

Mathematical theorems are often stated in the form of an implication



Example: If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$.

- $\forall x, y [(x > 0) \wedge (y > 0) \wedge (x > y) \rightarrow (x^2 > y^2)]$
- $\forall x, y P(x, y) \rightarrow Q(x, y)$

We will first discuss three applicable proof methods (Section 1.6):

- Direct proof
- Proof by contraposition
- Proof by contradiction

Direct proof



In a **direct proof**, we prove $p \rightarrow q$ by showing that if p is **true**, then q must necessarily be **true**

Example: Prove that if n is an odd integer, then n^2 is an odd integer.

Proof:

-
-
-
-

Direct proofs are not always the easiest way to prove a given conjecture.



In this case, we can try **proof by contraposition**

How does this work?

- Recall that $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Therefore, a proof of $\neg q \rightarrow \neg p$ is also a proof of $p \rightarrow q$

Proof by contraposition is an **indirect** proof technique since we don't prove $p \rightarrow q$ directly.

Let's take a look at an example...

Prove: If n is an integer and $3n + 2$ is odd, then n is odd.



First, attempt a direct proof:

- Assume that $3n + 2$ is odd, thus $3n + 2 = 2k + 1$ for some k
- Can solve to find that $n = (2k - 1)/3$ ←

Where do we go from here?!?

Now, try proof by contraposition:

-
-
-
-



Proof by contradiction

Given a conditional $p \rightarrow q$, the only way to reject this claim is to prove that $p \wedge \neg q$ is **true**.

In a **proof by contradiction** we:

1. Assume that $p \wedge \neg q$ is **true**
2. Proceed with the proof
3. If this assumption leads us to a contradiction, we can conclude that $p \rightarrow q$ is **true**

Let's revisit an earlier example...



Prove: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof:

-
-
-
-

We can also use proof by contradiction in cases where were the theorem to be proved is **not** of the form $p \rightarrow q$

Prove: At least 10 of any 64 days fall on the same day of the week



Proof:

- Let $p \equiv$ "At least 10 of any 64 days fall on the same day of the week"
- Assume $\neg p$ is true, that is "At most 9 of any 64 days fall on the same day of the week"
- Since there are 7 days in a week, at at most $7 \times 9 = 63$ days can be chosen
- This is a contradiction of the fact that we chose 64 days
- Therefore, we can conclude that at least 10 of any 64 days fall on the same day of the week. \square

This proof is an example of the pigeonhole principle, which we will study during our combinatorics unit.

Group work!



Problem: Prove the following claims

- Use a direct proof to show that the square of an even number is an even number.
- Show that if $m + n$ and $n + p$ are even integers, then the sum $m + p$ is also an even integer.
- Use proof by contraposition to show that if n is an integer and $n^3 + 5$ is odd, then n is even.

Writing proofs can be an error-prone process



Watch out for the following types of errors:

- Arithmetic and algebra
 - ↳ e.g., division by zero, incorrect factoring, etc.
- Circular reasoning
 - ↳ This occurs when one or more steps in the proof require that the theorem being proved is true
- Incorrect logic
 - ↳ e.g., assuming that $p \rightarrow q$ and $\neg p$ gives you $\neg q$

Recap



- There are multiple ways to construct **valid proofs**. Today we learned about:
 - Direct proofs
 - Proof by contraposition
 - Proof by contradiction
- Now, on to:
 - More proof techniques
 - Strategies for proof construction

Sadly, not all theorems are of the form $p \rightarrow q$



Sometimes, we need to prove a theorem of the form:

$$p_1 \vee p_2 \vee \dots \vee p_n \rightarrow q$$

Note: $p_1 \vee p_2 \vee \dots \vee p_n \rightarrow q$

Distributive law

So, we might need to examine **multiple cases!**

Sometimes, it makes sense to exhaustively search all possibilities



Not surprisingly, this is called **exhaustive proof**

When do we use this? When there are a **relatively small** number of possibilities to examine.



Good example: Show that $(n+1)^2 \geq n^3$ for positive integers less than or equal to 4.



Bad example: Show that $n^4 > 2n^2$ for all integers between 3 and 100.

Prove that $n^2 + 1 \geq 2n$ where n is a positive integer with $1 \leq n \leq 4$



Proof:

- $n = 1$:
- $n = 2$:
- $n = 3$:
- $n = 4$:

Since we have verified each case, we have shown that $n^2 + 1 \geq 2n$ where n is a positive integer with $1 \leq n \leq 4$. \square

With only 4 cases to consider, exhaustive proof was a good choice!

Sometimes, exhaustive proof isn't an option, but we still need to examine multiple possibilities



Example: Prove the triangle inequality. That is, if x and y are real numbers, then $|x| + |y| \geq |x + y|$.

Clearly, we can't use exhaustive proof here since there are **infinitely many** real numbers to consider.

We also can't use a simple direct proof either, since our proof depends on the signs of x and y .

What should we do?

Example: Prove that if x and y are real numbers, then

$$|x| + |y| \geq |x + y|.$$



Making mistakes when using proof by cases is all too easy!



