Introduction to Proofs

Terminology

Definition: *Conjecture*

A statement with an unknown truth value

Definition: *Theorem*

A conjecture that has been shown to be true

Definition: *Proof*

A sound argument that establishes the truth of a theorem

Terminology

Definition: *Lemma*

A simple theorem whose truth is used to construct more complex theorems.

Definition: *Corollary*

A theorem whose truth follows directly from another theorem

Example:

Theorem: If x is a multiple of 4, then 4|x.
Corollary: 2|x

Formal vs. Informal

Definition: *Formal Proof*

Arguments where all steps were supplied and rules for each step in the argument are given.

We saw this in the last lecture!

Definition: *Informal Proof*

Proofs where more than one rule of inference may be used in each steps, steps may be skipped, axioms begin assumed, and rules of inference are not explicitly stated.

What we'll primarily use, easier to read

Why do People Fear Proofs?

1. Proof don't come from an assembly line
   - Need knowledge, persistence, and creativity
2. Creating proofs seems like magic
   - But they are systematic in many ways
3. Proofs are hard to read and understand
   - Only if the writer makes them so
4. Institutionalized Fear
   - Many teachers avoid them in classes

Constructing a proof

1. There are several proof techniques for a reason
   - One may be easier to use than others
2. Knowledge of mathematics is important
   - Remember our math review?
3. There are “tricks” to know
   - Ex: Dividing an even # in half leaves no remainder
4. Practice helps …. a lot!
   - Just as it does for most everything
5. Dead ends are expected
   - Proofs in books are final, polished version

Types of Proofs

1. Direct Proof
   - The most common variety
2. Proof by Contraposition
   - Like Direct, but with a twist
3. Proof by Contradiction
   - A dark road on foggy night
4. Proof by Mathematical Induction
   - Wait for it

Direct Proofs

- We're trying to prove conjectures of the form $p \rightarrow q$ (if p is true, then the truth of q logically follows)

- So:

- To prove $p \rightarrow q$: Assume p and deduce q.

- (Show that $true \rightarrow false$ never happens)

Example

Conjecture: If n an is an even, then n^2 is also even, $n \in \mathbb{Z}$.

Proof (direct): Assume n is even.

By definition of an even integer, we know $\exists_{k \in \mathbb{Z}}$ s.t. $n = 2k$

Thus, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$

Since n^2 is a multiple of 2, we know that it is even.

Therefore, if n is an even, then n^2 is also even, $n \in \mathbb{Z}$.

Proof-Writing Miscellanea

- Remember: A conjecture isn't a theorem until proven
- Don't lose sight of your destination
- When writing proofs:
  1. Always start with "Proof (style):"
  2. State your allowed assumptions
  3. Define all introduced variables
  4. End proofs with "Therefore" and the conjecture

A Conjecture About Inequalities

Conjecture: **If** $0 < a < b$**, then** $a^2 < b^2$, **where** $a, b \in R$**.**

Proof (direct): Assume $a < b$ and both a and b are positive real numbers.

Multiplying both sides of $a < b$ by a gives $a^2 < ab$

Multiplying both sides of $a < b$ by b gives $ab < b^2$

By transitivity of $<$, we get $a^2 < b^2$

Therefore, if $0 < a < b$, then $a^2 < b^2$, where $a, b \in R$

Example

Conjecture: If m and n are both perfect squares, then nm is also a perfect square.

Proof (direct): a is perfect square if an integer b s.t. $a = b^2$

Assume m and n are perfect squares. By definition, $\exists_{k \in \mathbb{Z}}$ s.t. $m = k^2$ and $\exists_{j \in \mathbb{Z}}$ s.t. $n = j^2$.

$$mn = k^2 j^2 = kkjj = (kj)(kj) = (kj)^2$$

Thus mn is a perfect square.

Therefore, If m and n are both perfect squares, then nm is also a perfect square.

