How to Prove Things

Stuart Gluck, Ph.D.
Director, Institutional Research
Johns Hopkins University
Center for Talented Youth (CTY)

Carlos Rodriguez
Assistant Director, Academic Programs
Johns Hopkins University
Center for Talented Youth (CTY)

JOHNS HOPKINS
UNIVERSITY
Center for Talented Youth

What do mathematicians do?

- Solve problems/calculate solutions
- Develop models that describe real world situations
- Offer definitions
- Propose conjectures
- Prove/disprove conjectures

Proving (and Disproving)

- Which area of math does the study of proofs (proof theory) belong to?
- Logic!
- Question: How many of you majored in math or math education, or in education with a concentration in math?
- Question: How many of you took a course in logic?

The Problem

- We don’t explicitly teach proof techniques in math classes very much…

- …even though it’s arguably the most important mathematical skill, and certainly the one used most by working (pure) mathematicians

The Goal

- The goal of this session is to teach general strategies for writing proofs (and for constructing counterexamples)
- These strategies are not specific to any area of math
- Basically, we'll provide a taxonomy of the main strategies available

What is a Mathematical Proof?

- It’s an argument
- Specifically, it’s a deductive argument

Arguments

- An argument is a collection of premises and a conclusion
- Arguments can be inductive or deductive
- Inductive arguments can be strong or weak (and cogent or incogent)
- Examples include enumerative generalization (but not mathematical induction!)
- Deductive arguments can be valid or invalid (and sound or unsound)
- The classic example is a mathematical proof
- Deductive arguments are monotonic

Mathematical Proofs

- The premises are a set of statements, which could include:
  - Definitions
  - Axioms
  - Conditions specified by the problem/situation
  - Previously derived results/theorems/lemmas
- The conclusion is obviously the conjecture being proven

The Form of a Proof

- A proof can be formal or informal
- An informal proof is sometimes called a proof cartoon or proof sketch
- A formal proof can use a range of conventions, but typically revolves around numbered lines, specification of previous lines, and rules of inference; it might also include sub-derivations (sub-proofs) and conventions for indicating when these are closed

Proof Strategies

- Direct proofs
  - Direct derivation
  - By cases
  - Enumerative
- Conditional proofs
- Indirect proofs (aka reductio ad absurdum or proof by contradiction)
- Existential proofs (constructive)
- Universal proofs
  - Universal derivation
  - Mathematical induction
  - Strong induction

Direct Proofs

- Direct derivations are the simplest proofs

- The method is to simply start with premises and apply rules of inferences until the conclusion is derived

Example: Direct Derivation

Prove that the sum of any two even integers is also an even integer

Let m, n be the even integers

1.	**~~Show~~ m + n is even**	
2.	m = 2k, where k is an integer	By definition of even integer
3.	n = 2j, where j is an integer	By definition of even integer
4.	m + n = 2k + 2j	By substitution
5.	m + n = 2(k + j)	By distributive property
6.	m + n = 2(an integer)	Sum of any 2 integers is an integer
7.	m + n is an even integer	By definition of even integer

Q.E.D.

Example: Proof by Cases

- Prove that $n^2 + n$ is even, for any integer n
- Either n is even or n is odd
- We can consider the 2 cases separately

The Even Case

Case 1: n is even

1.	~~Show~~ $n^2 + n$ is even	
2.	$n = 2k$	Definition of even integer
3.	$n(n + 1) = 2k(n + 1)$	Multiply both sides by $n + 1$
4.	$n^2 + n = 2k(n + 1)$	Algebra
5.	$n^2 + n$ is even	Definition of even integer

The Odd Case

Case 2: n is odd

1.	~~Show~~ $n^2 + n$ is even	
2.	$n = 2k + 1$	Definition of odd integer
3.	$n + 1 = 2k + 2$	Add 1 to each side
4.	$n + 1 = 2(k + 1)$	Algebra
5.	$n(n + 1) = n \cdot 2(k + 1)$	Multiply both sides by n
6.	$n^2 + n = 2n(k + 1)$	Algebra
7.	$n^2 + n$ is even	Definition of even integer

Example: Proof by Cases

- We now know that:
  - If n is even, $n^2 + 1$ is even
  - If n is odd, $n^2 + 1$ is even
  - n must either be even or odd
- So $n^2 + 1$ is even for every integer n

