) + (2^2 - 1) + (2^3 - 1) + (2^4 - 1) + \dots (2^n - 1)$.

Problems

1. What is the value of:

$$\sum_{i=1}^{10} i$$

2. What is the value of:

$$\sum_{k=0}^4 (2^k + 1)$$

3. What is the value of:

$$\sum_{\substack{k=3 \\ k \text{ even}}}^{10} (2k + 1)$$

Our First Example of Induction

Suppose that we want to make some sort of useful claim about the nonnegative integers (or anything else that can be characterized by them, e.g., the size of some set).

For example, suppose that we'd like to know what the sum of the first n positive integers is. In other words we want to fill in the blank here:

$$\forall n \geq 1 \left(\sum_{i=1}^n i = \underline{\hspace{2cm}} \right)$$

Recall that we read the expression $\sum_{i=1}^n i$ as, “the sum, as i ranges from 1 to n , of i .”

A common way to proceed is in two steps:

- 1) Explore and attempt to come up with an answer that we believe to be correct.
- 2) Prove that the answer is, in fact, correct.

Mathematical induction, the proof technique that we are about to describe, is a useful tool for doing step 2. But, of course, before we can use it, we have to do step 1. Let's continue with the summation example to see how we can do that for the summation problem. Then we'll introduce induction to see how we can use it to prove our claim.

Think about it this problem. Can you fill in the blank? When you're ready, turn the page and let's discuss it.

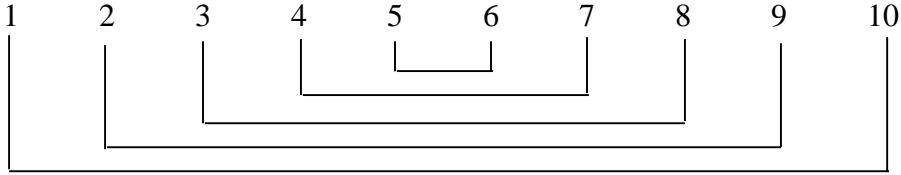
The Sum of the First n Positive Integers

We are trying to fill in the blank here:

$$\forall n \geq 1 \left(\sum_{i=1}^n i = \underline{\hspace{2cm}} \right)$$

Let's look at a few examples:

Let $n = 10$. Then we can lay out the numbers and pair them as shown here:



Notice that each pair sums to 11, which is $10+1$. And there are $\frac{10}{2}$ such pairs. So, when n is 10, we have that the sum of the first n integers is:

$$\frac{10}{2} \cdot (10 + 1), \text{ which we can rewrite as } \frac{10(10+1)}{2}, \text{ or } \frac{n(n+1)}{2}$$

This argument seems not to depend on n , so maybe we've got the answer in general. But, because we divided by 2, maybe our system only works for even values of n . Let's try it for 9:



Now each pair sums to 10 (i.e., $n+1$). There are $\frac{n-1}{2}$ (i.e., 4) such pairs. And then we must add 5 (i.e., $\frac{n+1}{2}$). So, when n is 9, we have that the sum of the first n integers is:

$$\frac{(n-1)(n+1)}{2} + \frac{n+1}{2} = \frac{n(n+1)}{2}$$

We got the same answer as for 10.

So now we have a claim that we believe is true:

$$\forall n \geq 1 \left(\sum_{i=1}^n i = \frac{n(n+1)}{2} \right)$$

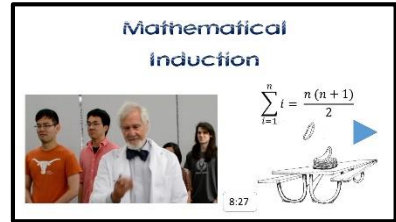
In other words, for any particular value of $n \geq 1$, the sum, as i goes from 1 to n , of i (i.e., the sum of the first n positive integers), is $\frac{n(n+1)}{2}$.

It is possible to generalize the argument that we just made and thus to turn it into a proof. But it's easy to make mistakes in arguments of this sort. More importantly, sometimes we have hunches like this that we can't see how to prove in this way.

What we need is a good, general purpose technique for proving claims of this sort. Mathematical induction is such a technique. Let's see how it works.

Visualizing Mathematical Induction

Suppose that we have a set S about which we want to prove some property P . Further suppose that the elements of S can be arranged in order such that:



[A] There is a smallest (first) element, and

[B] Every element, except possibly a final one, has a unique successor (i.e., next element) Video: <https://www.youtube.com/watch?v=fByqOD6CbR4>

Notice that we do not require that S be finite, although it may be.

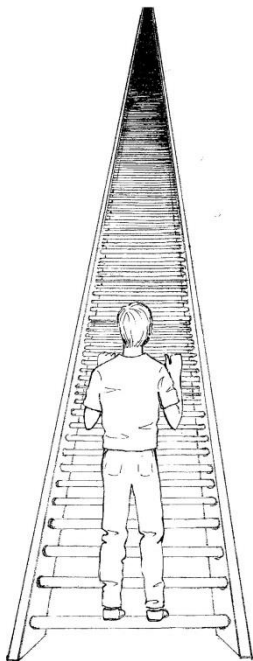
For example, the positive integers satisfy conditions [A] and [B]:

1 2 3 4 5 ...

The smallest positive integer is 1. And every positive integer has a unique successor, which we can compute simply by adding 1.

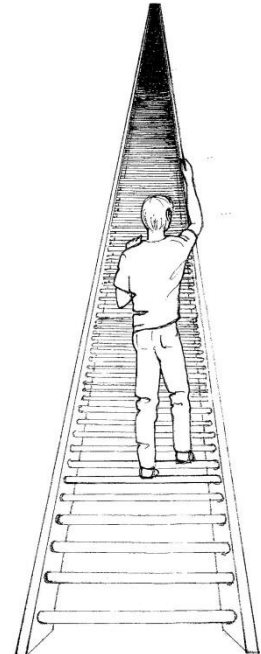
Then we can prove that every element of S satisfies P if we can show two things:

- The smallest (first) element satisfies P , and
- If any element satisfies P , so does its successor.



To visualize this, think about a man climbing an infinite ladder. Suppose that we know that he can step onto the first rung of the ladder. And we know that, whatever rung he's standing on, he can always reach the next one (simply by stepping up to it). Then we know that he can reach any arbitrary rung. He just needs to climb the ladder one rung at a time.

Let's call the informal technique that we've just described the ***ladder method*** (or the "flu shot method" if you prefer).



Problems

1. Starzzz is a hopelessly popular club. Outside the door the line is huge and getting longer every minute. It is, however, a perfect line – the bouncers see to that. Suppose that we want to prove that, eventually, everyone in the line will get the word that the star act has started. Is it possible that I could use the ladder method? (Hint: See if you can draw a ladder-like structure to describe the problem.)

- a) Yes. I could start with the person at the front of the line. He would be able to hear the act start. I could define the successor of someone to be the person behind him/her in line. Then I could use the ladder method if I could show that anyone who knows about the act will pass the word to their successor.
- b) No. The ladder method won't work because there's no reasonable first element.
- c) No. The ladder method won't work because there's no reasonable definition of successor.
- d) No. The ladder method surely won't work because there's no way we'll be able to show that anyone who knows about the act can pass the word on to their successor.

2. Consider the problem of proving that, no matter how far back I trace in a family tree, everyone has some property P . Is it possible that I can use the ladder method? (Hint: See if you can draw a ladder-like structure to describe the problem.)

- a) Yes. I could start with a current member of the family. I'd have to be able show that P holds for that person. Then I could define the successor of someone to be their parent. Then I could use the ladder method if I could show that, if P holds of some person x , then P must also hold of their parent.
- b) No. The ladder method won't work because there's no first element that I could start with.
- c) No. The ladder method won't work because there's no reasonable way to define the unique successor of someone.

3. Consider the problem of proving that, no matter how far back I trace in a family tree, everyone's mitochondrial DNA has some property P . Is it possible that I can use the ladder method? (Hint: Assuming no mutations, which we'll do, how is mitochondrial DNA inherited? Once you know the answer to that question, see if you can draw a ladder-like structure to describe the problem.)

- a) Yes. I could start with a current member of the family. I'd have to be able show that P holds for that person. I could define the successor of someone to be his or her mother. Then I could use the ladder method if I could show that, if P holds of some person x , then P must also hold of their mother.
- b) No. The ladder method won't work because there's no first element that I could start with.
- c) No. The ladder method won't work because there's no reasonable way to define the successor of someone.

The Principle of Mathematical Induction

Now we need to formalize the ladder method so that we can use it as the basis for a new, sound inference rule.

Before we do that, let's first define an important set:

\mathbf{N} = the *natural numbers*, i.e., the nonnegative integers. So \mathbf{N} contains 0, 1, 2, 3 and so forth.

Notice that \mathbf{N} possesses properties [A] and [B] as described on the previous slide:

[A] \mathbf{N} contains a smallest (first) element, namely 0.

[B] Every element of \mathbf{N} has a unique successor (i.e., next element). For any number n , its successor is $n+1$.

Now we can define a new inference rule that can be used to reason about \mathbf{N} . It is called the *Principle of Mathematical Induction*:

If: $P(b)$ is true for some natural number base case b , and
For all natural numbers $n \geq b$, $P(n) \rightarrow P(n+1)$

Then: For all natural numbers $n \geq b$, $P(n)$

We'll use this new rule when we want to show that some property P is true of every natural number (or maybe some subset of them, for example starting at 1 instead of 0).

And, by the way, we'll look later at examples in which we use mathematical induction to reason about sets other than the natural numbers. But typically, when we do that, we start by assigning a natural number to each element of the original set. So these is a first one, a second one, and so forth.

Nifty Aside

The soundness of the principle of mathematical induction rests on several key properties of the natural numbers. Where do those properties come from? Answer: the same place that everything we reason about comes from. We choose a set of axioms (premises) and then prove additional facts that can be derived from those axioms. In the case of the natural numbers, it's common to start with a set of axioms proposed by Giuseppe Peano (1858 – 1932). Peano's axioms form the basis for a large part of modern number theory.

A proof using mathematical induction, of an assertion of the form $\forall n (P(n))$ about some set of natural numbers greater than or equal to some specific value b , has three parts:

- 1) A clear statement of the predicate $P(n)$.
- 2) A proof that that P holds for some base case b , the smallest value with which we are concerned. Often, $b = 0$ or 1 , but sometimes P may hold only once we get past some initial unusual cases.
- 3) A proof that, for all integers $n \geq b$, if $P(n)$ is true, then it is also true that $P(n+1)$. We'll call the claim $P(n)$ the *inductive hypothesis*.

Let's look closely at what is going on in step 3. Let n be an arbitrary natural number. We reason as follows:

[1]	$P(n)$	(Conditional) Premise	
	Some reasoning steps in which we treat n as an <i>arbitrary</i> variable and we derive:	
[*]	$P(n + 1)$		
[**]	$P(n) \rightarrow P(n + 1)$	Conditionalization Discharge	[1], [*]
[***]	$\forall n (P(n) \rightarrow P(n + 1))$	Universal Generalization	[**]

Sometimes people read this process and come away thinking that we've assumed the thing we're trying to prove. No we haven't. We've assumed a conditional premise and then released it at the end by constructing a guarded conclusion. Then, since n was an arbitrary variable, we can generalize the claim to all values.

Returning to the ladder model: We are *not* assuming that it's possible to stand on rung n . We are assuming only that, *if it is possible to stand on rung n* , then it is possible to climb to rung $n + 1$.

Once steps 1 – 3 have been done, we appeal to the Principle of Mathematical Induction to assert:

$$\forall n (P(n))$$

The Sum of the First n Positive Integers

We're now ready to try our hand at using the Principle of Mathematical Induction.

Let's return to the claim that we derived several slides ago. It tells us what the sum of the first n positive integers is:

$$\forall n \geq 1 \left(\left(\sum_{i=1}^n i \right) = \frac{n(n+1)}{2} \right)$$

We want to prove it. Generally, before we try to prove a claim, we check for plausibility. We don't want to waste time trying to prove something that isn't true. But we've already done that in this case. So let's go directly to the proof.

The proof is by induction on n .