Remember: Contrapositive

Definition: *Contrapositive*

Given $p \to q$, the contrapositive is $\neg q \to \neg p$

p	q	$p \to q$	$\neg p$	$\neg q$	$\neg q \to \neg p$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Note: $p \to q \equiv \neg q \to \neg p$

Proof by Contraposition

- We know that $p \rightarrow q \equiv \neg q \rightarrow \neg p$

- So to prove $p \rightarrow q$, we can instead prove $\neg q \rightarrow \neg p$by assuming $\neg q$ is true and showing that $\neg p$ must follow.

Proof by Contraposition

Conjecture: If n^2 is even, then n is even ($n \in \mathbb{Z}$ is implicit)

Proof (by contraposition): (We need to show that when we assume that n is odd, this implies that n^2 is odd, given that $n \in \mathbb{Z}$.)

Assume that n is odd. We want to show that n^2 is also odd.

By definition of odd, $\exists_{k \in \mathbb{Z}}$ s.t. $n = 2k + 1$,

Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Since n^2 has the form $2m + 1$ (where $m = 2k^2 + 2k$ and $m \in \mathbb{Z}$), n^2 is odd

Therefore, if n^2 is even, then n is even.

What we just showed:

- We started with "Given that n is an integer (implicit), if n^2 is even, then n is even". In the form $p \rightarrow q$, $p : n^2$ is even and $q : n$ is even.

- So the contrapositive, $\neg q \rightarrow \neg p$, is $\neg(n \text{ is even}) \rightarrow \neg(n^2 \text{ is even})$ which is the same as n is odd $\rightarrow n^2$ is odd).

- We showed that given $n \in \mathbb{Z}$, n is odd $\rightarrow n^2$ is odd.

- Which is equivalent to showing "Given $n \in \mathbb{Z}$, if n^2 is even, then n is even"

Proof by Contraposition

Conjecture: **If** $ac \leq bc$**, then** $c \leq 0$**, when** $a > b$**.**

Proof (by contraposition): (We need to show that when we assume that $c > 0$, this implies that $ac > bc$, given that $a > b$.)

We are given $a > b$. Assume $c > 0$.

By multiplying both sides by positive value c, we get $ac > bc$. (Because c is positive, the inequality does not change)

Therefore, if $ac \leq bc$, then $c \leq 0$, when $a > b$.

Proof by Contradiction

- Recall the Law of Implication: $p \rightarrow q \equiv \neg p \vee q$
- Now consider $\neg(p \rightarrow q)$
  - $\neg(p \rightarrow q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$
- In a proof by contradiction, instead of trying to show that $p \rightarrow q \equiv T$, we try to show that $p \wedge \neg q \equiv F$.
- So:
  - To prove $p \rightarrow q$: Assume $p \wedge \neg q$ and show a contradiction.

Proof by Contradiction

Conjecture: **If $3n + 2$ is odd, then n is odd**

Proof (by contradiction):

By definition, $\exists_{k \in \mathbb{Z}}$ s.t. $n = 2k$,

Thus, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$

This shows that $3n + 2$ is even, which is a contradiction of the assumption that $3n + 2$ is odd.

Therefore, if $3n + 2$ is odd, then n is odd

What we just showed:

- We started with "If $3n + 2$ is odd, then n is odd". In the form $p \to q$, p : $3n + 2$ is odd and q : n is odd.

- Remember: $\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$

- So the negation is $(3n + 2$ is odd$) \wedge \neg(n$ is odd$)$ which is the same as $(3n + 2$ is odd$) \wedge (n$ is even$)$.

- We showed that $(3n + 2$ is odd$) \wedge \neg(n$ is odd$) \equiv$ F.

- Which is equivalent to showing "If $3n + 2$ is odd, then n is odd"

Proof by Contradiction

Conjecture: The sum of the squares of two odd integers is never a perfect square. (Or: If $n = a^2 + b^2$, then n is not a perfect square where $a, b \in \mathbb{Z}^{odd}$

Proof (Contradiction)

n is a perfect square.

By definition, $\exists_{k \in \mathbb{Z}}$ s.t. $a = 2k + 1$ and $\exists_{j \in \mathbb{Z}}$ s.t. $b = 2j + 1$.

$$n = a^2 + b^2 = (2k + 1)^2 + (2j + 1)^2$$

$$= 4k^2 + 4k + 1 + 4j^2 + 4j + 1 = 2(2k^2 + 2k + 2j^2 + 2j + 1)$$

Thus we know that n is even

(continued...)