Mistake 1: Proof by “a few cases” is **not** equivalent to proof by cases.

This is a “there exists” proof, not a “for all” proof!

Example: Prove that all odd numbers are prime.

“Proof:”

- Case (i): The number 1 is both odd and prime
- Case (ii): The number 3 is both odd and prime
- Case (iii): The number 5 is both odd and prime
- Case (iv): The number 7 is both odd and prime

Thus, we have shown that odd numbers are prime. \square

Making mistakes when using proof by cases is all too easy!



Mistake 2: Leaving out critical cases.

Example: Prove that $x^2 > 0$ for all integers x

“Proof:”

- Case (i): Assume that $x < 0$. Since the product of two negative numbers is always positive, $x^2 > 0$.
- Case (ii): Assume that $x > 0$. Since the product of two positive numbers is always positive, $x^2 > 0$.

Since we have proven the claim for all cases, we can conclude that $x^2 > 0$ for all integers x . \square

What about the case in which $x = 0$?

Sometimes we need to prove the **existence** of a given element



There are two ways to do this



The **constructive** approach



The **non-constructive** approach



A constructive existence proof

Prove: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Proof:

Obviously, the claim has been proven because we have shown that a specific instance of the claim is valid.



Constructive existence proofs are really just instances of “existential generalization.”



A non-constructive existence proof

Prove: Show that there exists two irrational numbers x and y such that x^y is rational.

Proof:

Note: We don't know whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. However, in either case, we can use it to construct a rational number.

Sometimes, existence is not enough and we need to prove uniqueness



This process has two steps:

- 1.
- 2.

Example: Prove that if a and b are real numbers, then there exists a unique real number r such that $ar + b = 0$

Proof:

- Note that $r = -b/a$ is a solution to this equality since $a(-b/a) + b = -b + b = 0$.
- Assume that $as + b = 0$, $s \neq r$
- Then $as = -b$, so $s = -b/a = r$, which is a contradiction \square

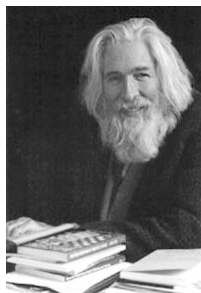
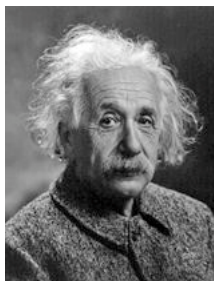
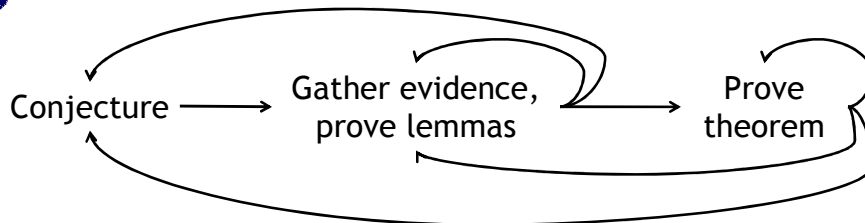
Existence



Uniqueness



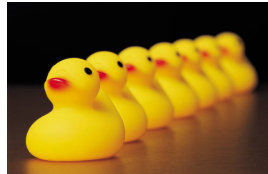
The scientific process is not always straightforward...



Proof strategies can help preserve your sanity



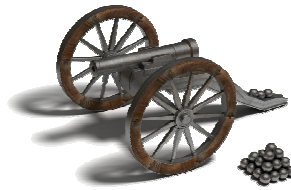
Proof strategies help us...



Organize our problem solving approach



Effectively use all of the tools at our disposal



Develop a coherent plan of attack

Types of “strategy”



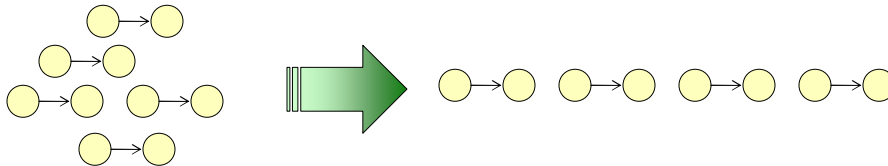
Today we'll discuss four types of strategy:

1. Forward reasoning
2. Backward reasoning
3. Searching for counterexamples
4. Adapting existing proofs

We've been doing forward reasoning all along!



In the **forward reasoning** strategy, we begin with our premises and axioms and reason towards our goal



Potential steps in the forward reasoning process:

1. Try a simple direct proof
 - ↳ Could be of form $p \rightarrow q$
 - ↳ Could be of form $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$
2. If direct proof fails, try proof by contraposition
3. If all else fails, a proof by contradiction might work

Sometimes forward reasoning doesn't work



In these cases, it is often helpful to reason **backwards**, starting with the goal that we want to prove.

Example: Prove that given two distinct positive real numbers x and y , the arithmetic mean of x and y is always greater than the geometric mean of x and y .

$$(x + y)/2$$

$$\sqrt{xy}$$

Sanity check: Let $x=8$ and $y=4$. $(8+4)/2 = 6$. $\sqrt{(8 \times 4)} = \sqrt{32} \cong 5.66$. $6 > 5.66$ \square

Prove that $(x+y)/2 > \sqrt{xy}$ for all distinct pairs of positive real numbers x and y .



