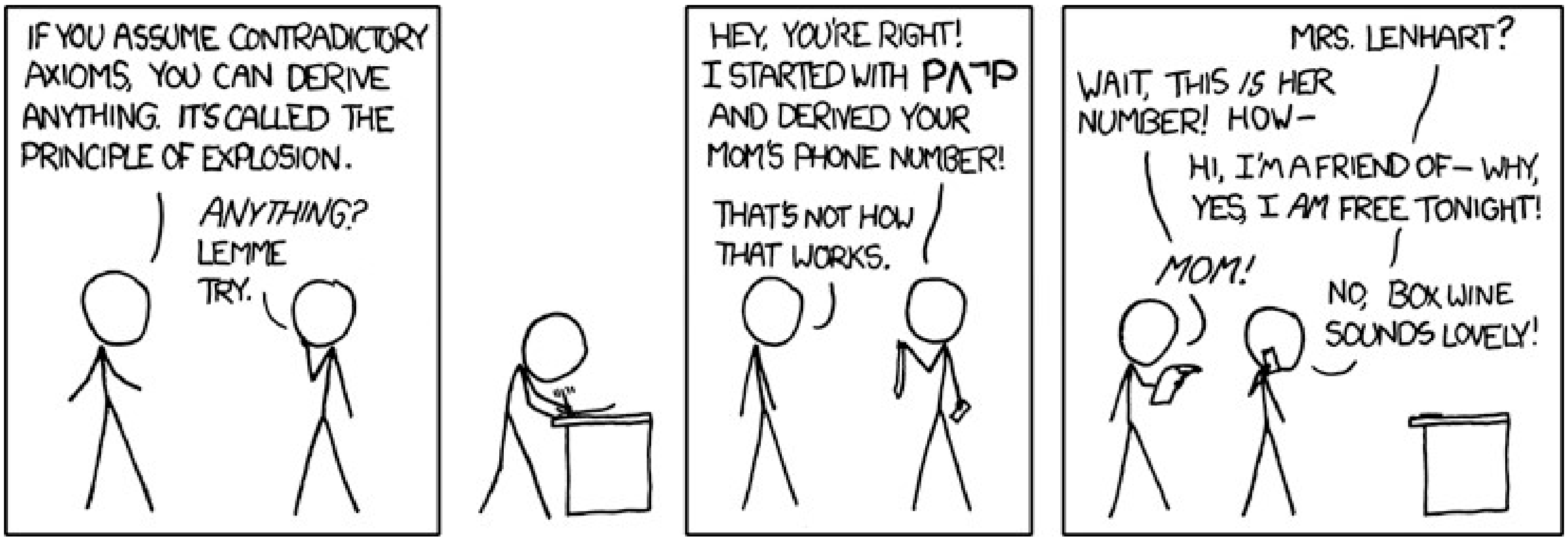



# Predicate Logic, Direct Proofs

CSE 311
Lecture 6

# Proof Strategy: Direct Proof

# Direct Proof

- Direct proof is one strategy for proving statements of the form
- $\forall x[P(x) \rightarrow Q(x)]$

# Direct Proof Template

**Prove:** $\forall x\big(\text{Even}(x) \rightarrow \text{Even}(x^2)\big)$

| | |
|---|---|
| Declare an arbitrary variable for each ∀. | Let $x$ be an arbitrary integer. |
| Assume the left side of the implication. | Suppose that $x$ is even. |
| Unroll the predicate definitions. | Then by definition of even, there exists some integer $k$ such that $x = 2k$. |
| Manipulate towards the goal. | Squaring both sides, we see that: $x^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$ |
| Reroll definitions into the right side of the implication. | Because $k$ is an integer, then $2k^2$ is also an integer. So $x^2$ is two times an integer. So by definition of even, $x^2$ is even. |
| Conclude that you have proved the claim. | Since $x$ was an arbitrary integer, we can conclude that for all integers $x$, if $x$ is even then $x^2$ is even. |

# Another Direct Proof

- Prove: "The product of two odd integers is odd."

- What's the claim in logic?
- $\forall x \forall y \left( \left( \text{Odd}(x) \wedge \text{Odd}(y) \right) \rightarrow \text{Odd}(xy) \right)$

- How would we prove this claim?

Direct Proof. In particular, we'll let $x, y$ be arbitrary integers. We'll suppose $x, y$ are odd. We'll show that $x \cdot y$ is odd.