Proof by Contradiction

Conjecture: The sum of the squares of two odd integers is never a perfect square. (Or: If $n = a^2 + b^2$, then n is not a perfect square where $a, b \in \mathbb{Z}^{odd}$

Proof (Contradiction): Because n is a perfect square, $n = m^2$, $m \in \mathbb{Z}$. We know n is even, so m^2 is even.

From an earlier proof, we know that if x^2 is even, x is even so by that result, m is even.

Thus, $\exists_{r \in \mathbb{Z}}$ s.t. $m = 2r$ and $n = m^2 = 4r^2$. Thus n is divisible by 4. But earlier, we showed that $n = 2(2k^2 + 2k + 2j^2 + 2j + 1)$ which is not divisible by four.

This is a contradiction. Therefore, if $n = a^2 + b^2$, then n is not a perfect square, where $a, b \in \mathbb{Z}^{odd}$

Proof by Contradiction

Conjecture: $\sqrt{2}$ **is irrational.**

Proof (by contradiction): Assume not. Assume that $\sqrt{2}$ is rational.

By definition of rational, $\exists_{p,q\in\mathbb{Z}}$ s.t. $\sqrt{2} = \frac{p}{q}$, where $\frac{p}{q}$ is in lowest terms.

$2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$, $2q^2 = p^2$ which implies that p^2 is even, which means p is even (proved earlier). Thus $\exists_{k\in\mathbb{Z}}$ s.t. $p = 2k$

$2q^2 = (2k)^2 = 4k^2$. Thus, $q^2 = 2k^2$ which means q^2 is even and thus q is even.

However, that means $\frac{p}{q}$ is not in lowest terms, which is a contradiction.

Therefore $\sqrt{2}$ is irrational.

Playposit: What type of proof is this

Conjecture: **If** $a, b \in \mathbb{Z}$**, then** $a^2 - 4b \neq 2$**.**

Proof (by ?): Assume $a, b \in \mathbb{Z}$. Assume $\exists_{a,b}$ s.t. $a^2 - 4b = 2$.

$a^2 = 2 + 4b = 2(2b + 1)$ so a^2 is even. We know from prior proofs that this means a is also even.

$a^2 - 4b = (2k)^2 - 4b = 4k^2 - 4b = 4(k^2 - b)$

$4(k^2 - b) = 2$. Dividing by 2 we get, $2(k^2 - b) = 1$.

This implies that 1 is even (because k and b are integers).

Thus, if $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

Proof by Cases

- How would you prove "if $n \in \mathbb{Z}^+$ and $n \leq 4$, then $(n+1)^2 \geq 3^n$"?

- There are only 4 cases!
  - $n = 1,2,3,4$

- Simply show that it is true for all cases:

Proof by Cases

Conjecture: **"if $n \in \mathbb{Z}^+$ and $n \leq 4$, then $(n+1)^2 \geq 3^n$"**

Proof (By Cases):

Case 1: $n = 1$. $(n+1)^2 = 2^2 = 4$. $3^n = 3^1 = 3$. Thus $(n+1)^2 \geq 3^n$.

Case 2: $n = 2$. $(n+1)^2 = 3^2 = 9$. $3^n = 3^2 = 9$. Thus $(n+1)^2 \geq 3^n$.

Case 3: $n = 3$. $(n+1)^2 = 4^2 = 16$. $3^n = 3^3 = 27$. Thus $(n+1)^2 \ngeq 3^n$.

Case 4: $n = 4$. $(n+1)^2 = 5^2 = 25$. $3^n = 3^4 = 81$. Thus $(n+1)^2 \ngeq 3^n$.

Thus the if $n \in \mathbb{Z}^+$ and $n \leq 4$, then it is **not** true that $(n+1)^2 \geq 3^n$

Proof by Cases

Conjecture: $|x||y| = |xy|$

Proof (By Cases):

Observe that if $x < 0$, then $|x| = -x$, otherwise, $|x| = x$.