(Step 1) Define $P(n)$ (the property that we're trying to prove holds):

$$P(n) \equiv \left(\sum_{i=1}^n i \right) = \frac{n(n+1)}{2}$$

(Step 2, Base Case) Prove $P(b)$ for some appropriately chosen base case, b . It makes sense here to start at 1 (as we did in the statement of our claim) since we cannot sum zero numbers. So we must prove $P(1)$. We have (substituting 1 for n):

$$\left(\sum_{i=1}^1 i \right) = \frac{1(1+1)}{2} = \frac{2}{2} = 1 \quad \text{This is correct. The sum of the first 1 integer is 1.}$$

(Step 3, Inductive Step) Prove that $P(n) \rightarrow P(n+1)$. Before we start, we should expand this generic statement of the claim to specify the specific P we are trying to prove something about. So, specifically we must prove:

$$[1] \quad \text{For } n \geq 1, \left(\sum_{i=1}^n i \right) = \frac{n(n+1)}{2} \rightarrow \left(\sum_{i=1}^{n+1} i \right) = \frac{(n+1)((n+1)+1)}{2}$$

Note that, in the expression on the right, we've simply substituted $(n+1)$ for n .

Before we begin the proof of this claim, let's write out explicitly the induction hypothesis (the expression to the left of \rightarrow). We have:

$$\text{Inductive hypothesis: } \left(\sum_{i=1}^n i \right) = \frac{n(n+1)}{2} \quad \text{This is what we will assume.}$$

Now we must prove [1].

Observe that the sum of the first $n+1$ positive integers is the sum of the first n of them, plus the next one. So we have:

$$[2] \quad \left(\sum_{i=1}^{n+1} i \right) = \left(\sum_{i=1}^n i \right) + (n+1)$$

At this point, generally the thing to do is to look at what we've written and see whether there is any way to exploit the inductive hypothesis. For example, can we use it to substitute for some piece of an equation that we're working with? In this case the answer is yes. It tells us a value for $(\sum_{i=1}^n i)$. Let's substitute that value into [2], giving us:

$$[3] \quad (\sum_{i=1}^{n+1} i) = \frac{n(n+1)}{2} + (n+1)$$

$$[4] \quad = \frac{n(n+1)}{2} + \frac{2(n+1)}{2}$$

$$[5] \quad = \frac{(n+1)((n+1)+1)}{2} \text{ Check this against [1], the thing we're trying to prove.}$$

Thus we've shown that $\forall n (P(n) \rightarrow P(n+1))$. Since the summation formula holds for 1 and, if it holds for any integer n it must also hold for $n+1$, by the Principle of Mathematical Induction, we have:

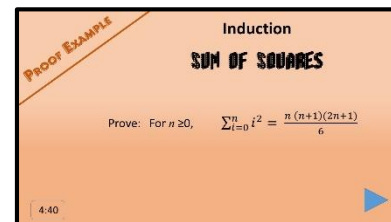
$$\forall n \geq 1 ((\sum_{i=1}^n i) = \frac{n(n+1)}{2})$$

The Sum of Squares

Let's prove another summation claim, again using induction.

Prove that, for $n \geq 0$,

$$\sum_{i=0}^n i^2 = \frac{n(n+1)(2n+1)}{6}$$



<https://www.youtube.com/watch?v=hit-K9EVAQY>

Problems

1. Consider the claim that the sum of the first n powers of 2 is $2^{n+1} - 1$. This time we want to start n at 0. So we can write the claim as follows:

$$\forall n \geq 0 \left(\sum_{i=0}^n 2^i \right) = 2^{n+1} - 1$$

Recall that we read this as, "For any $n \geq 0$, the sum, as i goes from 0 to n , of 2^i is $2^{n+1} - 1$. Using ... notation, we're claiming:

$$2^0 + 2^1 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 1$$

Also recall that $2^0 = 1$.

We first check for plausibility:

$(n = 0)$	1	= $2^1 - 1$	= 1
$(n = 1)$	$1 + 2$	= $2^2 - 1$	= 3
$(n = 2)$	$1 + 2 + 4$	= $2^3 - 1$	= 7
$(n = 3)$	$1 + 2 + 4 + 8$	= $2^4 - 1$	= 15, and so forth.

Now we'd like to use induction to prove that the claim is true. Do that in three steps:

- 1) Write an explicit statement of the predicate, which we'll call $P(n)$.
- 2) (Base Case) Prove that $P(n)$ holds for some base case b .
- 3) (Induction Step) Prove that, for all integers $n \geq b$, $P(n) \rightarrow P(n+1)$.

2. Consider the claim that the sum of the first n odd positive integers is n^2 . We first check for plausibility:

$(n = 1)$	1	= 1 = 1^2 .
$(n = 2)$	$1 + 3$	= 4 = 2^2 .
$(n = 3)$	$1 + 3 + 5$	= 9 = 3^2 .
$(n = 4)$	$1 + 3 + 5 + 7$	= 16 = 4^2 , and so forth.

Let $Odd_i = 2(i - 1) + 1$ denote the i^{th} odd positive integer. (So, for example, the first odd positive integer is $2(1 - 1) + 1 = 1$. Then we can rewrite the claim as:

$$\forall n \geq 1 \left(\sum_{i=1}^n Odd_i \right) = n^2$$

(In other words, $(1 + 3 + 5 + 7 + \dots + n^{\text{th}} \text{ odd integer}) = n^2$.)

The claim appears to be true. Now use induction to prove it. Show the following three steps:

- 1) Write an explicit statement of the predicate, which we'll call $P(n)$.
- 2) (Base Case) Prove that $P(n)$ holds for some base case b .
- 3) (Induction Step) Prove that, for all integers $n \geq b$, $P(n) \rightarrow P(n+1)$.

Sequences

So far, we've used induction to prove claims about common sequences that we're used to working with (for example, the positive integers or the powers of 2).

We can also use it to prove claims about arbitrary sequences, particularly ones that we define in a way that corresponds to the way in which we write inductive proofs:

- First we specify one (or maybe two or some other small number of) elements that get the sequence going.
- Then we specify a formula that lets us compute the remaining elements from one (or some small number) of earlier elements.

One standard notation for specifying a sequence, say s , is to write it as:

$$s_1, s_2, s_3, \dots$$

Or sometimes it's useful to start numbering the sequence starting at 0, in which case we write it as:

$$s_0, s_1, s_2, \dots$$

Problems

1. In this problem, we'll start by defining a sequence. Then we'll prove something about its elements.

Define the following sequence:

$$\begin{aligned} a_0 &= 0, \\ \text{For all } n \geq 0, \quad a_{n+1} &= 3a_n + 1 \end{aligned}$$

Write out the first several elements of this sequence. What is a_5 ?

So far, it looks like the only way to determine the value of a particular element, for example a_5 , is first to compute the values for all the earlier elements in the sequence. But in the case of some sequences (and this is one), that's not so. We can write a formula that gives us the value directly.

Consider the following claim: For $n \geq 0$, $a_n = \frac{3^n - 1}{2}$.

Use induction to prove that this claim is true.

The Fibonacci Sequence

We've now seen that we can define a sequence of numbers by specifying one, or some small number, of starting values. Then we write a formula that computes the values of later elements from preceding ones.

One of the best studied examples of such a sequence is this one:

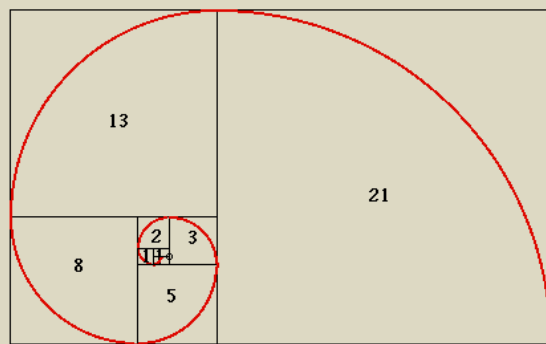
Define the *Fibonacci sequence* as follows:

$$\begin{aligned} f_1 &= 1, && \text{(The first element is 1.)} \\ f_2 &= 1, && \text{(So is the next one.)} \\ \text{for all } k \geq 2, f_{k+1} &= f_k + f_{k-1} && \text{(All other elements are computed from the two previous ones.)} \end{aligned}$$

The first several terms of the sequence are **1, 1, 1+1=2, 2+1=3, 3+2=5, 5+3=8, 8+5=13.**

Nifty Aside

The Fibonacci sequence has fascinated mathematicians for centuries. It is named for the Italian Leonardo Fibonacci (c 1170 – c 1250), who popularized it in Europe, although it was known before him in India. Fibonacci's most important contribution to European mathematics was the number system we now use (often called Arabic numerals). Unlike the Roman system, it exploits an explicit representation for zero. But the sequence that bears his name is also important for many reasons, including its relationship to the golden ratio and its appearance in the natural structure of many plants.



Problems

1. What is the value of f_9 (the 9th number in the Fibonacci sequence that starts with f_1)?

Mathematical Induction II

Proving Claims about Inequalities

Induction can be used to prove claims about inequalities, as well as equalities. Let's consider an interesting one (here we've used another common way of writing a universal claim):

$$\text{For } n \geq 4, n^2 \leq 2^n$$

This claim is significant. It says that, after a few small special cases, the value of the exponential function, 2^n , is always greater than or equal to the value of the quadratic function, n^2 .

Prove by induction: For $n \geq 4, n^2 \leq 2^n$

Define: $P(n) \equiv n^2 \leq 2^n$

Base case: $P(4)$ is true since: $4^2 = 16 \leq 16 = 2^4$

Inductive step: Prove that, for $n \geq 4, (n^2 \leq 2^n) \rightarrow ((n+1)^2 \leq 2^{n+1})$

Inductive hypothesis: $n^2 \leq 2^n$

https://www.youtube.com/watch?v=h_f5pAIVDFM

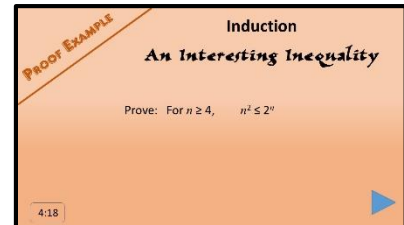
How should we start? Notice that we want to show that $(n+1)^2$ has some property (namely that it's less than or equal to 2^{n+1}). So let's start with $(n+1)^2$, do some algebra, and see if we can derive what we need.

[1]	$(n+1)^2 = n^2 + 2n + 1$	
[2]	$\leq n^2 + 2n + n$	Since n is at least 4 and thus > 1
[3]	$\leq n^2 + 3n$	
[4]	$\leq n^2 + nn$	Since n is at least 4 and thus > 3
[5]	$\leq 2n^2$	
[5]	$\leq 2 \cdot 2^n$	The inductive hypothesis says that $n^2 \leq 2^n$.

But $2 \cdot 2^n = 2^{n+1}$. So:

[6] $(n+1)^2 \leq 2^{n+1}$

Thus, by the principle of Mathematical Induction, we have proved our claim.



Notice that, in this example, the base case was 4 (not 0 or 1). That isn't uncommon. Often interesting properties don't appear until after a small number of special cases.

Problems

1. Consider this claim:

$$\text{For } n \geq 0, n < 2^n$$

Notice that this is yet another claim about a relationship between one function and another. For all positive integers, 2^n is greater than n itself.

We first check for plausibility. Do it for $n = 0, 1, 2,$ and 5 .

You'll find that the claim appears to be true. Now prove it.

2. Consider this claim:

$$\text{For } n \geq 4, n! > 2^n$$

Notice that this is yet another claim about a relationship between one function and another. Except for a few small special cases, $n!$ is always greater than the exponential function 2^n .

We first check for plausibility. Do it for $n = 4, 5,$ and 6 .

You'll find that the claim appears to be true. Now prove it.

Reviewing the Idea

So far, we've shown straightforward examples of induction proofs of claims about integer arithmetic. But induction can do way more than that. Recall the basic idea. We've shown it again in this rock climbing picture. If we can get started, and if, having made one step, we can always make the next one, we can show that we can make any number of steps.