Example: Enumerative Proof

- An enumerative proof is similar to proof by cases, except that we enumerate every specific possibility (rather than general categories) in order to show what must be the case

- Example (the Monty Hall problem): show that the probability of winning the prize is 2/3 if you switch doors after the game show host shows you the prize is not behind one of the other doors

The Monty Hall Problem

- You choose door #1 and decide to switch
- There are 3 equally likely possibilities:
  1. The prize is behind door #1. Doors #2 and #3 contain Zonks. You switch, Zonk!
  2. The prize is behind door #2. The host reveals door #3. You switch. Prize!
  3. The prize is behind door #3. The host reveals door #2. You switch. Prize!
- It works exactly the same way if you initially choose door #2 or door #3 and then switch.
- So you win 2/3 of the time if you switch.

Conditional Proofs

- To prove a claim of the form (if P then Q), assume P and then show Q must follow
- P is called the hypothesis (there may be more than one hypothesis)
- Q, obviously, is the conclusion
- This is a very common strategy, because mathematicians often state the answer to a mathematical question in the form of a theorem that says if certain assumptions (hypotheses) of the theorem are true, then some conclusion must also be true
- This strategy is obviously legitimate, since the hypotheses are conditions for the conclusion, so assuming them just limits us to the cases to which the theorem applies

Example: Conditional Proof

Let m and n be integers. If both m and n are odd, then mn is odd.

1.	**~~Show~~ (m, n are odd integers) → (mn is odd)**	
2.	m, n are odd integers	Assumption CD
3.	~~Show~~ mn is odd	
4.	$m = 2q + 1$	Definition of odd integer
5.	$n = 2r + 1$	Definition of odd integer
6.	$mn = (2q + 1)(2r + 1)$	
7.	$mn = 4qr + 2q + 2r + 1$	
8.	$mn = 2(2qr + q + r) + 1$	
9.	mn is odd	Definition of odd integer, since $2qr + q + r$ is an integer

Indirect Proof

- This is also known as *reductio ad absurdum* or proof by contradiction
- To prove P, assume P is false and then derive a contradiction
- This strategy is legitimate, because it shows that P can't possibly be false, so it must be true
- This strategy is often used to prove negative claims (e.g., "there is no x," or "x is not true,")
- This is a very powerful strategy, and is often the "go to" strategy when no other approach will apparently work

Example: Indirect Proof

There is no smallest positive rational number.

1.	~~Show~~ there is no smallest positive rational number	
2.	There is a smallest positive rational number, q	Assumption ID
3.	Let r = q/2	
4.	$0 < r < q$	From 3
5.	There exist m and n s.t. $q = m/n$ and $n \neq 0$	Definition of rational number
6.	$r = m/2n$	From 3, 5
7.	r is rational	Definition of rational number, since m and 2n are integers and $2n \neq 0$
8.	r is a positive rational number less than q	From 4, 7
9.	$\perp$	From 2, 8

Mixing Strategies using Subproofs

- Often we need to complete “proofs within a proof,” or subproofs
- Often subproofs use a strategy different than the overall strategy
- (A “mixed strategy” can also be used within a proof: deriving a contradiction allows you to conclude a proof, even if you didn’t begin with an indirect strategy!)

Example: Subproofs

We'll use an indirect subderivation within a conditional proof.

Let m, n be integers. If mn is odd, then both m and n are odd.

1.	~~Show~~ **(mn is odd) → (m and n are odd)**	
2.	m and n are integers s.t. mn is odd	Assumption CD
3.	~~Show~~ m and n are odd	
4.	m and n are not both odd	Assumption ID
5.	Either m or n is even	From 4
6.	Without loss of generality, assume m is even	(do this when it's sufficient to prove a result for only 1 of the cases)
7.	m = 2k	Definition of even integer
8.	mn = 2kn	Multiply both sides by n
9.	mn is even	Definition of even integer, since kn is an integer
10.	⊥	From 2, 9

Review and the Contrapositive

- Review—to prove something of form:
  - $P \wedge Q$, prove both P and Q (directly or indirectly)
  - $P \vee Q$, prove either P or Q (directly or indirectly)
  - $P \rightarrow Q$, use conditional proof
  - $\neg P$, use indirect proof
  - $P \leftrightarrow Q$, prove each direction using conditional proof (see below)
- Tip: Often to prove $P \rightarrow Q$ it's easier to prove $\neg Q \rightarrow \neg P$, which is logically equivalent
- Let's show why, which gives us a chance to point out that biconditional claims [e.g., $(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$] are really conjunctions of two conditionals
- To prove a conjunction (per above), prove each conjunct
- Since the conjuncts of a biconditional are conditionals, prove each by conditional proof