# Another Direct Proof

Definitions
$\mathrm{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

- Prove: "The product of two odd integers is odd."

$$\forall x \forall y \left( \left( \mathrm{Odd}(x) \wedge \mathrm{Odd}(y) \right) \rightarrow \mathrm{Odd}(xy) \right)$$

Let $x$ and $y$ be arbitrary integers. Suppose that $x$ and $y$ are odd. Then by definition of odd, there exists some integer $k$ such that $x = 2k + 1$, and some integer $j$ such that $y = 2j + 1$.

Then multiplying $x$ and $y$, we can see that:

$$xy = (2k + 1) \cdot (2j + 1) = 4kj + 2j + 2k + 1 = 2(2kj + j + k) + 1$$

Since $k, j$ are integers, $2kj + j + k$ is an integer. So by definition of odd, $xy$ is odd. Since $x, y$ were arbitrary, we have shown that the product of two odd integers is odd.

# A note on Domain of Discourse

"The product of two odd integers is odd."

Domain: Integers

Translation:

$\forall x \forall y \left( \left( \mathrm{Odd}(x) \wedge \mathrm{Odd}(y) \right) \rightarrow \mathrm{Odd}(xy) \right)$

Proof Outline:

Let $x$ and $y$ be arbitrary integers.

Suppose $x$ and $y$ are odd.

Show $xy$ is odd.

Domain: Odd Integers

Translation:

$\forall x \forall y \left( \mathrm{Odd}(xy) \right)$

Proof Outline:

Let $x$ and $y$ be arbitrary odd integers.

Show $xy$ is odd.

# Square

- Definition:
- An integer $x$ is square iff there exists an integer $k$ such that $x = k^2$.

- $\mathrm{Square}(x) \coloneqq \exists k\ (x = k^2)$

# Yet Another Direct Proof

Definitions
$\text{Square}(x) := \exists k\ (x = k^2)$

Prove: The product of two square integers is square.

What's the claim in logic?

$$\forall n \forall m \left( \left( \text{Square}(n) \land \text{Square}(m) \right) \rightarrow \text{Square}(nm) \right)$$

Prove this claim.

# Yet Another Direct Proof

<u>Definitions</u>
$\text{Square}(x) \coloneqq \exists k\ (x = k^2)$

Prove: "The product of two square integers is square."

$$\forall n \forall m \Big( \big(\text{Square}(n) \land \text{Square}(m)\big) \to \text{Square}(nm) \Big)$$

Let $n$ and $m$ be arbitrary integers. Suppose that $n$ and $m$ are square. Then by definition of square, $n = k^2$ for some integer $k$, and $m = j^2$ for some integer $j$.

Then multiplying $n$ and $m$, we can see:

$$nm = k^2 \cdot j^2 = (kj)^2$$

Since $k$ and $j$ are integers, $kj$ is an integer. So by definition of square, $nm$ is square. Since $n$ and $m$ were arbitrary, we have shown that the product of two square integers is square.

# Proof Strategy: Contrapositive

# Proof by Contrapositive

- Proof by contrapositive is another strategy for proving statements of the
- form $\forall x\big(\mathrm{P}(x) \rightarrow \mathrm{Q}(x)\big)$.

- The strategy is to prove the contrapositive, i.e. prove $\forall x\big(\neg\mathrm{Q}(x) \rightarrow \neg\mathrm{P}(x)\big)$

# Proof by Contrapositive

Definitions
$\mathrm{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

- Prove: For an integer $x$, if $3x + 2$ is odd, then $x$ is odd.

- What's the claim in logic? $\forall x\big(\mathrm{Odd}(3x + 2) \rightarrow \mathrm{Odd}(x)\big)$

- Try to prove this claim with a direct proof.

Let $x$ be an arbitrary integer. Suppose that $3x + 2$ is odd. Then $3x + 2 = 2k + 1$ for some integer $k$. Subtracting both sides by 2, we have $3x = 2k - 1$. Then $x = \frac{2k-1}{3}$…?

Note: We actually *can* prove this directly. But it's much less obvious to see.