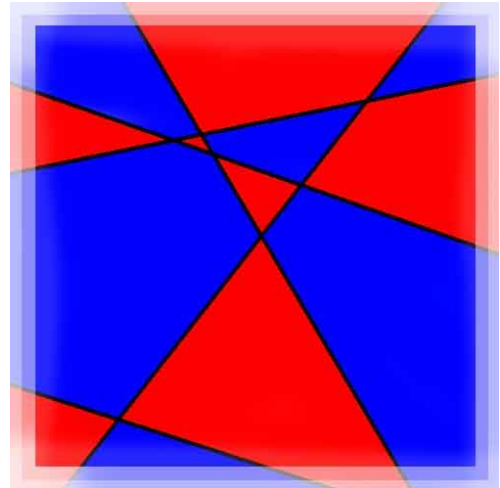
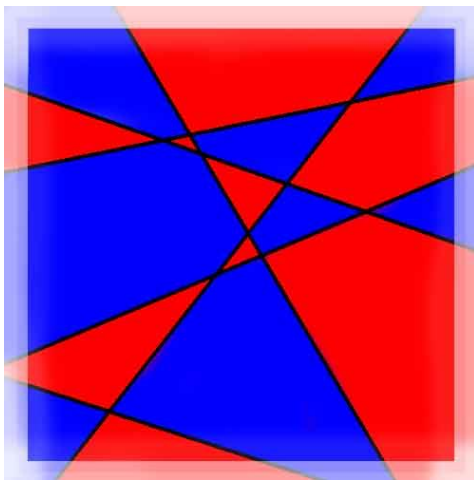
Big Idea

Mathematical induction is a powerful tool for proving that some property holds of natural numbers or anything that can be characterized by them.

Prove that, for $n \geq 1$, if the plane is cut by n distinct lines, the interiors of the regions bounded by the lines can be colored with red and blue so that no two regions sharing a common line segment as a boundary will be colored identically.

Here's an example that illustrates the idea. In this case, $n = 5$. To see whether you believe the claim, try adding one more line to the figure. Can you recolor it as required?

Here's what happened when we did that:



To prove the claim, we start by clearly articulating $P(n)$:

$P(n) \equiv$ If the plane is cut by n distinct lines, the interiors of the regions bounded by the lines can be colored with red and blue so that no two regions sharing a common line segment as a boundary will be colored identically.

Basis step: $P(1)$ is true since, if the plane cut by one line, two regions are formed. One may be colored red and the other blue. Thus the two regions are colored differently.

Inductive step: For $n \geq 1$, we prove $P(n) \rightarrow P(n+1)$.

Given the plane cut by $n+1$ distinct lines, select any one line and remove it. The plane is then cut by n distinct lines. By the inductive hypothesis, the interiors of the regions bounded by the lines can be colored with red and blue so that no two regions sharing a common line segment as a boundary will be colored identically.

Now reintroduce the $n+1^{\text{st}}$ line. Choose one side of that line. Reverse the color of all regions on the chosen side.

Consider any line segment s that corresponds to a boundary of some region we'll call r . Then s must lie either on the $n+1^{\text{st}}$ line or one of the other n lines but not both since the lines are distinct.

- If s lies on the $n+1^{\text{st}}$ line, then the $n+1^{\text{st}}$ line has cut across what was a larger region, which was thus divided into r and some other region t . The larger region previously had a single color. But the color on one side (but not the other) of the $n+1^{\text{st}}$ line (and thus s) has been flipped. So the two regions (r and t) on opposite sides of s must have different colors.
- The other case is that s lies on one side or the other of the $n+1^{\text{st}}$ line. (It can't cross the $n+1^{\text{st}}$ line because, if it did, it would be two separate boundary segments.) Since the regions on either side of s previously had different colors, they still do because, after the introduction of the $n+1^{\text{st}}$ line, either they were both unchanged or they were both reversed.

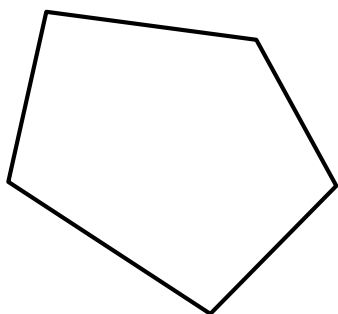
In both cases, the interiors of the regions bounded by the $n+1^{\text{st}}$ line can be colored with red and blue so that no two regions sharing a common line segment as a boundary will be colored identically.

So, by the principle of Mathematical Induction, our claim is true.

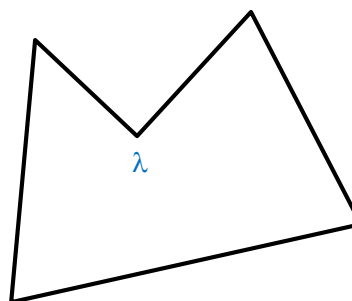
Problems

1. Prove by induction that, for $n \geq 3$, the sum of the interior angles of a convex polygon of n vertices is $(n-2) \cdot \pi$. Recall that a **convex polygon** is a polygon every one of whose interior angles is less than π (180°).

Consider:



(A)



(B)

(A) is convex. (B) isn't, because of the angle labeled λ . It is an inside angle, but it is larger than 180° .

The first step in writing our proof should be a clear articulation of $P(n)$. Write one.

The next step is the base case. What value of n should be used for the base case?

Now write your proof that P holds of the base case.

Now write your proof of the inductive step. You must prove:

$$\text{For } n \geq 3, \text{ if } P(n) \text{ then } P(n+1).$$

2. Prove that, for $n \geq 1$, $(\sum_{i=1}^n (4i - 3)) = n(2n - 1)$.

Start by writing an explicit statement of $P(n)$.

Base case. Prove it.

Induction step: Write out the specific claim that we must prove.

Now write out the proof.

3. Prove that, for $n \geq 1$, the product of any n odd integers is odd.

We need to start by writing an explicit statement of $P(n)$. Before we can do that, we need to define a notation for products. We'll use this:

$\prod_{i=1}^n f(i)$ is the product, as i goes from 1 to n , of $f(i)$.

Π is to multiplication what Σ is to addition.

So let o_i be the i^{th} odd number in some arbitrary list of odd numbers. (Note that they don't have to come in order: 1, 3, 5, Our claim applies to any n odd numbers.) Then:

$\prod_{i=1}^n o_i$ is the product of the n odd numbers in the given list.

Using this notation, write a definition of $P(n)$.

Base case. Prove it.

Induction step: Write out the specific claim that we must prove.

Write out the proof of the inductive step.

4. This problem is interesting, but harder than most of the ones we've done. We suggest that you try it, but do not get worried if you're not sure you've got it.

Define the **harmonic numbers** h_i , for $i \geq 1$ as:

$$h_i = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{i}$$

Or, using summation notation, we can say:

$$h_i = \sum_{j=1}^i \left(\frac{1}{j}\right)$$

These numbers have been studied for hundreds of years, as has the infinite **harmonic series**:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots$$

The harmonic series does not converge to any fixed value. As i grows, so does h_i , although it does grow very slowly. In this problem, we'll use mathematical induction to prove that this is so. To do that, we'll prove a claim about the harmonic numbers h_k , where k is a power of two. Specifically:

$$\text{For any integer } n \geq 0, h_{2^n} \geq 1 + \frac{n}{2}$$

First, you may want to convince yourself that this claim is believable. Write out the values of h_{2^0} , h_{2^1} , and h_{2^2} .

Let $n = 2$. What is h_{2^n} (i.e., h_4) to 2 decimal places?

To check our claim, what is $1 + \frac{n}{2}$? (n is still 2.)

So, at least in the case of $n = 2$, we have that $h_{2^n} \geq 1 + \frac{n}{2}$.

Now on to our proof. Write out an explicit statement of the proposition P that we are trying to prove.

Base case: Prove $P(0)$.

Induction step: We need to prove:

$$\left(h_{2^n} \geq 1 + \frac{n}{2}\right) \rightarrow \left(h_{2^{n+1}} \geq 1 + \frac{n+1}{2}\right)$$

Write this proof.

Induction Can be an Alternative Even When Other Proofs Exist

Many of the claims that we can prove by induction can also be proved in other ways. This shouldn't come as a surprise. We've already seen many other examples in which there existed more than one proof for a given claim.

Recall the stamp problem, which we've already proved using Case Enumeration:

Suppose that the postage required to mail a letter is always at least 6¢. Prove that it is possible to apply any required postage to a letter given only 2¢ and 7¢ stamps.

$P(n)$ \equiv It is possible to apply n ¢ using only 2¢ and 7¢ stamps.

Base case: Let $b = 6$. We can apply 6¢ by applying three 2¢ stamps.

Induction step: Prove:

[1] possible to apply n ¢ \rightarrow possible to apply $(n+1)$ ¢

Induction hypothesis: possible to apply n ¢

We'll now use Case Enumeration:

- To apply n ¢, we used at least one 7¢ stamp. In that case, to apply $(n+1)$ ¢, remove the 7¢ stamp and add four 2¢ stamps. We've added 1¢ to the total postage.
- To apply n ¢, we used only 2¢ stamps. Since n is at least 6, we must have used at least three of the 2¢ stamps. Remove three of them and add one 7¢ stamp. We've added 1¢ to the total postage.

So, by the Principle of Mathematical Induction, we have that it is possible to apply any required postage (i.e., any amount that is at least 6¢).



Mathematical Induction III

Strong Induction

So far, our inductive arguments have relied on our ability to prove:

If P holds **for a single arbitrary value n** , then it also holds for the next value, $n+1$.

Sometimes, however, we'll need to use a stronger form of induction; we'll argue:

If P holds **for all values up to n** , then it also holds for the next value, $n+1$.

We'll call the inference rule that allows us to do that ***strong induction***.

We can state the ***Principle of Strong Induction*** as follows:

If: $P(b)$ is true for some integer base case b , and

For all integers $n \geq b$:

$$(P(b) \wedge P(b+1) \wedge \dots \wedge P(n-1) \wedge P(n)) \rightarrow P(n+1)$$

Then: For all integers $n \geq b$, $P(n)$

Sometimes, to make clear which technique we're using, we'll call our old Principle of Mathematical Induction, ***weak induction***.

While we are calling this new form of induction “strong” and we're calling our old one “weak”, we should point out that, from a logical point of view, neither is stronger than the other. The soundness of one follows from the soundness of the other. Nevertheless, when we're trying to do proofs, we may find strong induction a more potent tool.

Just like proofs that use weak induction, a proof using strong induction, of an assertion of the form $\forall n (P(n))$ about some set of natural numbers greater than or equal to some specific value b , has three parts. The first two are the same. The third one is different because it can use the fact that we assume P is true of all preceding values, not just the immediately preceding one.

The three proof steps are:

- 1) A clear statement of the predicate $P(n)$.
- 2) A proof that that P holds for some base case b .
- 3) A proof that:

$$(\forall n \geq b (P(b) \wedge P(b+1) \wedge \dots \wedge P(n-1) \wedge P(n))) \rightarrow P(n+1)$$

As before, in step 3 we'll exploit an *inductive hypothesis*, which, as in weak induction, is the antecedent of \rightarrow . In other words, it's:

$$\forall n \geq b (P(b) \wedge P(b+1) \wedge \dots \wedge P(n-1) \wedge P(n))$$

Consider the following claim:

Every positive integer can be written as the sum of distinct powers of 2.

We'll prove it using strong induction. The idea is similar to the one we've used for all of our induction proofs. We want to prove something about $n+1$. We'll figure out a way to describe it in terms of some smaller number. But that smaller number may not be n . It could be any smaller number. So it would be very awkward to use weak induction.

We proceed in the usual three steps.

First we define $P(n) \equiv (n \text{ can be written as the sum of distinct powers of } 2)$

Base case: $P(1)$ is true because $1 = 2^0$.

Induction step: We must prove:

Every positive integer less than or equal to n can be written as the sum of distinct powers of 2

\rightarrow

$n + 1$ can be written as the sum of distinct powers of 2.

The induction hypothesis is, of course, the claim to the left of \rightarrow . Now we must figure out how to use it to prove our claim about $n+1$. We must find something relevant about $n+1$ to start with.

Consider any $n \geq 1$. There exists some integer k such that:

$$[1] \quad 2^k \leq n + 1 < 2^{k+1}$$

To see why this must be so, consider the powers of 2 laid out on a number line:

1 2 4 8 16 and so forth.

Then any integer (including $n + 1$), is either equal to one of these (i.e., it's 2^k for some k), or it's not, in which case it falls in some hole strictly between two numbers, 2^k and 2^{k+1} .

Suppose that $n + 1$ is equal to some 2^k . Then, trivially, it can be written as the sum of distinct powers of 2. It's just 2^k .