Proof: The Contrapositive

First conditional:

1.	**~~Show~~ $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$**	
2.	$P \rightarrow Q$	Assumption CD
3.	~~Show~~ $\neg Q \rightarrow \neg P$	
4.	$\neg Q$	Assumption CD
5.	~~Show~~ $\neg P$	
6.	$\neg P$	2, 4 Modus Tollens

Proof: The Contrapositive

The second conditional:

1.	~~Show~~ $(\neg Q \rightarrow \neg P) \rightarrow (P \rightarrow Q)$	
2.	$\neg Q \rightarrow \neg P$	Assumption CD
3.	~~Show~~ $P \rightarrow Q$	
4.	P	Assumption CD
5.	~~Show~~ Q	
6.	$\neg\neg P$	4, Double Negation
7.	$\neg\neg Q$	2, 6 Modus Tollens
8.	Q	7, Double Negation

Existential (Constructive) Proofs

- Existence claims (of the form $\exists xPx$) are sometimes proven directly or conditionally from premises or hypotheses, or proven indirectly
- Typically, though, they are proven by construction
- This strategy involves constructing an example (finding something with the relevant property) and then generalizing using existential generalization
- Existential generalization just says that since m has the property P, there must be at least one thing which has the property P

Example: Existential Proof

Prove there exists a rational number x such that $x - x^2 > 0$

1.	~~Show~~ $\exists x(x - x^2 > 0)$	
2.	Let a = ½	
3.	$a - a^2 = ½ - (½)^2 = ½ - ¼ = ¼$	Substitution, arithmetic
4.	$a - a^2 > 0$	From 3
5.	$\exists x(x - x^2 > 0)$	4, Existential Generalization

Aside: Intuitionism

- Intuitionism is a school of thought amongst some (a minority of) mathematicians that all existence claims must be proven constructively, rather than indirectly

- The view amounts to saying that if you want to prove to me that an x exists, find me an x; it's not sufficient to show that assuming there is no x leads to a contradiction if we have no example of an x

Universal Proofs

- Universal claims (e.g., of the form $\forall xPx$), are sometimes proven directly or conditionally from premises or hypotheses, or proven indirectly

- Typically, though, they are proven using universal derivation

- This strategy involves choosing an arbitrary object and proving it has the property P. Since the object was chosen arbitrarily and it has the property, all objects of that type must have the property.

Example: Universal Derivation

Prove that for every integer $n > 1$, $n^2 > n + 1$

1.	**~~Show~~ $\forall x \in Z((x > 1) \rightarrow (x^2 > x + 1))$**	
2.	Let a be an (arbitrary) integer s.t. $a > 1$	UD
3.	~~Show~~ $a^2 > a + 1$	
4.	$a \geq 2$	From 2, definition of integer
5.	$a^2 \geq 2a$	Multiply both sides by a
6.	$2a > a + 1$	From 2, add a to both sides
7.	$a^2 > a + 1$	From 5, 6, Transitivity ($a^2 \geq 2a > a + 1$)

Mathematical Induction

- A special case of universal proof is mathematical induction—it is designed for proving statements about natural numbers

- This strategy involves proving:
  1. The result/property is true for the base (first) case [base case]
  2. For every natural number n, if the result/property is true for n, then it is also true for n + 1

     [inductive step or induction step]

Example: Mathematical Induction

Prove that for every natural number n, $2^n > n$

1.	~~Show~~ $\forall n \in N(2^n > n)$	
2.	~~Show~~ P(N) is true for n = 1	
3.	$2^1 = 2 > 1$	
4.	~~Show~~ $P(k) \rightarrow P(k + 1)$	
5.	$2^k > k$	Assumption CD
6.	~~Show~~ $2^{k+1} > k + 1$	
7.	$2^{k+1} > 2k$	From 5, multiply both sides by 2
8.	$k \geq 1$	k is a natural number
9.	$k + k \geq k + 1$	From 8, add k to both sides
10.	$2k \geq k + 1$	From 9
11.	$2^{k+1} > k + 1$	From 7, 10, Transitivity ($2^{k+1} > 2k \geq k + 1$)

Strong Induction

- Sometimes it's best to use an alternate form of mathematical induction known as strong induction (it's actually of equivalent strength to mathematical induction)
- We want to prove P(n) for all natural numbers n
- We prove $\forall n[(\forall k<nP(k)) \rightarrow P(n)]$
- In other words, this strategy involves:
  1. Assuming P(k) is true for all natural numbers k < n, where n is an arbitrary natural number
  2. Then proving P(n)

Example: Strong Induction

Prove every integer n > 1 is either prime or a product of primes.

