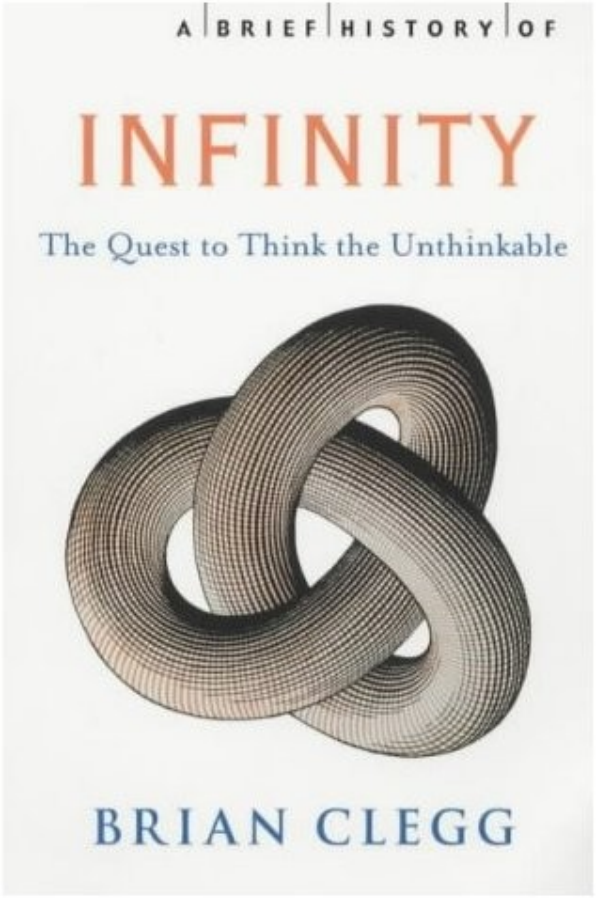
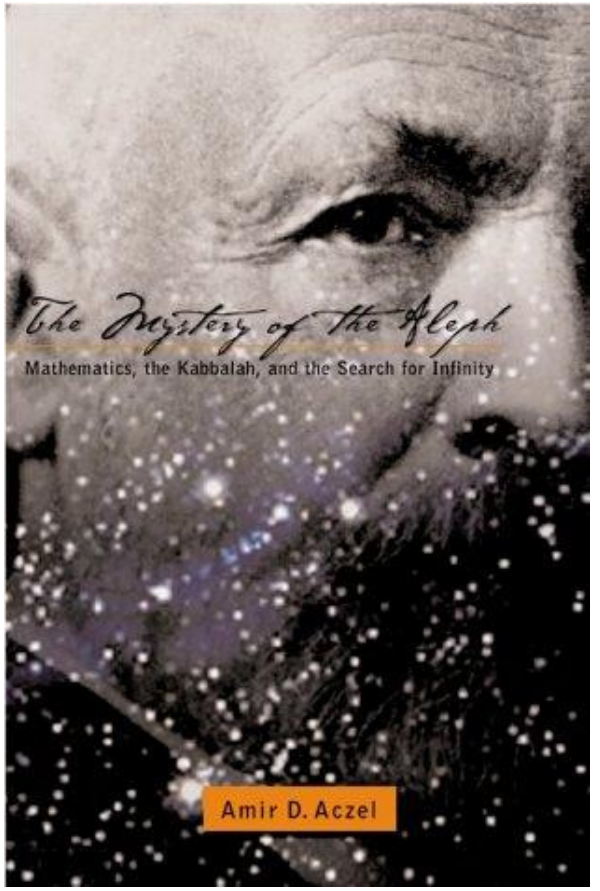
Direct Proofs