Now suppose that it's not equal to any 2^k . Then it's *strictly in between* two such values and we can rewrite [1] to say that:

$$\begin{array}{llll}
 [2] & 2^k & < n + 1 & < 2^{k+1} & \text{Just substituting } < \text{ for } \leq \\
 [3] & 0 & < n + 1 - 2^k & < 2^{k+1} - 2^k & \text{Subtracting } 2^k \text{ from all sides} \\
 [4] & & < n + 1 - 2^k & < 2^k & \text{Since } 2^{k+1} - 2^k = 2 \cdot 2^k - 2^k
 \end{array}$$

But we also know that $2^k \leq n$. To see why this is so, recall [2]. We have that 2^k is strictly less than $n + 1$. So it must be less than or equal to n . From [4] and the fact that $2^k \leq n$, we have:

$$[5] \quad 0 < n + 1 - 2^k < n$$

Since the value of $n + 1 - 2^k$ is positive, but less than n , the inductive hypothesis guarantees that it can be written as the sum of distinct powers of 2. Further, we know from [4] that $n + 1 - 2^k$ is less than 2^k . So all of those powers are less than k . So we have:

$$\begin{array}{ll}
 [6] & n + 1 - 2^k = \text{(some sum of distinct powers of 2, all less than } k) \\
 [7] & n + 1 = 2^k + \text{(some sum of distinct powers of 2, all less than } k)
 \end{array}$$

We've added one new power of 2, but we know that it is distinct from all the others. Thus $n + 1$ can be written as the sum of distinct powers of 2.

By the Principle of Strong Induction then, we have that every positive integer can be written as the sum of distinct powers of 2.

Nifty Aside

If the claim that we just proved weren't true, we wouldn't be able to represent numbers in modern computers. Why not? Computer memory is a long string of bits, or binary digits. At the hardware level, each bit corresponds to an electronic component that has two states. Think of it as on/off, or positive/negative, or something else. The only thing that matters is that there are exactly two states. We'll call them 0 and 1.

In the decimal number system that we use every day, a number is represented as the sum of powers of 10. So, for example, 5023 is $5 \cdot 1000 + 0 \cdot 100 + 2 \cdot 10 + 3 \cdot 1$. Note that each power of ten is multiplied by some factor between 0 and 9. If we needed to multiply by anything larger, we'd just use a higher power. So, for example, we don't say that 5023 has 23 1's. We give it 2 10's and just use 1's (3 of them) for the remainder. So we use digits from 0 up to 9 (which is $10-1$). In the binary system that computers use, a number is represented similarly, except as the sum of powers of 2. So we only need two digits, 0 and 1 (which is $2-1$). This is perfect if our hardware only has two states.

This means that we represent any natural number, in binary, as the sum of powers of 2. For example, $21 = 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$. So we represent 21 in binary (and in our computers) as 10101.

Fortunately, we now know that it's always possible to do this.

Problems

1. We've already seen that we can use weak induction to prove that there's always a solution to our stamps problem: Suppose that the postage required to mail a letter is always at least 6¢ . Prove that it is possible to apply any required postage to a letter given only 2¢ and 7¢ stamps. Recall that that solution required that we consider two cases when we did the inductive step. Using strong induction, we don't have to do that. Write the proof.



The Fibonacci Sequence

Recall that we can define a sequence of numbers by specifying one, or some small number, of starting values. Then we write a formula that computes the values of later elements from preceding ones. Notice the natural correspondence between the structure of a definition like this and the structure of an inductive proof. Thus, no surprise, we can often use induction to prove claims about sequences defined in this way.

We used exactly this technique to define the **Fibonacci sequence**:

$$\begin{array}{lll} f_1 & = 1, & \text{(The first element is 1.)} \\ f_2 & = 1, & \text{(So is the next one.)} \\ \text{for all } k \geq 2, & f_{k+1} & = f_k + f_{k-1} \quad \text{(Other elements are computed from the two previous ones.)} \end{array}$$

So the first several terms of the sequence are **1, 1, 1+1=2, 2+1=3, 3+2=5, 5+3=8, 8+5=13**.

Problems

1. Define the Fibonacci sequence as follows:

$$\begin{array}{lll} f_1 & = 1, & \text{(i.e., the first element of the sequence is 1)} \\ f_2 & = 1, & \text{(and so is the second element)} \\ \text{for all } k > 2, & f_{k+1} & = f_k + f_{k-1} \quad \text{(other elements computed from the two previous ones)} \end{array}$$

Prove that for all $n \geq 1$: $(\sum_{i=1}^n f_i^2) = f_n f_{n+1}$

The proof is by induction on n .

Define: $P(n) \equiv (\sum_{i=1}^n f_i^2) = f_n f_{n+1}$

Base case: Write a proof of the base case.

Induction step: Begin by writing the induction hypothesis

Write your proof.

Strong Induction Can Exploit Multiple Prior Values

So far, we've used strong induction to prove that every positive integer can be written as the sum of distinct powers of 2. When we did that, we exploited strong induction to do something that weak induction couldn't straightforwardly do: While we only needed to exploit the induction hypothesis to assert the truth of P for a single value, we reached back arbitrarily far to choose that value.

In the next example, we'll reach back in a more controlled way, but we'll need to use the induction hypothesis to assert the truth of P for *two* values (in particular n and $n - 1$). We'll prove a claim about the Fibonacci numbers. Because all but the first two values of this sequence are computed from the values of the previous *two* values, the most straightforward way to prove our claim is by strong induction.

Recall the definition of the Fibonacci numbers:

$$\begin{array}{lll} f_1 & = & 1, & \text{(The first element is 1.)} \\ f_2 & = & 1, & \text{(So is the next one.)} \\ \text{for all } k \geq 2, & f_{k+1} & = & f_k + f_{k-1} & \text{(Other elements computed from the two previous ones.)} \end{array}$$

We want to prove the following claim about the elements of this sequence:

$$[1] \quad \text{For all } n \geq 1: \quad f_n \geq \left(\frac{3}{2}\right)^{n-2}$$

The proof is by strong induction. We begin with a clear statement of P : For any $n \geq 1$,

$$P(n) \equiv f_n \geq \left(\frac{3}{2}\right)^{n-2}$$

$$\begin{array}{l} \text{Base cases: } P(1) \text{ is true: } \left(\frac{3}{2}\right)^{1-2} = \frac{2}{3}. \quad 1 \geq \frac{2}{3}. \\ P(2) \text{ is true: } \left(\frac{3}{2}\right)^{2-2} = 1. \quad 1 \geq 1. \end{array}$$

Induction step: We must prove that, for any $n > 2$, if $f_k \geq \left(\frac{3}{2}\right)^{k-2}$ is true for all positive values of k up to and including n , then $f_{n+1} \geq \left(\frac{3}{2}\right)^{(n+1)-2}$.

The induction hypothesis is that $f_k \geq \left(\frac{3}{2}\right)^{k-2}$ is true for all positive values of k up to and including n .

We begin by writing down what we know about f_{n+1} :

$$\begin{aligned} [2] \quad f_{n+1} &= f_n + f_{n-1} && \text{Definition of the sequence} \\ [3] \quad &\geq \left(\frac{3}{2}\right)^{n-2} + \left(\frac{3}{2}\right)^{n-3} && \text{Using the induction hypothesis twice.} \end{aligned}$$

At this point, we realize that we need to manipulate the right hand side expression to make it $\left(\frac{3}{2}\right)^{n-2}$. So we start trying to do that.

$$\begin{aligned} [4] \quad &\geq \left(\frac{3}{2}\right) \left(\frac{3}{2}\right)^{n-3} + \left(\frac{3}{2}\right)^{n-3} \\ [5] \quad &\geq \left(\frac{3}{2} + 1\right) \left(\frac{3}{2}\right)^{n-3} && \text{Factoring out } \left(\frac{3}{2}\right)^{n-3} \\ [6] \quad &\geq \left(\frac{5}{2}\right) \left(\frac{3}{2}\right)^{n-3} \\ [7] \quad &\geq \left(\frac{9}{4}\right) \left(\frac{3}{2}\right)^{n-3} && \text{Okay because } \left(\frac{9}{4}\right) < \left(\frac{5}{2}\right). \text{ Done to get us closer} \\ &&& \text{to the goal.} \\ [8] \quad &\geq \left(\frac{3}{2}\right)^2 \left(\frac{3}{2}\right)^{n-3} = \left(\frac{3}{2}\right)^{n-1} \\ &&& = \left(\frac{3}{2}\right)^{(n+1)-2} \end{aligned}$$

So, using the Principle of Strong Induction, we have that, for all $n \geq 1$: $f_n \geq \left(\frac{3}{2}\right)^{n-2}$.

Problems

1 & 2. Prove that, for any integer $n > 1$, n can be written as the product of primes. Let's first check this claim for plausibility. We can observe:

$$2 = 2$$

$$5 = 5$$

$$10 = 2 \cdot 5$$

$$12 = 2 \cdot 2 \cdot 3$$

and so forth

Note that the "product of primes" may have just a single factor (e.g., 2 or 5).

Use strong induction to prove the claim.

Note that, for the induction step: We must prove:

(for any i such that $2 \leq i \leq n$ it is the case that i can be written as the product of primes)

→

($n+1$ can be written as the product of primes)

3 & 4. Define the following sequence:

$$a_0 = 0,$$

$$a_1 = 1,$$

$$\text{For all } n \geq 1, \quad a_{n+1} = 3a_n - 2a_{n-1}$$

The first several terms of the sequence are 0, 1, 3, 7, 15, 31, 63, 127.

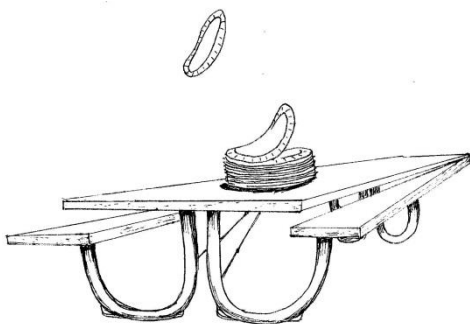
Prove the following claim about the elements of this sequence:

[1] For all $n \geq 0$: $a_n = 2^n - 1$

Induction When the Objects Don't Look Like Numbers

Mathematical induction works when there's the notion of a first thing, a well-defined next thing, and so forth. The domain in which that's the most natural way to look at things is the integers. The base case is typically 0 or 1. Then, for any integer n , the "next" one is its successor, i.e., $n+1$.

But mathematical induction can also be useful in other kinds of domains. Often the reason it's useful is that we can assign integers in some natural way to the objects we've got. For example, maybe they have size or age or position in a stack or list.



Consider the stack of paper plates. Suppose that I want to prove that, no matter how tall the stack, all the plates will fly away. You might come back and say, "Surely not. That stack is way too heavy to be blown away." But, if I can get you to agree that, yes, a single plate can easily be blown away, then I can prove, by induction, that all of them can.

To do this, we need two premises about the plates. (We didn't usually need to add premises when proving things about numbers or about geometry because we assumed all of the ones that we already had.) But now we need two:

- [1] The top plate will blow away.
- [2] When the top plate blows away, the next plate becomes the top one.

Number each plate, starting from the top, with the positive integers. Number the top plate 1.

Claim to be proved: $\forall n$ ($Plate_n$ will blow away)

Base case: $Plate_1$ will blow away. This is so by premise [1].

Induction step: We must prove:

$$\forall n ((Plate_n \text{ will blow away}) \rightarrow (Plate_{n+1} \text{ will blow away}))$$

The proof is straightforward. As soon as $Plate_n$ blows away, $Plate_{n+1}$ becomes the top plate (by premise [2]). But then, by premise [1], it too, will blow away.

So, by the Principle of Mathematical Induction, all plates will blow away.

Nifty Aside

A stack of paper plates is a physical thing. Now imagine a stack or list or set that is represented in a computer. For example, the ordered list of students wanting to sign up for a class that's full. Or the set of employees for whom paychecks need to be issued. Programs that deal with such data structures generally do so by processing one element at a time. But we want to be able to prove that, eventually, all the elements will be correctly processed. To do that, we often use induction proofs that look very similar to the one we just did for the paper plates.

An Everyday Example of Strong Induction

Our last example relied on weak induction. There are also everyday examples that rely on strong induction.

Suppose that we want to argue that parents will love however many children they've got. Let's accept two premises:

- [1] A first child is always loved.
- [2] If you love all the children you've already got, you can always love one more.

Number the children in a family by birth order, starting with 1.

We can use strong induction to prove our claim. In fact, it's very easy to do that since premise [2] is the claim that we usually have to establish in the induction step. So we have:

Base case: ($n = 1$) Premise [1] guarantees that the parents love the first child.