Case 1: $x \geq 0,\ y \geq 0.\ |x||y| = xy,\ |xy| = xy.$

Case 2: $x \geq 0,\ y < 0.\ |x||y| = (x)(-y),\ |xy| = -xy.$

Case 3: (Same as case 2 with x and y reversed)

Case 4: $x < 0,\ y < 0.\ |x||y| = (-x)(-y) = xy,\ |xy| = xy.$

Therefore, $|x||y| = |xy|$.

Proof by Cases

Conjecture: if $n \in \mathbb{Z}$, **then** $n^2 \geq n$

Proof (By Cases):

Case 1: $n > 0$. $n \geq 1$. Multiply both sides by n : $n \cdot n \geq n$.
Thus $n^2 \geq n$.

Case 2: $n < 0$. $n \leq -1$. By definition, $n^2 > 0 > -1 \geq n$.
Thus $n^2 \geq n$.

Case 3: $n = 0$. $n^2 = 0 = n$. Thus $n^2 \geq n$.

Therefore, $n^2 \geq n$.

Proof by Cases

Conjecture: $s \rightarrow r \equiv \neg r \rightarrow \neg s$

Proof (By Cases):

Consider all possible combinations of values of r and s

	s	r	$s \rightarrow r$	$\neg r \rightarrow \neg s$
Case 1	T	T	T	T
Case 2	T	F	F	F
Case 3	F	T	T	T
Case 4	F	F	T	T

Therefore, $s \rightarrow r \equiv \neg r \rightarrow \neg s$

(Truth tables are a direct proof by cases)

Playposit: What case is missing from this proof?

Conjecture: if $x \in \mathbb{R}$, then $x^2 > 0$

Proof (By Cases):

Case 1: $x > 0$. When x is positive, x^2 is positive because it is the product of two positive numbers, x and x.

Case 2: $x < 0$. When x is negative, x^2 is positive because it is the product of two negative numbers, x and x.

Therefore, if $x \in \mathbb{R}$, then $x^2 > 0$

Poor Arguments lead to Poor Proofs

Conjecture: 2=1

Proof:

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $(a + b) = b$	Divide (4) by $a - b$
6. $2b = b$	Replace a with b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

$a - b = 0$!

Where did we go wrong?

Poor Arguments lead to Poor Proofs

Conjecture: $1 < 0$

Proof:

Consider x s.t. $0 < x < 1$.

Take the base 10 log of both sides of $x < 1$: $\log_{10} x < \log_{10} 1$

By definition, $\log_{10} 1 = 0$

Divide both sides by $\log_{10} x$: $\dfrac{\log_{10} x}{\log_{10} x} < \dfrac{0}{\log_{10} x}$

Which reduces to $1 < 0$

Therefore, $1 < 0$.

$\log_{10} x < 0$**! So < flips to .**

This yields $1 > 0$

Where did we go wrong?

Playposit: Is this proof correct?

Conjecture: $\forall_{n \in \mathbb{Z}^{odd}},\ (n^2 - 1)\,\%\,4 = 0$

Proof:

Let $x = 1.\ \ 1^2 - 1 = 0.\ \ 0\,\%\,4 = 0.$

Let $x = 3.\ \ 3^2 - 1 = 8.\ \ 8\,\%\,4 = 0.$

Let $x = 5.\ \ 5^2 - 1 = 24.\ \ 24\,\%\,4 = 0.$

This shows no sign of failing.

Therefore, $\forall_{n \in \mathbb{Z}^{odd}},\ (n^2 - 1)\,\%\,4 = 0.$

Where did we go wrong?