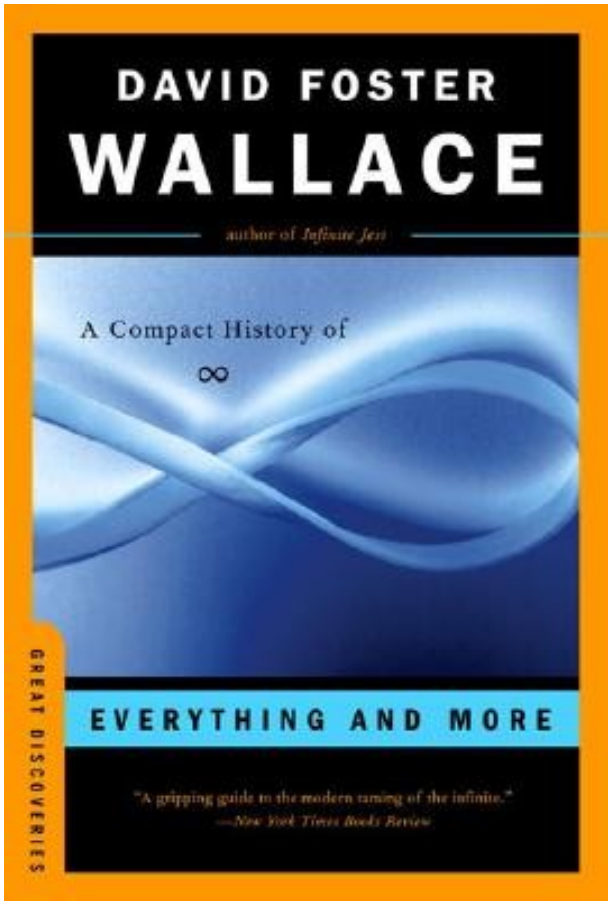
Recommended Reading



A Brief History of Infinity



The Mystery of the Aleph



Everything and More

Recommended Courses

Math 161: Set Theory

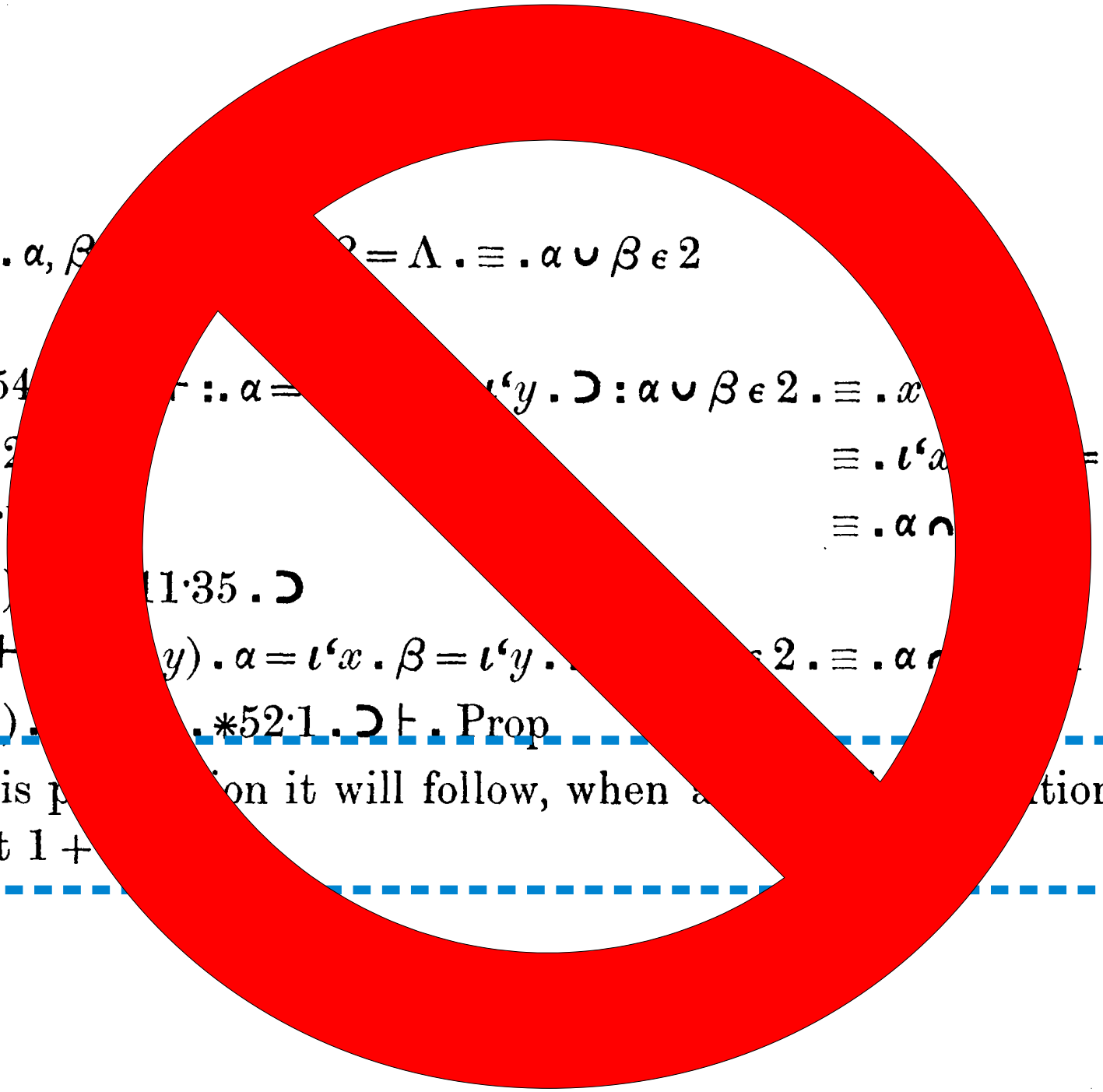
Outline for Today

- ***Mathematical Proof***
  - What is a mathematical proof? What does a proof look like?
- ***Direct Proofs***
  - A versatile, powerful proof technique.
- ***Universal and Existential Statements***
  - What exactly are we trying to prove?
- ***Proofs on Set Theory***
  - Formalizing our reasoning.

What is a Proof?

A ***proof*** is an argument that demonstrates why a conclusion is true.

A ***mathematical proof*** is an argument that demonstrates why a mathematical statement is true.



*54·43. $\vdash :. \alpha, \beta$ $\cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54$ $\vdash :. \alpha =$ $\iota' y . \supset : \alpha \cup \beta \in 2 . \equiv . x$

[*51·2 $\equiv . \iota' \alpha$ $= \Lambda .$

[*13· $\equiv . \alpha \cap$ (1)

$\vdash . (1)$ $11{\cdot}35 . \supset$

$\vdash$ $y) . \alpha = \iota' x . \beta = \iota' y .$ $\in 2 . \equiv . \alpha \cap$ (2)

$\vdash . (2) .$ $. *52{\cdot}1 . \supset \vdash . \text{Prop}$

From this p on it will follow, when a tion has been defined, that $1 +$

Modern Proofs

Two Quick Definitions

- An integer n is ***even*** if there is some integer k such that $n = 2k$.
  - This means that 0 is even.
- An integer n is ***odd*** if there is some integer k such that $n = 2k + 1$.