Induction step: Prove that if you already love n children you will love the $(n+1)^{\text{st}}$ one. This is given as premise [2].

So, by Strong Induction, we have that parents love all their children.

Problems

1. Consider the claim that every tissue in the box will eventually be removed.

Let's number the tissues. The top one will be 1, the one below it 2, and so forth. We'll say that a tissue can be removed if part of it sticks up out of the box (as shown in the picture).



We'll start with four premises:

- [1] When the box is opened, the top tissue can be pulled up as shown in the picture.
- [2] The tissues have been folded and put into the box in such a way that, whenever a tissue is removed, the one below it is pulled up as shown in the picture.
- [3] Any tissue that is sticking out of the box, as shown in the picture, can easily be removed.
- [4] Any tissue that can be removed will eventually be removed. (Imagine it's allergy season.)

Define: $P(n) \equiv \text{Tissue}_n \text{ will be removed.}$

We want to prove: $\forall n (P(n))$

Base case: Show that Tissue_1 will be removed. Write your proof.

Induction step: We must prove:

$$\forall n ((\text{Tissue}_n \text{ will be removed}) \rightarrow (\text{Tissue}_{n+1} \text{ will be removed}))$$

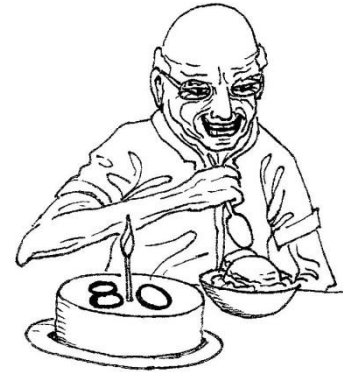
Do it.

2. Suppose that we want to prove that one will like ice cream on one's 80th birthday. Further suppose that we have the following premises:

- [1] One will (of course) like ice cream on one's first birthday.
- [2] If you liked ice cream on your birthday last year, you'll like it this year.

How shall we prove the claim about the octogenarian birthday?

The two premises that we've got suggest that we could perhaps use mathematical induction to prove that one would like ice cream on every birthday. That's not exactly our claim, but it's a stronger generalization of it. If we knew that one likes ice cream on every birthday, then, by Universal Instantiation, we'd have that, in particular, one likes it on the 80th.



By the way, this idea of proving something stronger than what we really need isn't crazy. It's a fairly common strategy. Sometimes a more general (stronger) claim is easier to prove than a more specific (weaker) one.

So let's do the induction proof of the generalization. Number annual birthdays in sequence starting with the first one (the one at the end of year 1 of life).

Define: $P(n) \equiv$ One likes ice cream on one's n^{th} birthday.

We want to prove: $\forall n (P(n))$

Base case: Write your proof.

Induction step: Write your proof. Hint: It's trivial.

Finally, prove the specific claim about 80th birthdays.

3. Recall De Morgan's Laws for Boolean logic:

$$\begin{aligned}\neg(p \wedge q) &\equiv (\neg p \vee \neg q) \\ \neg(p \vee q) &\equiv (\neg p \wedge \neg q)\end{aligned}$$

These two identities let us "push *nots* through *ands* and *ors*". We've made a lot of use of them, both in Boolean logic and in predicate logic.

But, as stated here, they apply only when we want to push a *not* through a single *and* or *or*. What about something like this:

$$\neg(p \wedge q \wedge s \wedge t)$$

(Notice here that we haven't used additional parentheses to indicate associativity of \wedge . We've already proved that $(p \wedge q) \wedge s$ is equal to $p \wedge (q \wedge s)$. In other words, that if there are two instances

of \wedge , the operation is associative. It is possible to generalize that claim to any number of instances of \wedge . In fact the proof is by induction and is similar to the one we're about to do. For now, take it as a theorem that it doesn't matter how we associate the \wedge operations.)

Now back to the problem of dealing with \neg . Can we exploit De Morgan here? The answer is yes. But, using only the version of De Morgan that we've got so far, we'd have to do it one step at a time, starting with this original expression:

$$\neg(((p \wedge q) \wedge s) \wedge t)$$

Could we instead generalize De Morgan to apply to any finite sequence of *ands* or *ors*? The answer to this too is yes. We'd like to have:

$$[1] \quad \text{For } n \geq 2, \neg \wedge_{i=1}^n p_i = \vee_{i=1}^n \neg p_i \quad (\text{pushing } \neg \text{ through } \wedge)$$

$$[2] \quad \text{For } n \geq 2, \neg \vee_{i=1}^n p_i = \wedge_{i=1}^n \neg p_i \quad (\text{pushing } \neg \text{ through } \vee)$$

Read $\wedge_{i=1}^n p_i$ as the *and* of the n variables p_i . Similarly for the large *or*. These two symbols are to \wedge and \vee what Σ is to addition.

Just to be clear about this new notation: $(\wedge_{i=1}^5 p_i) = p_1 \wedge p_2 \wedge p_3 \wedge p_4 \wedge p_5$.

How shall we prove that these generalized De Morgan's laws are valid?

We've just been seeing that, when we want to prove that some property holds of an arbitrary number of items that can be arranged in a reasonable order, induction is a good approach. Let's see if it works here. In particular, we'll use induction on the number of variables p_i .

Use induction to prove [1].

First write an explicit statement of $P(n)$.

Now prove the base case ($n = 2$). (We need n to be at least 2, since we need two operands for a single \wedge .)

Now do the induction step. First, write an explicit statement of exactly what we must prove in this step.

Now write the rest of the induction step

Recursion and Induction

Sometimes the easiest way to define an object is in terms of other (generally smaller) objects just like it. We call such definitions *recursive*.

Recursive definitions generally have a structure that is very similar to the structure of an inductive proof:

- We begin by writing a simple (nonrecursive) definition of a small number of base cases.
- Then we write a general definition, useful for all other values, that constructs values from others that are closer to the base case(s).

We've already seen several recursive definitions. We just didn't call them that.

Recall that we defined the Fibonacci sequence as follows, using two base cases:

$$\begin{array}{lll} f_1 & = 1, & \text{(i.e., the first element of the sequence is 1)} \\ f_2 & = 1, & \text{(and so is the second element)} \\ \text{for all } k > 2, & f_{k+1} & = f_k + f_{k-1} \quad \text{(other elements are computed from the two previous ones)} \end{array}$$

The first several terms of the sequence are 1, 1, 2, 3, 5, 8, 13.

Because recursive definitions and inductive proofs share the same structure, it's often the case that the most straightforward way to prove claims about objects that have been defined recursively is by induction.

Recall that we've already proved the following claim about the Fibonacci sequence:

$$\text{For all } n \geq 1: \quad (\sum_{i=1}^n f_i^2) = f_n f_{n+1}$$

Also, in an optional section we used (strong) induction to prove:

$$\text{For all } n \geq 1: \quad f_n \geq \left(\frac{3}{2}\right)^{n-2}$$

Inductive Proofs of Other Recursively Defined Structures

Induction is a common way to prove claims about recursively defined sequences. But it's also useful in proving claims about other kinds of recursively defined structures. We'll present two examples here. They're interesting. But if you choose to skip them, you can still go on to the next page

Recall our definition of a Boolean well-formed formula (or wff). It was spread out over several pages, but let's summarize it concisely here:

- T and F are wffs.
- Individual variables, like p or R are wffs.
- If w is a wff, so is $\neg w$.
- If x and y are wffs, so are $x \vee y$, $x \wedge y$, $x \rightarrow y$, and $x \equiv y$.
- If w is a wff, so is (w) .
- Nothing else is a wff.

Notice that we have exploited a recursive definition of a wff. It begins with the smallest units. Then it describes all the ways in which those smaller units can be combined to form larger ones.

This recursive definition lets us generate wffs such as:

$$((R \rightarrow S) \vee ((T \vee \neg R) \wedge \neg(Y \rightarrow S))) \wedge X$$

In any wff that we can build, the parentheses will be balanced (i.e, the number of '('s equals the number of ')'s and they will be properly nested. (You can see an example of proper nesting in the wff above. We've nested smaller pairs inside larger ones.)

We can use induction to prove that all wffs will have properly nested parentheses.

Define the **length** of a wff w to be the number of symbols it contains (blanks don't count). We'll write the length of w as:

$$|w|$$

We'll count symbols as follows:

- T and F are each symbols.
- Each individual variable is a symbol (even if we give it a multi-character name like RAIN).
- \neg , \vee , \wedge , \rightarrow , \equiv , $($, and $)$ are each symbols.

So, for example, $|((R \rightarrow S) \vee ((T \vee \neg R) \wedge \neg(Y \rightarrow S))) \wedge X| = 25$.

We'll prove our claim by strong induction on $|w|$.

Define: $P(n) \equiv$ "Every wff of length n has balanced parentheses."

Base cases: $P(1)$ is true, trivially; the shortest wff that contains parentheses has length 3.
 $P(2)$ is true. The only wffs of length two have the form $\neg T$, $\neg F$, or $\neg p$, for some variable p . Thus no parentheses.

Induction step: We must prove that, for $n \geq 2$, if all wffs of length n or less have balanced parentheses, then so do all wffs of length $n + 1$. So we must prove:

$$(\text{For all } 1 \leq i \leq n, P(i)) \rightarrow P(n + 1)$$

We can use Case Enumeration to help us here.

Consider any wff w of length $n + 1$, where $n \geq 2$:

- Suppose w has the form (s) , for some wff s . Then $|s| = |w| - 2$. By the induction hypothesis, s has balanced parentheses. So w does too, since a matched pair has been added around an expression that already has balanced parentheses.
- Suppose w has the form $\neg s$ for some wff s . Then $|s| = |w| - 1$. By the induction hypothesis, s has balanced parentheses. So w does too, since none have been added or removed.
- Suppose w has the form $x \vee y$, $x \wedge y$, $x \rightarrow y$, or $x \equiv y$. Then both $|x|$ and $|y|$ must be less than $|w|$. By the induction hypothesis, both x and y have balanced parentheses. So w does too, since none have been added or removed.

We'll define a **language** to be a collection of strings. There are various ways to describe particular languages that we might wish to reason about. We'll present one very useful such technique here.

A **grammar** is a special initial string, plus a set of rules for transforming one string into another. The job of a grammar is to define a language, so we'll say that a grammar G **generates** some language L . Define a useful notation:

$L(G)$ is the language that grammar G generates.

A grammar will exploit two kinds of symbols:

- Working symbols: These will be used by a grammar, G , but must be removed before we can claim that G has generated some string in $L(G)$.
- Terminal symbols: These are the symbols that can occur in strings in $L(G)$.

And we need one more notation. We need a way to write the empty string, i.e., the string that contains no characters. It's hard to print nothing. So we will use the special symbol:

ϵ (read "epsilon") stands for the empty string

Each rule in G has two parts, a left-hand side, which you can think of as a pattern, and a right-hand side, which is a string that will be substituted for the matched pattern whenever the rule is applied. So, for example, consider this simple rule:

$$S \rightarrow a T a$$

The left-hand side of this rule is S . If this rule is applied, then some S that matched will be chopped out and replaced with the rule's right-hand side ($a T a$).

G 's job is to start with its initial string and apply rules to derive strings in $L(G)$. At each step, it may choose to apply any rule whose left hand side matches the string it has derived so far. To actually apply the rule, it chops out the string that matched the rule's left hand side and replaces it with the rule's right hand side. We call a sequence of steps such as this a **derivation**.

Consider the grammar G that has starting string S and the following rules:

$$\begin{array}{ll} [1] & S \rightarrow a S a \\ [2] & S \rightarrow b S b \\ [3] & S \rightarrow \varepsilon \end{array}$$

S is a working symbol and both a and b are terminal symbols.

Let's watch G in action. We'll use the symbol \Rightarrow to indicate one step in a derivation (the process of applying G 's rules). In this example, we'll apply rule [2] twice, then rule [1], then rule [3]. At each step, we've underlined the string that matches and then gets removed. Ignore blanks. They're just here to make the example easier to read.

$$\underline{S} \Rightarrow b \underline{S} b \Rightarrow bb \underline{S} bb \Rightarrow bba \underline{S} abb \Rightarrow bbaabb$$

So we can say that $bbaabb$ is in the language $L(G)$.

We have just given a definition of the language $L(G)$. It's all and only the strings that G can generate. Notice that this definition is recursive. We define the simplest strings that G can generate and we have a way to build larger ones from those.