Proof:

Since $(x - y)^2 > 0$ whenever $x \neq y$, the final inequality is true. Since all of these inequalities are **the same**, it follows that $(x + y)/2 > \sqrt{xy}$. \square

Other times, searching for a **counterexample** is helpful



Proof by counterexample is helpful if:

- Proof attempts repeatedly fail
- The conjecture to be proven looks “funny”

Example: Prove that every positive integer is the sum of two squares.

This seems strange to me, since other factorizations (e.g., prime factorizations) can be complex.

Counterexample:

3 is not the sum of two squares, so the claim is false. \square

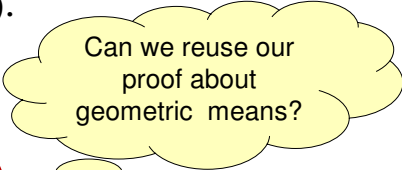
In some situations, we can “cheat” and modify existing proofs!



Observation: Often times, proofs of related facts have a similar structure.

If you ever notice this, try to reuse an existing proof to make proving a new theorem easier!

Example: Prove that for any two distinct positive real numbers that $\frac{2xy}{x+y} < \sqrt{xy}$.



Can we reuse our proof about geometric means?

This is called the harmonic mean of x and y

Prove that for any two distinct positive real numbers that $\frac{2xy}{x+y} < \sqrt{xy}$





These four proof strategies are just a start!

When trying to prove a new conjecture, a good “meta strategy” is to:

1. If possible, try to reuse an existing proof
2. If the conjecture looks fishy, check for a counterexample
3. Attempt a “real” proof
 - a) Either apply the forward reasoning strategy
 - b) Or, apply the backward reasoning strategy

Unfortunately, not every proof can be solved using this nice little meta strategy...

In fact, there are many, many proof strategies out there, and NONE of them can be guaranteed to find a proof!!!



Group work!

Problem 1: Prove that there exists a positive integer that is equal to the sum of all positive integers not exceeding it. Is your proof constructive or non-constructive?

Problem 2: Prove that there is no positive integer n such that $n^2 + n^3 = 100$.

Problem 3: Use proof by cases to show that $\min(a, \min(b, c)) = \min(\min(a, b), c)$ whenever a , b , and c are real numbers.



That's it for proofs!

Well, not really...

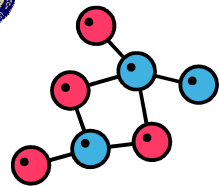


Throughout the remainder of this course, we will **repeatedly** use the proof skills that we've acquired

Our existing proof techniques (as well as a few more that we'll pick up along the way) will help us gain a deeper understanding of the mathematical foundations of other sub-areas of computer science



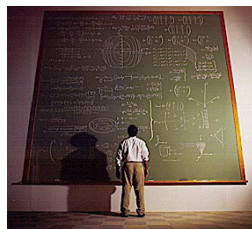
A retrospective



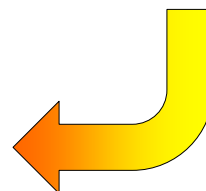
Representation



Formal proof,
equivalence, and
derivation



Informal proof,
proof strategies





Final Thoughts

- Proving theorems is not always straightforward
- Having several **proof strategies** at your disposal will make a huge difference in your success rate!
- We are “done” with our intro to logic and proofs



EXTRA SLIDES

Example: Prove that if x and y are real numbers, then $|x| + |y| \geq |x + y|$.



Proof:

Case (i): Assume that x and y are both non-negative. In this case $|x| + |y| = x + y = |x + y|$.

Case (ii): Assume that x and y are both negative. In this case $|x| + |y| = -x + -y = -(x + y) = |x + y|$.

Case (iii):

- Assume that $x \geq 0$ and $y < 0$.
- Note that $|x| + |y| = x + (-y)$.
- If $x > |y|$, then $|x + y| = x + y$. Since $-y > y$, we have that $x + -y > x + y$, so $|x| + |y| > |x + y|$.
- If $x < |y|$, then $|x + y| = -(x + y) = -x + (-y)$. Since $-x < x$, we have that $x + (-y) > -x + (-y)$, so $|x| + |y| > |x + y|$.

Case (iv): Same as case (iii).

Since we have proven the claim in all possible cases, we have proven that $|x| + |y| \geq |x + y|$ for all real numbers x and y . \square

Prove that for any two distinct positive real numbers that $2xy/(x+y) < \sqrt{xy}$



Proof: Note that if we multiply the inequality

$$2xy/(x+y) < \sqrt{xy}$$

by the quantity $(x+y)/(2\sqrt{xy})$ on both sides, we obtain the inequality

$$\sqrt{xy} < (x+y)/2$$

Since we proved earlier in lecture that $\sqrt{xy} < (x+y)/2$ for any distinct positive real numbers, and this inequality is equivalent to $2xy/(x+y) < \sqrt{xy}$, we have proven our claim. \square