  - This means that 0 is not odd.
- We'll assume the following for now:
  - Every integer is either even or odd.
  - No integer is both even and odd.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

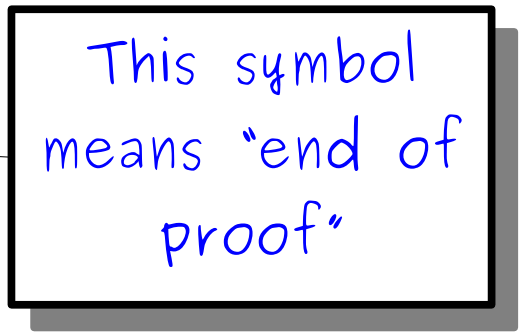
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■



Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

Since n i… such tha…

This mea… .

From thi… r m (name…

Therefor…

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means th … ^{2}).

From this, we … er m (namely, $2k$ …

Therefore, n^2 …

This is the definition of an even integer. When writing a mathematical proof, it's common to call back to the definitions.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Fr
m

Th

Notice how we use the value of ***k*** that we obtained above. Giving names to quantities, even if we aren't fully sure what they are, allows us to manipulate them. This is similar to variables in programs.

Our First Direct Proof

Theorem: If n [illegible] en.

Proof: Let n b[illegible]

Since n [illegible]
such th[illegible]

This me[illegible] $= 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

Our ultimate goal is to prove that n^2 is even. This means that we need to find some m such that $n^2 = 2m$. Here, we're explicitly showing how we can do that.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This mea

From thi

m (name

Therefore, n^2 is even. ■

Hey, that's what we were trying to show! We're done now.