Given this recursive definition, we might expect that we could prove things about $L(G)$, using induction. And we can.

We'll leave as an exercise the proof that, given our example grammar G , every string in $L(G)$ has even length.

Problems

1. Let's return to the grammar G with starting string S and these rules:

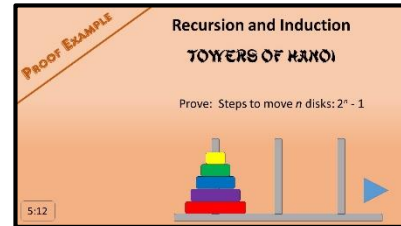
$$\begin{array}{ll} [1] & S \rightarrow a S a \\ [2] & S \rightarrow b S b \\ [3] & S \rightarrow \varepsilon \end{array}$$

Prove by induction on the length of the generated strings that every string in $L(G)$ has even length.

Inductive Proofs of Recursive Programs – The Towers of Hanoi

There's yet another reason that inductive proofs are so important, particularly to people who write code: When we write programs to solve problems that themselves have a natural recursive structure, the most straightforward way to reason about those programs is by induction.

<https://www.youtube.com/watch?v=SMleU0oeGLg>



Recall the Towers of Hanoi problem:



To solve this problem requires that we move all the disks from the starting pole to one of the other poles. But we must do that by following a few rules: Whenever a disk is removed from a pole, it must immediately be placed on some other pole. No disks may be placed on the ground or held. Further, a disk may never be placed on top of a smaller disk.

In some descriptions of this problem, we fix the number of disks, often at 64. But let's consider what we'll call the Generalized Towers of Hanoi problem: Find a way to do the job with any number of disks on the poles.

Recall that we proposed the following algorithm for solving this problem:

towersofHanoi(*n*: positive integer) =

1. If $n = 1$ then move the disk to the goal pole.
2. Else:
 - 2.1. Use *towersofHanoi*($n-1$) to move the top $n-1$ disks to the pole that is neither the current one nor the goal.
 - 2.2. Move the bottom disk to the goal pole.
 - 2.3. Use *towersofHanoi*($n-1$) to move the $n-1$ disks that were just set aside to the goal pole.

Summarizing in English what this procedure does: To move n disks, first move $n-1$ of them out of the way to the third pole. Next, move the bottom disk into place on the goal pole. Finally, move the remaining $n-1$ disks from their temporary location to the goal pole.

This algorithm is recursive: To move n disks, we first move a smaller number ($n-1$) of them out of the way. Of course to do that, we must start by moving ($n-2$) of them out of the way. And so forth.

And notice that, just as in an inductive proof, there is a base case that must be treated specially. In this case: to move exactly one disk, just move it.

Now consider the following claim about this problem and the program we have just written to solve it:

For any number of disks, n , it is possible to solve the problem in $2^n - 1$ moves.

Notice that we're not claiming that it's not possible to do better (although it is possible to prove that). We are claiming, though, that the problem isn't worse than this.

Our argument that it is possible to solve the problem in $2^n - 1$ moves is going to be that the program we've just presented does so in exactly that number of moves.

Let's prove the correctness of this claim about the computational complexity of our program.

The proof is by induction on n , the number of disks.

Call the number of moves required for n disks $M(n)$. Then:

$$P(n) \equiv M(n) = 2^n - 1 \text{ moves.}''$$

Base case: $n = 1$. Our program requires exactly one move when there is one disk. So:

$$M(1) = 1 = 2^1 - 1 = 2^n - 1.$$

Induction step: Assuming $P(n)$, prove $P(n+1)$. Analyzing the program, we see that $M(n+1)$ (the total number of moves required to move $n+1$ disks), for $n+1 > 1$, is:

$$M(n+1) = M(n) + 1 + M(n)$$

By the induction hypothesis, we have that $M(n) = 2^n - 1$. So we can rewrite this as:

$$\begin{aligned} M(n+1) &= (2^n - 1) + 1 + (2^n - 1) &= 2 \cdot (2^n - 1) + 1 \\ & &= 2^{n+1} - 1 \end{aligned}$$

Faulty Induction Proofs

Induction is subtle. When used as defined, it is sound. It cannot prove something that is false.

However, and this is a big however, it is easy to use it incorrectly. We must be careful.

Consider the claim that all M&Ms are the same color.

We'll "prove" this claim by induction. Define:

$P(n) \equiv$ "In an arbitrary set of n M&Ms, all candies are the same color."



Base case: For $n = 1$, there is only one M&M, which must be the same color as itself.

Induction step: We must prove:

(In an arbitrary set of n M&Ms, all candies are the same color)

→

(In an arbitrary set of $n+1$ M&Ms, all candies are the same color)

Suppose that we have $n+1$ candies. Remove one. We now have a set of n candies. By the induction hypothesis, they are all the same color.

Now place the removed candy back in the pile and remove a different one. Again we have a set of n candies and they are all the same color.

And they are the same color as the newly removed one since we already have that it shared the pile's color before it was removed. Thus all $n+1$ candies are the same color. Q.E.D.

If we had stopped to do a plausibility check before trying to write a proof, we might not even have tried. But we did try. And we got this. It looks like a proof. But it can't be. It's demonstrably ridiculous to claim that all M&Ms are the same color. We know, in fact, that they keep adding new colors. So what is wrong? See if you can figure it out.

Problems

1. Consider the following claim:

For any integer $n \geq 0$, $2n = 0$.

What is wrong with the following inductive proof of this claim?

The proof is by strong induction. Define:

$$P(n) \equiv (2n = 0)$$

Base case: $P(0)$ is true since $2 \cdot 0 = 0$.

Induction step: Assume P is true for all nonnegative integers $\leq n$. We show that it must also be true of $n + 1$. We can rewrite $n + 1$ as the sum of two smaller numbers, i and j . Specifically, there must exist integers i and j such that $n + 1 = i + j$ and $0 \leq i, j < n + 1$. (For example, if $n + 1 = 5$, then we could rewrite it as $2 + 3$.) So we have:

$$\begin{aligned} n + 1 &= i + j \\ 2(n + 1) &= 2(i + j) \\ &= 2i + 2j \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

Induction hypothesis

2. Let's consider another postage stamp problem. This time assume that there are 3¢ and 4¢ stamps.

Consider the claim that it is possible to form any amount of postage of at least 3¢ using only 3¢ and 4¢ stamps. What is wrong with the following inductive proof of this claim?

The proof is by strong induction. Define:

$P(n) \equiv$ "It is possible to form n ¢ using just 3¢ and 4¢ stamps.

Base cases: It is possible to form 3¢ using just a single 3¢ stamp.
It is possible to form 4¢ using just a single 4¢ stamp.

Induction step: We assume that it is possible to form all amounts up to n ¢ with 3¢ and 4¢ stamps. We must now show that it is possible to form $(n + 1)$ ¢. This can easily be done by either replacing one 3¢ stamp with a 4¢ one or by replacing two 4¢ stamps (totaling 8¢) with three 3¢ stamps (totaling 9¢).



Stronger and Weaker Claims

Proving a Stronger Claim

Sometimes the easiest way to prove a claim is to prove a stronger one.

Consider the claim:

for $n \geq 0$, ($\neg \text{Prime}(3^n + 1)$).

If we examine its truth for several values of n , we observe that, for all n , $(3^n + 1)$ is more than just not prime. It is always divisible by 2 (i.e., it is even). It's quite easy to prove this more general claim. So let's do it. Notice, as we do so, that in our proof of the stronger claim we get to exploit a stronger induction hypothesis.

Prove: for $n \geq 0$, $(3^n + 1)$ is even).

The proof is by induction on n .

Base case: $n = 0$: $3^0 + 1 = 2$.

Induction step: The induction hypothesis is that $3^n + 1$ is even and thus is equal to $2k$ for some integer k .

$$\begin{aligned} 3^{n+1} + 1 &= 3(3^n) + 1 \\ &= 3(3^n + 1) - 2 \\ &= 3(2k) - 2 && \text{For some integer } k. \text{ Induction hypothesis} \\ &= 2(3k - 1) \end{aligned}$$

So $3^{n+1} + 1$ is divisible by 2 (so it's even).

Guards

Sometimes, we'd like to prove some very general claim, say something of the form:

$$[1] \quad \forall x (P(x))$$

But when we try to prove [1], we find that we're stuck unless we can make one or more additional assumptions.

When this happens, what we'd like to do is simply to add those assumptions. We can't of course just do that and still claim to have a proof of [1]. What we can do is to add the assumptions, push through the proof, and then use the Conditionalization rule, thus enabling us to prove something of the form:

$$[2] \quad \forall x ((Q(x) \wedge R(x)) \rightarrow P(x))$$

Recall that, in implications such as [2], we've called expressions like $(Q(x) \wedge R(x))$ **guards**: they restrict the circumstances under which we can conclude $P(x)$. Of course, we'd rather not be restricted. But restricted is better than nothing.

As a very simple example, let's return to our initial <ex>Who Drives Me</ex> problem. We don't even need quantifiers.

J: John must drive me to the store.
M: Mary must drive me to the store.
L: John will be late for work.

Using those statements, we will state the two premises that we will assume:

[1] $J \vee M$ John or Mary must drive me to the store.
[2] $J \rightarrow L$ If John drives me to the store, he will be late for work.

The conclusion that we'd like to draw is:

M Mary must drive me to the store.

We can begin the proof as follows:

[1] $J \vee M$ Premise
[2] $J \rightarrow L$ Premise
[3] $\neg L \rightarrow \neg J$ Contrapositive [2]

Now we're stuck. If we knew $\neg L$, we could conclude $\neg J$. Then, using [1], we could conclude M . So we need to exploit the Conditionalization rule. We'll assume $\neg L$ and see what we can do:

[4]		$\neg L$	(Conditional) Premise	
[5]		$\neg J$	Modus Ponens	[3], [4]
[6]		M	Disjunctive Syllogism	[1], [5]
[7]		$\neg L \rightarrow M$	Conditionalization Discharge	[4], [6]

We can't prove the (comparatively) strong claim that Mary must drive me. We can prove that if it's true that John can't be late, then Mary must drive. So we now know what we'd have to prove if we wanted to convince Mary to get in the car.

We just saw that introducing guards can be useful in everyday reasoning. It is also very often useful in mathematics.

Assume an x-y plane. Let L be any line in the plane. Prove that there is a point on L whose y coordinate is positive and one whose y coordinate is negative.

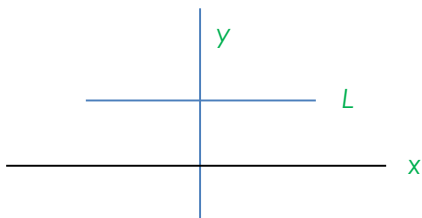
Let's first use case enumeration and consider two cases:

- 1) L is vertical. In this case, since it extends infinitely in both directions, it must have both positive and negative values of y .
- 2) L isn't vertical. In this case, it can be described as:

$$y = ax + b, \text{ where } a \text{ is the slope and } b \text{ is the y-intercept.}$$

We need to show that, for any line (i.e., for any values of a and b), the required points exist.

Let's first think about whether our claim is in fact true for all non-vertical lines. What about:



What we see is that if L has a slope of 0 (i.e., L is horizontal and its equation is $y = b$) our claim is false. So let's add a guard. Our new problem is:

Let L be any line *with slope $\neq 0$* . Prove that there is a point on L whose y coordinate is positive and one whose y coordinate is negative. We still have a proof that the claim is true for vertical lines. Let's now do the rest.

Let's try to do a proof by construction. (This means that we'll not just prove that the required points exist. We'll actually know what they are.) Compute the two points as follows:

$$\text{Let } x_1 = \frac{1}{a} \cdot 2 \cdot |b|$$

$$\text{So } y_1 = ax_1 + b = a \cdot \left(\frac{1}{a} \cdot 2 \cdot |b|\right) + b = 2 \cdot |b| + b$$

$$\text{Let } x_2 = \frac{-1}{a} \cdot 2 \cdot |b|$$

$$\text{So } y_2 = ax_2 + b = -a \cdot \left(\frac{1}{a} \cdot 2 \cdot |b|\right) + b = -2 \cdot |b| + b$$

Do these two points meet our requirements? They do as long as $b \neq 0$. Then $2 \cdot |b|$ is positive and larger than b . So, even if b is negative, $2 \cdot |b| + b$ is positive. Similarly, $-2 \cdot |b|$ is negative and larger in absolute value than b . So, even if b is positive, $-2 \cdot |b| + b$ is negative.