Poor attempt at an inductive proof. The argument must convince us that the pattern holds indefinitely

Proving "if and only if" Expressions

- Recall: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- So:
  - To prove $p \leftrightarrow q$, we need to prove both $p \rightarrow q$ and $q \rightarrow p$

Example: We've recently shown:

$n \in \mathbb{Z}^{even} \rightarrow n^2 \in \mathbb{Z}^{even}$, and

$n^2 \in \mathbb{Z}^{even} \rightarrow n \in \mathbb{Z}^{even}$

Therefore $(n \in \mathbb{Z}^{even}) \leftrightarrow (n^2 \in \mathbb{Z}^{even})$

Disproving Conjectures

- Typical Approaches:

1. Prove that the conjecture's negation is true
   - i.e. show that $\neg(p \rightarrow q) \equiv p \wedge \neg q \equiv \mathsf{T}$
2. Find a ***counterexample*** (very commonly used!)
   - An element for which the conjecture is false

Disproving Conjectures

Conjecture: No integer n exists s.t. the sum of its divisors equals $2n$

Proof:

Let $n = 6$. $6's$ divisors are $1, 2, 3,$ and 6.

$1 + 2 + 3 + 6 = 12 = 2n.$

Thus at least one such integer does exist, showing that the conjecture is not true.

(such integers are called 'perfect' numbers)

Note: We know that no odd from 1 through $10^{300} - 1$ is a perfect number, but there is no ***proof*** that no odd number is perfect.

Existence Proofs

- Proposition that has the form $\exists x P(x)$.
- Find an object or show that one exists
- Two main types:
  - ***Constructive*** - find an element such that $P(x)$ is true
  - ***Non-Constructive*** - don't find an element, prove existence in some other way (e.g. contradiction or contrapositive)

Constructive Existence Proofs

Conjecture: There exists an integer that can be written as the sum of two perfect squares

Proof:

$$13 = 4 + 9 = 2^2 + 3^2$$

Non-Constructive Existence Proofs

Conjecture: There exists irrational numbers x and y s.t. x^y is rational

Proof:

In Example 11 from 1.7, we know that $\sqrt{2}$ is irrational.

Let $x = y = \sqrt{2}$. Now $x^y = \sqrt{2}^{\sqrt{2}}$.

If $\sqrt{2}^{\sqrt{2}}$ is rational, we are done.

If not, it is irrational. In that case, let's try $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$.

$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$ which is rational.

Thus, there exists irrational numbers x and y s.t. x^y is rational

Uniqueness Proofs

- Proposition has the form $\exists x(P(x) \wedge \forall y\ (P(X) \rightarrow x = y))$.
- Show that exactly one object exists that makes $P(x)$ true
- Steps:
  - First show that for some object x, $P(x)$ is true
  - Second, Show that for any other y, if $P(y)$ is true, then $x = y$
    - Alternatively, if $y \neq x$, then $P(y)$ must be false.

Uniqueness Proofs

Conjecture: If a and b are real numbers and $a \neq 0$, then there is a unique real number r s.t. $ar + b = 0$

Proof:

First, note that $r = -\frac{b}{a}$ is a solution to $ar + b = 0$

Now, suppose that s is a real number s.t. $as + b = 0$

Then $ar + b = as + b$ where $r = -\frac{b}{a}$.

Subtracting b from both sides, we get $ar = as$.

Dividing both sides by a (which is not zero), we see that $r = s$.

Thus, if a and b are real numbers and $a \neq 0$, then there is a unique real number r s.t. $ar + b = 0$

Summary of Proof Strategies

- **Direct Proof:** $p \rightarrow q$ is proved by directly showing that if p is true, then q must follow.

- **Proof by Contraposition:** Prove $p \rightarrow q$ by proving $\neg q \rightarrow \neg p$

- **Proof by Contradiction:** Prove that the negation of the theorem yields a contradiction

- **Proof by Cases:** Exhaustively enumerate all different possibilities and prove the theorem for each case

Invalid Proof Strategies

- **Proof by Obviousness:** "The proof is so clear it need not be mentioned"
- **Proof by Intimidation:** Don't be stupid - of course it's true!
- **Proof by mumbo-jumbo:** "$\forall a \in A, \exists b \in a \diamond b \cong c$"
- **Proof by Intuition:** "I have a gut feeling"
- **Proof by resource limits:** "Due to lack of space, we omit this part of the proof…."
- **Proof by Illegibility:** "asdfasdgijelkd. ■"