Our First Direct Proof

Theorem: If n is an even integer, then n^2 is even.

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Therefore, n^2 is even. ■

That wasn't so bad! Let's do another one.

Set Theory Review

- Recall from last time that we write $x \in S$ if x is an element of set S and $x \notin S$ if x is not an element of set S.
- If S and T are sets, we say that S is a subset of T (denoted $S \subseteq T$) if the following statement is true:

  For every object x, if $x \in S$, then $x \in T$.

- Let's explore some properties of the subset relation.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

How do we prove that this is true for *any* choice of sets?

Proving Something Always Holds

- Many statements have the form

  For any *x*, `[some-property]` holds of *x*.

- Examples:

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

  For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

  For all sets S, $|S| < |\wp(S)|$.

  Everything that drowns me makes me wanna fly.

- How do we prove these statements when there are (potentially) infinitely many cases to check?

Arbitrary Choices

- To prove that some property holds true for all possible x, show that no matter what choice of x you make, that property must be true.
- Start the proof by making an ***arbitrary choice*** of x:
  - "Let x be chosen arbitrarily."
  - "Let x be an arbitrary even integer."
  - "Let x be an arbitrary set containing 137."
  - "Consider any x."
- Demonstrate that the property holds true for this choice of x.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$.

We're showing here that regardless of what ***A***, ***B***, *and* ***C*** you pick, the result will still be true.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$.

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

This is, by definition, what it means for $A \subseteq C$ to be true. Our job will be to prove this statement.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$.

We're showing here that regardless of what **x** you pick, the result will still be true.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$.

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Theorem: For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof: Let A, B, and C be arbitrary sets where $A \subseteq B$ and $B \subseteq C$. We need to prove that $A \subseteq C$. To do so, we will prove that for every x, if $x \in A$, then $x \in C$.

Consider any x where $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$. Similarly, since $B \subseteq C$ and $x \in B$, we see that $x \in C$, which is what we needed to show. ■

Transitivity

- We just proved that if A, B and C are sets where $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
- This property of the $\subseteq$ relation is called ***transitivity***. We'll revisit it later in the quarter.

Theorem: For any sets A, B, C, and D, if $A \subseteq B$, $B \subseteq C$, and $C \subseteq D$, then $A \subseteq D$.

Proof: Let A, B, C, and D be arbitrary sets where $A \subseteq B$, $B \subseteq C$, and $C \subseteq D$. We need to prove that $A \subseteq D$.

Since $A \subseteq B$ and $B \subseteq C$, by our earlier theorem we know that $A \subseteq C$. Similarly, since $A \subseteq C$ and $C \subseteq D$, our previous theorem tells us that $A \subseteq D$, which is what we needed to show. ■

We're heavily leveraging our previous proof here. *This is extremely common!* Most of mathematics is about building on earlier results.

The Story So Far

- If you need to prove an implication (a statement of the form “if P, then Q”), you should assume P is true, then prove Q is true.
- To prove a statement of the form “for all x, some property $P(x)$ is true,” state that you're choosing an arbitrary x, then prove that $P(x)$ must be true.
- Proofs usually call back to some key terms or definitions (here, even numbers, and subsets).
- Proofs build on top of one another. Once you do enough math, you start to use older proofs as building blocks in larger proofs.

How Not To Write Proofs

An Incorrect Proof

Theorem: For all sets A and B, we have $A \subseteq A \cap B$.

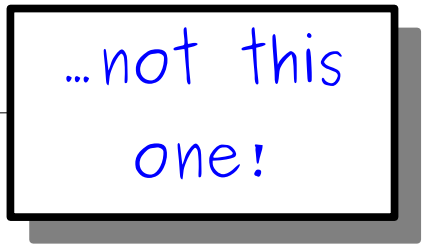
Proof: Consider two arbitrary sets, say, $A = \varnothing$ and $B = \mathbb{N}$. Since $\varnothing$ is a subset of every set and $A = \varnothing$, we see that $A \subseteq A \cap B$. Since our choices of A and B were arbitrary, we conclude that if A and B are any sets, then $A \subseteq A \cap B$. ■

An Incorrect Proof

Theorem: For all sets A and B, we have $A \subseteq A \cap B$.