But what about the case in which $b = 0$? Then both (x_1, y_1) and (x_2, y_2) are in fact $(0, 0)$. But, if $b = 0$, these two points meet our requirements:

$$\begin{aligned} \text{Let } x_1 &= 1 \\ \text{Let } x_2 &= -1 \end{aligned}$$

$$\begin{aligned} \text{So } y_1 &= a \\ \text{So } y_2 &= -a \end{aligned}$$

Since we've already restricted a to be nonzero, one of those values must be positive and one must be negative.

Let's review the structure of this proof:

- We used case enumeration to separate two cases. We handled vertical lines as a special case and then went on to consider all non-vertical lines.
- Then we realized that horizontal lines posed a more serious problem. Our claim isn't true of them. So we added a guard and then went on to prove a more restricted claim.
- Then we used proof by construction to show how to find the required points given some arbitrary line L .
- But, again, we realized that there was a special case ($b = 0$) for which a separate construction was required.

This proof is interesting because of the way that it combines all of these proof techniques into a single proof.

Sometimes, when we have to introduce guards, we end up with a claim that's the best we're going to be able to do. Ever. For example, if we must restrict a numerical value to be nonzero, that's that. No amount of additional information will let us clear such guards.

But sometimes, when we have to introduce guards, we end up with a claim that might be strengthenable. In other words, maybe if we did some more research, we'd find out that the guard is, in fact, always satisfied. Then we can add it as a real premise and remove it as a guard.

Recall the **Eradicate Ucklufery** example. We gave names to the following statements:

V Ucklufery (a very nasty tropical disease) is caused by a virus.

E : We might be able to eradicate ucklufery by developing a vaccine against it.

When we started this example, we assumed the following fact:

[1] $V \rightarrow E$ If ucklufery is caused by a virus, we might be able to eradicate it by developing a vaccine against it.

In other words, we were forced to introduce the guard, $V \rightarrow$. But we realized that if we could do research and discover that, in fact, ucklufery is caused by a virus, then we'd be able to release the guard and assert the stronger claim:

[2] E Now we know that we should search for a vaccine.

When we're working in the real world, examples like this arise often. When they do, they can help direct future research in useful directions.

While perhaps rarer in mathematics (where no amount of additional research will get us to a point where we can divide by zero, for example), cases where we can do research to try to remove guards do arise.

Problems

1. Let the domain be the real numbers. Try to prove: $\forall x (x^2 > 0)$.

If this claim isn't true, add the weakest guard that makes it true.

2. Let the domain be the real numbers. Try to prove: $\forall x (x^2 > x)$.

If this claim isn't true, add the weakest guard that makes it true.

3. Recall that, for any positive integer n , $n!$ (read, " n factorial") is $n \cdot (n - 1) \cdot (n - 2) \dots \cdot 1$.

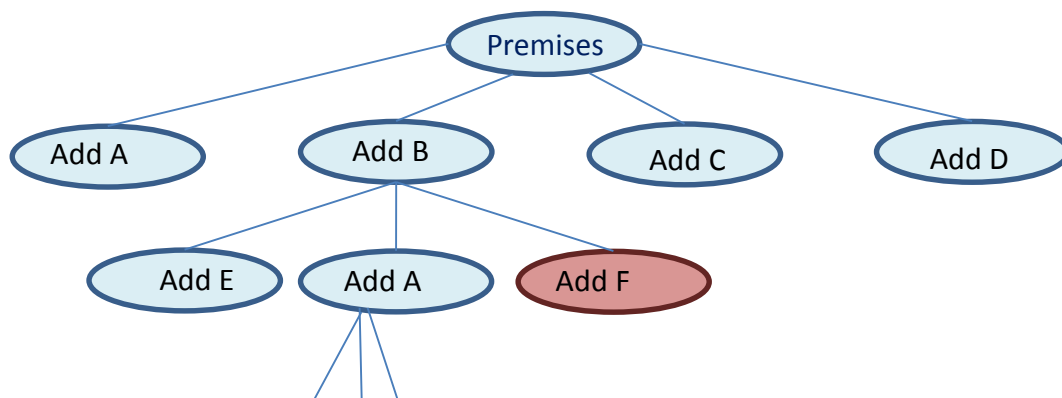
Try to prove: $\forall x (Even(x!))$.

If this claim isn't true, add the weakest guard that makes it true.

Strategies for Discovering Proofs

We have just presented a collection of major strategies for designing proofs. Suppose that you have a nontrivial statement that you'd like to prove. How should you go about choosing one or more of these strategies? Then let's say you've picked one (or more). For example, suppose you plan to write a forward, direct proof. You still have a lot of decisions left to make. What premises should you use? What key inference rules should you use? In what order? In nontrivial domains, you'll find yourself searching in a very large space of possible proofs, hoping to find one that leads to the conclusion that you seek.

Here's a picture that may help you understand the problem.



Read the picture as follows: Assume that you start your proof with a set of premises (some or all of which may be relevant). So you start in the state that corresponds to the top oval. The premises are what you know. Each time you write a non-premise line in your proof, you add a new statement that you know to be true. So you move to a new state in which you know everything you used to know, plus something new. Each line in the picture corresponds to one application of a sound inference rule or identity. Your goal is to arrive at a state (represented as an oval) in which your desired conclusion has become one of the things that you know. If, say, your desired conclusion were F, then the oval shown in red would correspond to a goal state.

Your problem may now be obvious. There may be a lot of branches coming out of the state you're currently in. How do you know which of them will take you to your desired conclusion? You don't want to waste time on paths that don't lead to your goal.

So what's a budding proof engineer to do?

The answer is that you need to develop for yourself a set of rules of thumb that will guide you in the direction of effective proofs.

We call these rules of thumb *heuristics*. Think of a heuristic not as an algorithm that is guaranteed to lead you immediately to the right answer. Rather, it's a technique that (substantially, we hope) beats blind search most of the time.

Nifty Aside

The word "heuristic" comes from the same Greek word as "Eureka", the exclamation that Archimedes is reputed to have uttered when, while sitting in the bath tub, he realized that he could compute the amount of gold in the king's crown by measuring its displacement in water. The Greek root word means "to find".



The heuristics that you'll develop will typically look like pattern/action rules. Think of them as being written as:

$$A \Rightarrow B$$

This rule says that if your problem looks like A, do B.

Here's a table with some simple rules:

Problem Characteristics	Proof Technique to Try
Straightforward application of logical or algebraic rules may work.	Direct proof.
I'm trying to prove something about a sequence.	Inductive proof.
I tried direct proof and got stuck.	Proof by contradiction.
I'm trying to prove a claim of the form: $\exists y (...)$	Proof by example.
I'm trying to prove a claim of the form: $\forall x (\exists y (...))$	Proof by construction.
I'm trying to prove a claim of the form: $\neg \forall x (...)$	Proof by counterexample
I can't find a good general proof but a manageable number of cases covers everything	Case Enumeration

And then, once you've chosen your overall approach, you'll have to exploit similar pattern/action rules that are specific to the technique that you're using.

At this point, you're probably saying something like, "Bring them on. Tell me exactly how I'll know what to do next at each step of my proof." Unfortunately, we don't know how to do that. Every situation is different. Writing a proof is like designing anything else. We will attempt to give you some good advice. But the best way to get good at writing proofs is to practice. If you do that, you'll acquire rules that work.

Nifty Aside

It's so hard that powerful automatic theorem provers are often interactive so human experts can guide them when necessary. Several such interactive provers are being developed today. Visit http://en.wikipedia.org/wiki/Proof_assistant for more about them.

In the next set of problems, you will need to figure out which technique(s) to use to complete the required proofs.

Problems

1. Define the following predicates:

$USP(x)$: True if x was a President of the United States.
 $M(x, y)$: True if x and y have ever been married to each other.

Prove or disprove the claim that every US President has been married. We can state the claim as:

$$[1] \quad \forall x (USP(x) \rightarrow \exists y (M(x, y)))$$

2. Prove or disprove the following claim. (Recall that $|x|$, read as “absolute value of x ”, is simply x if x is nonnegative. It is $-x$ otherwise. For any x , $|x|$ is thus nonnegative.)

$$[1] \quad \text{For any reals } x \text{ and } y, |xy| = |x| \cdot |y|$$

3. Assume the universe of positive integers. Prove or disprove the following claim:

$$[1] \quad \forall n (Prime(n^2 + 4n + 3))$$

4. Prove or disprove the following claim:

$$[1] \quad \text{For all } x \geq 1 \text{ and } k \geq 1, (x + k)^2 > x^2 + k^2$$

5. Prove or disprove the following claim:

$$[1] \quad \text{For any nonnegative integer } n, (\sum_{i=0}^n i^3) = \frac{n^2(n+1)^2}{4}.$$

Empirical Induction

Induction from Observations

If we prove by mathematical induction that the sum of the first n positive integers is $\frac{n(n+1)}{2}$, it must be so. No exceptions. It's over.

But now let's look at the real world and consider another reasoning strategy that is typically also called induction. To avoid confusion, we'll call it *empirical induction*. When most people, in nonmathematical contexts, use the term "induction", what they mean is empirical induction.

In empirical induction, we examine a large and representative set of examples. If we observe a consistent pattern, we generalize and conclude that the pattern will always occur. In other words, we assert something of the form:

$$\forall x (P(x))$$

Unlike mathematical induction, empirical deduction isn't sound. It can derive conclusions that are false.



For example, we could wander through zoo after zoo and finally conclude that all peacocks have colored feathers. This conclusion is false. But note that a related conclusion, namely that most peacocks have colored feathers, is in fact true.

If we reason, by empirical deduction, that people seem to get mad if you lie to them, it's nevertheless possible that we could lie and a particular person won't get mad.

But, since we need to act, this sure beats saying "I don't know."

Nifty Aside

Dante Alighieri (1265 - 1321) described what would happen in eternity to those who couldn't make up their minds: They would run around the vestibule of the Inferno (Hell).



Problems

1. Assuming observations that can reasonably be made, indicate, for each of these claims, what role empirical induction could play in attempting to determine the truth of the claim:

(Part 1) Larger cars weigh more than smaller ones.

- a) Empirical induction would be a good way to tackle the problem and will likely support the claim.
- b) In the process of trying empirical induction we would almost certainly find a counterexample that would refute the claim.
- c) Empirical induction isn't likely to tell us much about the claim.

(Part 2) $\sqrt{2809} = 53$.

- a) Empirical induction would be a good way to tackle the problem and will likely support the claim.
- b) In the process of trying empirical induction we would almost certainly find a counterexample that would refute the claim.
- c) Empirical induction isn't applicable to this problem.

(Part 3) Rain comes to Austin on prime numbered days. (So it rains on the 2nd, 3rd, 5th, etc. of every month.)

- a) Empirical induction would be a good way to tackle the problem and will likely support the claim.
- b) In the process of trying empirical induction we would almost certainly find a counterexample that would refute the claim.
- c) Empirical induction isn't applicable to this problem.

Empirical Induction Leads the Way

Empirical induction often gives us a sensible basis for deciding how to act given the knowledge that we have at the moment.

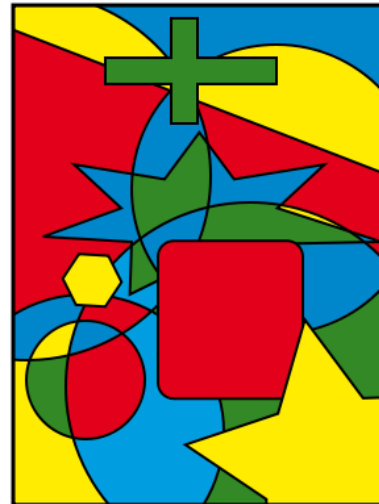
But it does something else too: it can point us in a sensible direction. We can then look for a more robust way to prove claims that we think are very likely to be true.

Consider the **Four Color Problem**: Divide a plane (a flat surface) into contiguous regions. This can be done with straight lines or with curves. Call the resulting structure a map. Is it possible to color all of the regions of the map in such a way that no two regions that share a boundary (a single point doesn't count) are colored in the same way?

In the mid-nineteenth century it was conjectured that the answer to this question was yes. A lot of people spent a lot of time looking at a lot of maps, trying to find ones for which four colors were not enough. No luck.