1.	~~Show~~ $\forall n \in N[(n > 1) \rightarrow$ (n is prime or n is a product of primes)]	
2.	If 1 < k < n, then k is prime or k is a product of primes	Assumption
3.	~~Show~~ (n > 1) $\rightarrow$ (n is prime or n is a product of primes)	
4.	Case 1: n is prime…done for this case!	
5.	Case 2: n is not prime	
6.	Choose natural numbers a, b, s.t. n = ab, a < n, b < n	
7.	a, b > 1	From 6 (since a < n, b > 1, and similarly for a)
8.	a and b each are either prime or a product of primes	From 2
9.	n is a product of primes	From 6, 8 (n = ab and a, b are primes or the product of primes)

Proof Strategies

- To prove P from premises and there's an obvious route, use direct derivation
- To prove conditional statements, use conditional proof
- To prove negations, or if you don't know how to get going with another strategy, use indirect proof
- To prove an existence claim, use proof by construction (existential generalization)
- To prove a universal claim, use universal derivation
- To prove a universal claim about natural numbers, use mathematical induction or strong induction

Counterexamples (Disproving)

- Finding a counterexample is much like an existential (constructive) proof…you just find an example!
- Example: conjecture that if $x > 3$ then $x^2 - 2y > 5$
- Let $x = 4$ and $y = 6$
- Then $x > 3$ but $4^2 - 2(6) = 16 - 12 = 4$ (not > 5)

Counterexamples by Truth Table

- For some conjectures, though, we can find a counterexample by way of a truth table
- Example: if $P \rightarrow Q$ and $\neg P$, then $\neg Q$

P	Q	$P \rightarrow Q$	$\neg P$	$\neg Q$
T	T	T	F	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	T

- We can read off from the table that the argument is invalid due to row 3, so this is the counterexample, i.e., when P is false and Q is true

A Note on Decidability

- Can we decide whether a conjecture is valid (provable) or invalid (there's a counterexample)?
- For some relatively simple types of arguments/conjectures, yes
- These are the ones that can be characterized using propositional logic (basic sentences and logical connectives, i.e., negation, conjunction, disjunction, conditional, biconditional) only
- For conjectures that require more resources to characterize—predicate or quantified logic (i.e., quantifiers like $\forall$ or $\exists$, sets, functions, etc.)—then we only know it is valid when we find a proof or invalid when we find a counterexample!
- There are even some conjectures (e.g., the continuum hypothesis) for which we know we'll never be able to find a proof or counterexample!!

A Note on Proof Systems

- A proof is actually just a series of symbols (an ordered n-tuple) manipulated step-by-step using only a pre-allowed set of mechanical rules (rules of inference and/or rules of substitution)
- The combination of allowable rules and allowable proof strategies forms a proof system
- How do we know if a proof system is a good system?
- We need to prove things about our system of proof—this is the domain of meta-logic
- A good proof system must be:
  - Sound—if there's a proof, the argument must be valid
  - Complete—if the argument is valid, there must be a proof possible in the system

Further Aside on Proof Systems

- If a proof system is sound and complete, syntactic and semantic concepts will coincide (e.g., consistency and satisfiability)
- If a proof system is sound and complete, it is compact (in the logic sense): a set of sentences has a model (is satisfiable) if and only if every finite subset has a model (is satisfiable)
- Compactness in the logic sense is actually equivalent to compactness in the topological sense!

How to Prove Things

Stuart Gluck, Ph.D.
Johns Hopkins University
Center for Talented Youth
stu@jhu.edu

Carlos Rodriguez
Johns Hopkins University
Center for Talented Youth
ctycarlos@jhu.edu

JOHNS HOPKINS
UNIVERSITY
Center for Talented Youth

Rate this presentation on the conference app.
www.nctm.org/confapp

Download available presentation handouts from the Online Planner!
www.nctm.org/planner

Join the conversation! Tweet us using the hashtag **#NCTMDenver**