Proof: Consider two arbitrary sets, say, $A = \varnothing$ and $B = \mathbb{N}$. Since $\varnothing$ is a subset of every set and $A = \varnothing$, we see that $A \subseteq A \cap B$. Since our choices of A and B were arbitrary, we conclude that if A and B are any sets, then $A \subseteq A \cap B$. ■

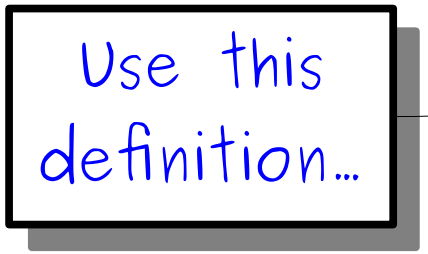
ar·bi·trar·y
adjective /'ärbi,trerē/



1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value



Source: Google

To prove something is true for all x, don't choose an x and base the proof off of your choice.

Instead, leave x unspecified and show that no matter what x is, the specified property must hold.

Another Incorrect Proof

Theorem: For all sets A and B, we have $A \subseteq A \cap B$.

Proof: Consider two arbitrary sets A and B. We need to prove that $A \subseteq A \cap B$. To do so, we will prove that if $x \in A$, then $x \in A \cap B$ as well.

Consider any arbitrary $x \in A \cap B$. We will prove that $x \in A$. To do so, notice that since $x \in A \cap B$, we know that $x \in A$ and that $x \in B$. In particular, this means that $x \in A$, which is what we needed to show. ■

Another Incorrect Proof

Theorem: For all sets A and B, we have $A \subseteq A \cap B$.

Proof: Consider two arbitrary sets A and B. We need to prove that $A \subseteq A \cap B$. To do so, we will prove that if $x \in A$, then $x \in A \cap B$ as well.

Consider any arbitrary $x \in A \cap B$. We will prove that $x \in A$. To do so, notice that since $x \in A \cap B$, we know that $x \in A$ and that $x \in B$. In particular, this means that $x \in A$, which is what we needed to show. ■

If you want to prove that P implies Q,
assume P and prove Q.

Don't assume Q and then prove P!

Special Classes of Statements

Universal and Existential Statements

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

This is a fundamentally different type of proof that what we've done before. Instead of showing that *every* object has some property, we want to show that *some* object has a given property.

Universal vs. Existential Statements

- A ***universal statement*** is a statement of the form

  For all *x*, `[some-property]` holds for *x*.

- We've seen how to prove these statements.
- An ***existential statement*** is a statement of the form

  There is some *x* where `[some-property]` holds for *x*.

- How do you prove an existential statement?

Proving an Existential Statement

- Over the course of the quarter, we will see several different ways to prove an existential statement.
- ***Simplest approach:*** Just go and find some x where the property $P(x)$ is true.
  - In our case, we need to find a positive natural number n such that that sum of all smaller natural numbers is equal to n.
  - Can we find one?

An Entirely Different Proof

Theorem: There exists a natural number $n > 0$ such that the sum of all natural numbers less than n is equal to n.

Proof: Take $n = 3$.

The three natural numbers smaller than three are 0, 1, and 2.

Notice that $0 + 1 + 2 = 3$.

Therefore, there is a natural number greater than zero equal to the sum of all smaller natural numbers. ■

Biconditional Statements

Biconditionals

- You often see statements like these in mathematics:

  The natural number n is even *if and only if* n^2 is even.

  G is bipartite *if and only if* G has no odd cycles.

  $L \in$ **RE** *if and only if* there is a verifier for L.

- All of these statements involve the phrase "if and only if."
- The statement "P if and only if Q" means the following:

  If *P*, then *Q*, *and* if *Q*, then *P*.

- In other words, both P and Q imply each other.
- These statements are called ***biconditional statements***. To prove a biconditional statement, you usually prove both implications separately.

Set Equality

- If A and B are sets, we say that $A = B$ precisely when the following statement is true:

  For any object x, $x \in A$ if and only if $x \in B$.