Empirical induction thus suggested the truth of what is now known as the **Four Color Theorem**: Four colors suffice to color any planar map.

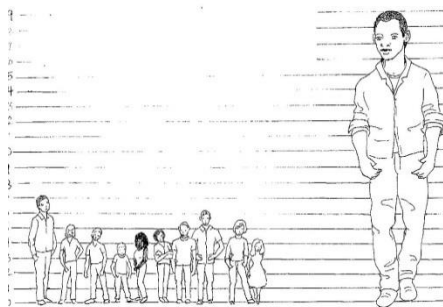
But many failures by many people do not a proof make. So the search was on. And, in 1976, a proof was found. By the way, that proof is significant for anyone interested in computation. It was a computer-assisted proof that checked 1,936 cases.



Empirical induction can be risky though and we must use it carefully. To see how hard it can be even to know what constitutes supporting evidence, consider this example:

Suppose that we want to argue the truth of the claim:

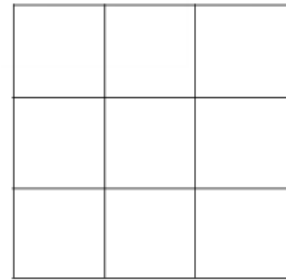
All people are less than 20 feet tall



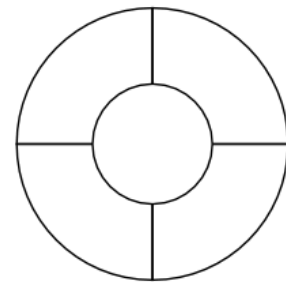
Suppose that we've looked at thousands of people and the tallest one has been under 9 feet tall. We may be ready to assert that we believe the claim. We haven't found anyone even close to 20 feet tall. But suppose that we look just a little farther. And we find a 19 foot tall man. Officially, we've found another person who substantiates our claim. But, perhaps counterintuitively, most of us, on seeing this example, would think the claim less, rather than more likely to be true. Why? Because now, apparently, people can get at least close to the 20 foot mark.

Problems

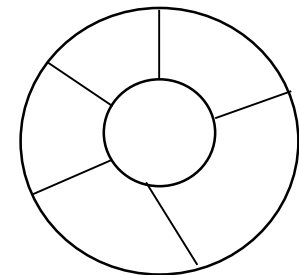
1. How many colors are required to color this map (according to the rules of the Four Color Problem)?



2. How many colors are required to color this map (according to the rules of the Four Color Problem)?



3. How many colors are required to color this map (according to the rules of the Four Color Problem)?



4. Finding a proof or a counterexample for the Four Color Theorem was an open problem in mathematics for a long time. It isn't any more.

But there are still other open problems. Here's one. It has various names. We'll call it the ***3n+1 Problem***.

Given any integer n , do the following until $n = 1$:

- If n is even divide it by 2.
- If n is odd, multiply it by 3 and add 1.

Now consider this question: Will the procedure given above always halt? In other words, regardless of the original value of n , must it eventually become 1?

(Part 1) Try it yourself. Suppose that $n = 6$. Counting both 6 and 1, how many values are computed before the procedure stops?

(Part 2) Now try it with 16. How many values (including 16 and 1) are computed?

Nifty Aside

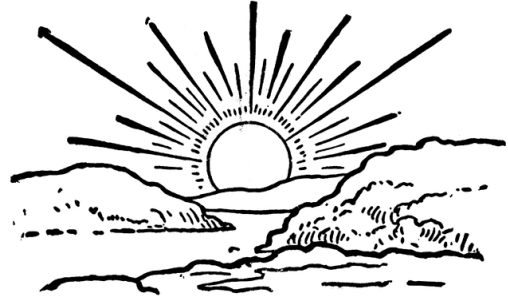
By the way, it is generally thought that this process does always halt by producing the value 1. The claim that it does so is called the ***Collatz Conjecture***. No proof of it has yet been found. On the other hand, the search for a counterexample that would prove it false has also (so far) failed. If you want to try your hand at that search, go to:

<http://www.nitrxgen.net/collatz.php>

Statistical and Probabilistic Truth

When we talk about empirical induction, we generally want to say things like:

- It's likely that there are no 20 foot tall people.
- I'm more sure, after seeing another 3000 peacocks, that all peacocks have colored feathers.
- It's nearly certain that the sun will come up tomorrow. It always has.



The theory of probability gives us powerful tools for reasoning with statements of this sort. Unfortunately we can't explore them here, but you can and should some time.

Everyday Reasoning

Why It's Hard


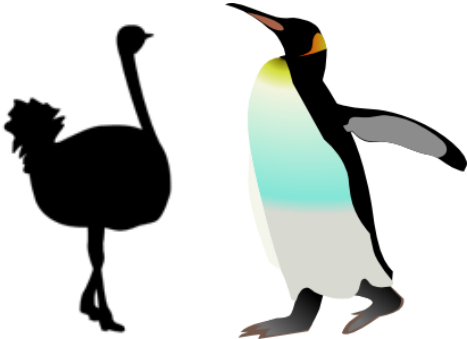
In everyday reasoning, we use all of the techniques that we've been discussing. But it turns out that the real world is complex and our understanding of it is incomplete.

Consider the claim:

$$\forall x (\text{Bird}(x) \rightarrow \text{CanFly}(x))$$

This seems straightforward enough. But, of course, it's false.

Consider these:



Ostriches don't fly and neither do penguins. And neither do baby birds or ones with clipped wings or ones with crude oil all over their wings.

In fact, there are very few universal claims that are true in the real world.

And there are other problems. Even coming up with predicates that capture everything we might like to be able to say and think about is hard. For example, a lot of real world concepts are squishy around the edges.

Consider the predicate *CanFly* that we've mentioned above. Do chickens fly? They can do something that is a little more powerful than "jump". But they can't fly across town the way other birds do. If x is a chicken, should we assert $\text{CanFly}(x)$?

Despite these problems, the sorts of logical reasoning that we've been studying are powerful tools in the real world. We can still use the argument structures that we've defined. And there are additional formal theories that can be used to solve some of the problems that we have with the straightforward theory that we've got.

Problems

1. Let's return to this version of *Who Drives Me*. Here are the premises:

- | | | |
|-----|-------------------|--|
| [1] | $J \vee M$ | John or Mary must drive me to the store. |
| [2] | $J \rightarrow L$ | If John drives me to the store, he will be late for work. |
| [3] | $\neg L$ | John cannot be late for work. |
| [4] | $M \rightarrow G$ | If Mary must drive me to the store, she must buy gas. |
| [5] | $G \rightarrow Y$ | If Mary must buy gas, she must have money. |
| [6] | $Y \rightarrow W$ | If Mary must have money, then she must work at a paying job. |

(Part 1) Focus on premise [5]. How have we simplified the world here? Are there other ways Mary could buy gas?

(Part 2) Focus on premise [6]. How have we simplified the world here? Are there other ways Mary could get money?

When We Get to Declare What's True

When our goal is to **describe** the natural world, it's hard to write logical statements that are true without exception.

However, if our goal is to **prescribe** the world (i.e., declare how it must be), then the logical tools that we've been describing may work in the same straightforward way in which they work for mathematics. This is why, throughout this course, we've often used examples of database integrity constraints. There we state rules that we insist must be true of data entered into our system.

Sometimes we write rules that just prevent data entry errors.

Suppose that we have a database that contains records for all the contracts that our company has ever had. Our company was founded in 1875. Each record has at least these two fields: *startyear* and *endyear*. We might have these rules (where the domain of *r* is the collection of records in the database):

$$\begin{aligned}\forall r (\textit{startyear}(r) \geq 1875) \\ \forall r (\textit{endyear}(r) \geq 1875)\end{aligned}$$

We can assert that these claims are true without exception. If someone tries to enter a record that violates these claims, they'll get an error message and have to fix what we assume was a data entry error.

We can also write rules that correspond to our business practices. These rules tell our employees what they must do in order to maintain the truth of the rules. We've already seen several examples of rules like this.

Here are some examples:

$$\begin{aligned}\forall x (\textit{Employee}(x) \rightarrow \exists y (\textit{EmergencyContact}(y, x))) \\ \forall x (\textit{Employee}(x) \rightarrow \exists y (\textit{CurrentProjectOf}(y, x))) \\ \forall x (\forall y (\forall z (\forall t (((\textit{Employee}(x) \wedge \textit{CurrentProjectOf}(y, x) \wedge \textit{CurrentProjectOf}(z, x) \\ \wedge \textit{CurrentProjectOf}(t, x) \rightarrow ((y = z) \vee (y = t) \vee (z = t))))))) \\ \forall x, y ((\neg \textit{Super}(x) \wedge \textit{Timecard}(y)) \rightarrow \neg \textit{CanSign}(x, y))\end{aligned}$$

And of course, rule-writing isn't limited to businesses.

Recall our rule that said that everyone may board the bus once everyone has arrived:

$$(\forall x (\textit{HasArrived}(x))) \rightarrow \forall y (\textit{MayBoardBus}(y))$$

Appendix

The Daisy Petal Game

First let's think about whether you want to move first or second. You want to move second. One reason that this seems likely to be the right answer is that if both players are going to get the same number of moves, you want to move last (thus taking the last petal). That's of course not a proof that moving second is the correct thing to do. We'll get to that. But here's another way to think of it: Before anyone moves, you have the possibility of winning (i.e., there are still petals for you to remove.) If you let your opponent move first, you get to choose your response in such a way as to preserve that possibility. (We'll soon see how to do that.)

Now let's look at a couple of small cases:

Imagine that the petals are numbered 1 – 4:

- a. If your opponent moves first and takes petal 1, what should you do?
- b. If your opponent moves first and takes petals 1 and 2, what should you do?

If opponent takes just 1, you should take 3. Then opponent must take one of the remaining petals and you can take the other. Opponent cannot take 2 because there aren't 2 adjacent ones to take: you split them up. If opponent takes 2, you take the remaining 2 and win.

Now suppose that there are initially 6 petals, numbered 1 – 6:

- a. If your opponent moves first and takes petal 1, what should you do?
- b. If your opponent moves first and takes petals 1 and 2, what should you do?

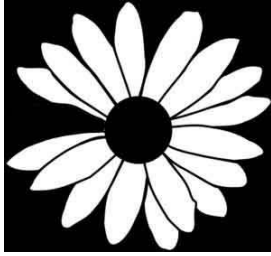
If opponent takes just 1, you should take 4. Again you've taken the same number and you've taken the one directly opposite the one that got taken first. If opponent takes 2, you should take 4 and 5.

Now let's solve the general case:

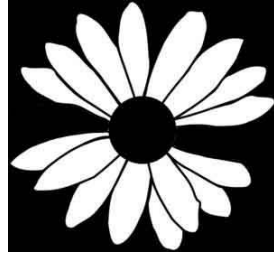
There is a winning strategy for the player who plays second. The idea is to preserve the following invariant:

There is a move that can be made (i.e. it's not true that all petals have already been removed). You lose only if there is no move that you can make, so if this claim is always true when it's your turn, you cannot lose.

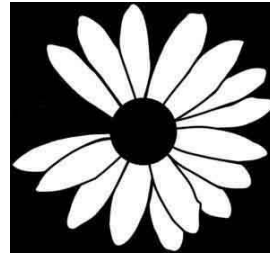
Specifically, one such move is to mirror the opponent's last move by removing the same number of petals and, more specifically, those that are exactly opposite the ones the opponent just took. (By opposite we mean the petals that you get by following a straight line from the opponent's petals through the middle of the flower.) The following pictures illustrate the idea. If your opponent moves as in (A), you should move as in (B). If your opponent takes two petals, as in (C), you should also take two, as in (D).



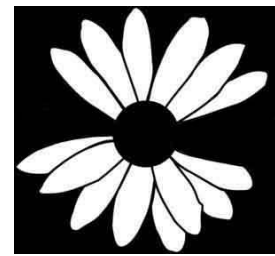
(A)



(B)



(C)



(D)

What about the claim that the invariant always holds for the second player (in, other words, player 2 hasn't lost yet)? Must it be true? It is true right after the first time that player 1 moves since the number of initial petals is even (and thus there are opposite petals). And it can be maintained by player 2 throughout the game. Since after each of player 1's moves, player 2 takes the opposite petal(s), player 1 is forced next to take other petal(s) whose opposite(s) are still available to player 2.