- (This is called the ***axiom of extensionality***.)
- In practice, this definition is tricky to work with.
- It's often easier to use the following result to show that two sets are equal:

  For any sets A and B,
  if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Theorem: For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof: Let A and B be arbitrary sets where $A \subseteq B$ and $B \subseteq A$. We will prove that $A = B$ by proving that, for any arbitrary x, that $x \in A$ if and only if $x \in B$.

First, we'll prove that if $x \in A$, then $x \in B$. Take any $x \in A$. Since $A \subseteq B$ and $x \in A$, we see that $x \in B$, as required.

Next, we'll prove that if $x \in B$, then $x \in A$. Take any $x \in B$. Since $B \subseteq A$ and $x \in B$, we see that $x \in A$, as required.

Since we've proven both directions of implication, we see that $A = B$, as required. ■

Time-Out for Announcements!

Things to Read

- We've released two handouts you should read over:
  - Handout 03: How to Succeed in CS103
  - Handout 04: Set Theory Definitions.
- Additionally, if you haven't yet read over the Guide to Elements and Subsets, we'd recommend doing so.
- Finally, we strongly recommend reading over Chapter 1 and Chapter 2 of the online course reader to get some more background with proofs and set theory.

Piazza

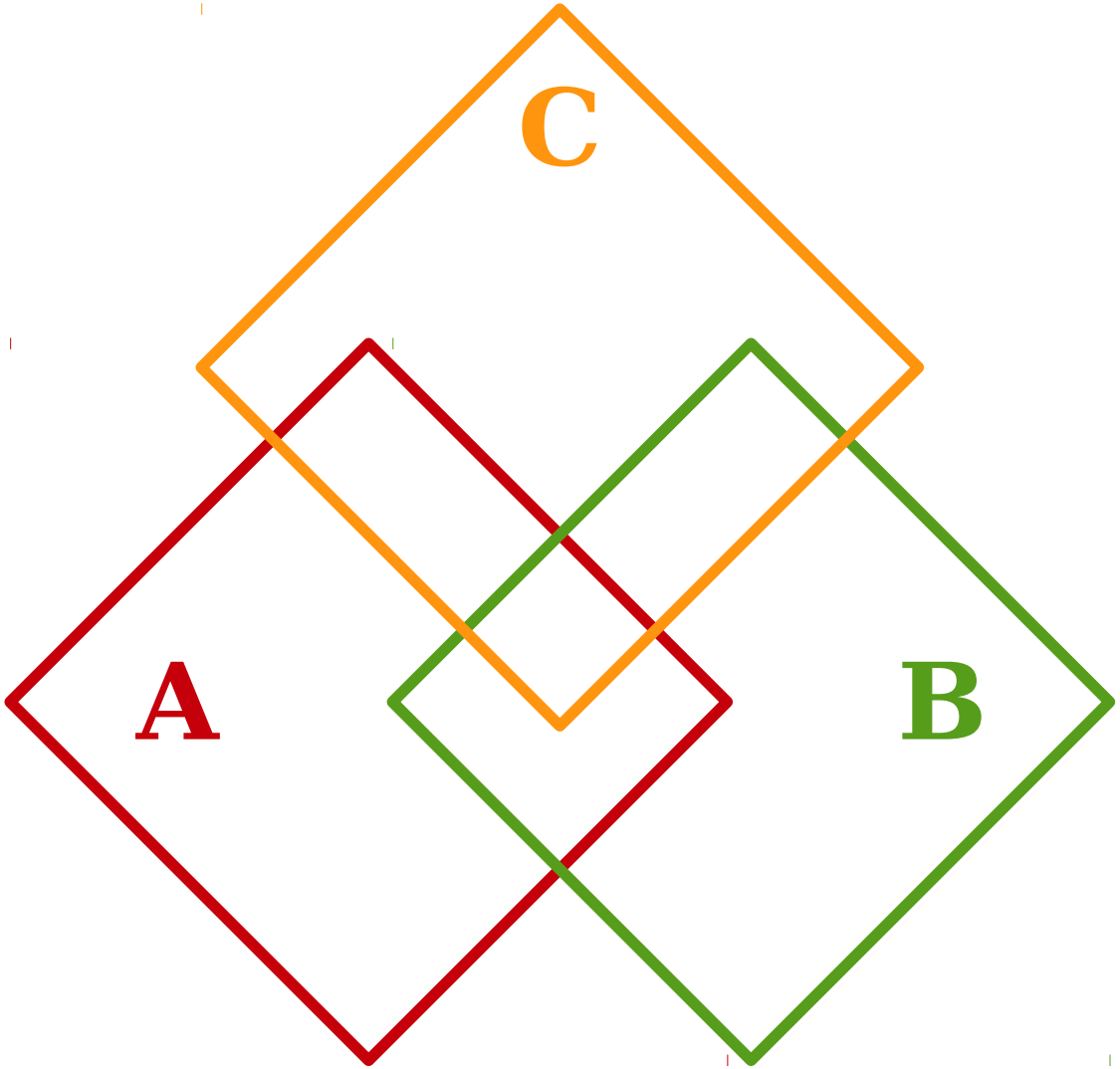
- We now have a Piazza site for CS103.
- Sign in to www.piazza.com and search for the course CS103 to sign in.
- Feel free to ask us questions!
- ***Use the site to find a partner for the problem sets!***

Back to CS103!

Proofs on Set Combinations

Theorem: Let A, B, and C be any sets. Then

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$



Theorem: Let A, B, and C be any sets. Then

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

To prove this, we'll prove each is a subset of the other:

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$$

$$(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$$

Relations Between Proofs

- Proofs often build off of one another: large results are almost often accomplished by building off of previous work.
  - Like writing a large program – split the work into smaller methods, across different classes, etc. instead of putting the whole thing into `main`.
- A result that is proven specifically as a stepping stone toward a larger result is called a ***lemma***.
- We'll prove each of these smaller statements as a lemma for part of the larger proof. It's decomposition, proof style!

Lemma 1: For any sets A, B, and C, the following is true:

$$(A \cup B) \cap C \quad \subseteq \quad (A \cap C) \cup (B \cap C).$$

Proof: Consider any arbitrary sets A, B, and C. We need to prove that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. To do so, consider an arbitrary $x \in (A \cup B) \cap C$. We will prove that $x \in (A \cap C) \cup (B \cap C)$.

Since $x \in (A \cup B) \cap C$, we know … what, exactly?

The Need for Formalisms

- In all of our previous proofs, we've used formal definitions for terms that we have a good intuitive feel for.
  - Even numbers, subsets, set equality, etc.
- Mathematics revolves around formal definitions. Definitions give us a clear sense of what something means and guides the structure of our proofs.

Set Operations

- Last time, we introduced four operations for combining sets together:
  - Union: $S \cup T$
  - Intersection: $S \cap T$
  - Difference: $S - T$
  - Symmetric Difference: $S \Delta T$
- While we may have an intuitive feel for these terms, we haven't actually defined them anywhere. Therefore, we can't rigorously reason about them in proofs.
- Let's go fix that!

Set Operations

- The union of two sets S and T is defined as follows:

$$\boldsymbol{S \cup T = \{ x \mid x \in S \text{ or } x \in T \text{ (or both)} \}}$$

- As a result, if x is any object, then $x \in S \cup T$ if and only if $x \in S$ or $x \in T$ (or both).
- The intersection of two sets S and T is defined as follows:

$$\boldsymbol{S \cap T = \{ x \mid x \in S \text{ and } x \in T \}}$$

- As a result, if x is any object, then $x \in S \cap T$ if and only if $x \in S$ and $x \in T$.
- We can use these definitions and these properties to write formal proofs about unions and intersections.

Lemma 1: For any sets A, B, and C, the following is true:

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C).$$

Proof: Consider any arbitrary sets A, B, and C. We need to prove that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. To do so, consider an arbitrary $x \in (A \cup B) \cap C$. We will prove that $x \in (A \cap C) \cup (B \cap C)$.

Since $x \in (A \cup B) \cap C$, we know that $x \in A \cup B$ and that $x \in C$. Because $x \in A \cup B$, we know that $x \in A$ or $x \in B$ (or both). We consider two cases:

Case 1: $x \in A$.

Case 2: $x \in B$.

This is called a **proof by cases** (alternatively, a **proof by exhaustion**) and works by showing that the theorem is true regardless of what specific outcome arises.

Lemma 1: For any sets A, B, and C, the following is true:

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C).$$

Proof: Consider any arbitrary sets A, B, and C. We need to prove that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. To do so, consider an arbitrary $x \in (A \cup B) \cap C$. We will prove that $x \in (A \cap C) \cup (B \cap C)$.

Since $x \in (A \cup B) \cap C$, we know that $x \in A \cup B$ and that $x \in C$. Because $x \in A \cup B$, we

Case 1: x ∈ A. Then since

that $x \in A \cap C$. Therefor

Case 2: x ∈ B. Then since

that $x \in B \cap C$. Therefore, $x \in (A \cap C) \cup (B \cap C)$.

In both cases, we see that $x \in (A \cap C) \cup (B \cap C)$, which is what we needed to show.

After splitting into cases, it's a good idea to summarize what you just did so that the reader knows what to take away from it.

Lemma 1: For any sets A, B, and C, the following is true:

$$(A \cup B) \cap C \quad \subseteq \quad (A \cap C) \cup (B \cap C).$$

Proof: Consider any arbitrary sets A, B, and C. We need to prove that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. To do so, consider an arbitrary $x \in (A \cup B) \cap C$. We will prove that $x \in (A \cap C) \cup (B \cap C)$.

Since $x \in (A \cup B) \cap C$, we know that $x \in A \cup B$ and that $x \in C$. Because $x \in A \cup B$, we know that $x \in A$ or $x \in B$ (or both). We consider two cases:

Case 1: $x \in A$. Then since $x \in A$ and $x \in C$, we know that $x \in A \cap C$. Therefore, $x \in (A \cap C) \cup (B \cap C)$.

Case 2: $x \in B$. Then since $x \in B$ and $x \in C$, we know that $x \in B \cap C$. Therefore, $x \in (A \cap C) \cup (B \cap C)$.

In both cases, we see that $x \in (A \cap C) \cup (B \cap C)$, which is what we needed to show. ■

Lemma 2: For any sets A, B, and C, the following is true:

$$(A \cap C) \cup (B \cap C) \quad \subseteq \quad (A \cup B) \cap C.$$

Proof: Consider any arbitrary sets A, B, and C. We need to prove that $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$. To do so, consider an arbitrary $x \in (A \cap C) \cup (B \cap C)$. We will prove that $x \in (A \cup B) \cap C$.

Since $x \in (A \cap C) \cup (B \cap C)$, we know that either $x \in A \cap C$ or that $x \in B \cap C$ (or both). We consider two cases:

Case 1: $x \in A \cap C$. This means that $x \in A$ and $x \in C$. Since $x \in A$, we see that $x \in A \cup B$. Therefore, we see that $x \in (A \cup B) \cap C$.

Case 2: $x \in B \cap C$. This means that $x \in B$ and $x \in C$. Since $x \in B$, we see that $x \in A \cup B$. Therefore, we see that $x \in (A \cup B) \cap C$.

In both cases, we see that $x \in (A \cup B) \cap C$, which is what we needed to show. ■

Theorem: For any sets A, B, and C, the following is true:

$$(A \cap C) \cup (B \cap C) \quad = \quad (A \cup B) \cap C.$$

Proof: Consider any sets A, B, and C. By Lemma 1, we see that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. From Lemma 2, we see that $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$. Since each of these sets are subsets of one another, we conclude that the two sets are equal. ■

What We've Covered

- ***What is a mathematical proof?***
  - An argument – mostly written in English – outlining a mathematical argument.
- ***What is a direct proof?***
  - It's a proof where you begin from some initial assumptions and reason your way to the conclusion.
- ***What are universal and existential statements?***
  - Universal statements make a claim about all objects of one type. Existential statements make claims about at least one object of some type.
- ***How do we write proofs about set theory?***
  - By calling back to definitions! Definitions are key.

Next Time

- ***Indirect Proofs***
  - How do you prove something without actually proving it?
- ***Mathematical Implications***
  - What exactly does "if P, then Q" mean?
- ***Proof by Contrapositive***
  - A helpful technique for proving implications.
- ***Proof by Contradiction***
  - Proving something is true by showing it can't be false.