# Proof by Contrapositive

Definitions
$\mathrm{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

- Prove: For an integer $x$, if $3x + 2$ is odd, then $x$ is odd.

$$\forall x\big(\mathrm{Odd}(3x+2) \rightarrow \mathrm{Odd}(x)\big) \equiv \forall x\big(\mathrm{Even}(x) \rightarrow \mathrm{Even}(3x+2)\big)$$

We prove by contrapositive. Let $x$ be an arbitrary integer. Suppose that $x$ is even. Then by definition of even, $x = 2k$ for some integer $k$. Consider $3x + 2$:

$$3x + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$$

Since $k$ is an integer, $3k + 1$ is an integer. So $3x + 2$ is 2 times an integer. So by definition of even, $3x + 2$ is even. Since $x$ was arbitrary, we have shown that for all integers $x$, if $x$ is even then $3x + 2$ is even. Thus the contrapositive also holds: for all integers $x$, if $3x + 2$ is odd, then $x$ is odd.

# Proof by Contrapositive

- How do we identify *when* to use a direct proof vs. a proof by contrapositive?

- Try a direct proof first. If it seems challenging, then consider the contrapositive.

# Another Proof by Contrapositive

Definitions
$\text{Even}(x) \coloneqq \exists k(x = 2k)$

- Prove by Contrapositive: For an integer $n$, if $n^3$ is even, then $n$ is even.

$$\forall n\big(\text{Even}(n^3) \rightarrow \text{Even}(n)\big) \equiv \forall n\big(\text{Odd}(n) \rightarrow \text{Odd}(n^3)\big)$$

We prove by contrapositive. Let $n$ be an arbitrary integer. Suppose that $n$ is odd. Then by definition of odd, $n = 2k + 1$ for some integer $k$. Consider $n^3$:

$$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$$

Since $k$ is an integer, $4k^3 + 6k^2 + 3k$ is an integer. Thus by definition of odd, $n^3$ is odd. Since $n$ was arbitrary, we have shown that for all integers $n$, if $n$ is odd then $n^3$ is odd. Thus the contrapositive also holds: for all integers $n$, if $n^3$ is even, then $n$ is even.

# Remark: Proof by Contrapositive

- Just like we can show $p \to q$ is true by using a direct proof of $\neg q \to \neg p$, we can use our other logical equivalences.
-

Suppose for example the original claim is of the form $p \to (q \vee r)$. Then the contrapositive would be:

$$\begin{aligned} p \to (q \vee r) &\equiv \neg(q \vee r) \to \neg p \\ &\equiv (\neg q \wedge \neg r) \to \neg p \end{aligned}$$

So the proof by contrapositive would be of the form:

Suppose $\neg q$ and $\neg r$. Try to show $\neg p$.

# Proof Strategy: Biconditional

# Proof of a Biconditional

- Recall that biconditionals are statements of the form:

$\forall x\big(\mathrm{P}(x) \leftrightarrow \mathrm{Q}(x)\big)$

- The strategy is to prove such statements is to prove an implication in both directions. I.e. prove $\forall x\big(\mathrm{P}(x) \rightarrow \mathrm{Q}(x)\big) \wedge \forall x\big(\mathrm{Q}(x) \rightarrow \mathrm{P}(x)\big)$.

# Proof of a Biconditional

Prove: For an integer $x$, $2x + 3 = 15$ if and only if $x = 6$.

$\Rightarrow$ Let $x$ be an arbitrary integer. Suppose $2x + 3 = 15$. Then $2x = 12$. Then $x = 6$. Since $x$ was arbitrary, for all integers $x$ if $2x + 3 = 15$ then $x = 6$.

$\Leftarrow$ Let $x$ be an arbitrary integer. Suppose $x = 6$. Then consider $2x + 3$:

$$2x + 3 = 2(6) + 3 = 12 + 3 = 15$$

Since $x$ was arbitrary, for all integers $x$ if $x = 6$ then $2x + 3 = 15$.

Therefore, we have shown that for an integer x, 2x + 3 = 15 iff x = 6

# Remark: Biconditional Proofs

- Each direction of the biconditional proof can use whichever proof type fits best (direct, contrapositive, etc.).

- Consider the claim: For an integer $n$, $3n + 3$ is odd iff $n$ is even.

$\Leftarrow$ Prove that $\forall n\big(\mathrm{Even}(n) \rightarrow \mathrm{Odd}(3n+3)\big)$. Use direct proof.

$\Rightarrow$ Prove that $\forall n\big(\mathrm{Odd}(3n+3) \rightarrow \mathrm{Even}(n)\big)$. Use contrapositive. I.e. prove that $\forall n\big(\mathrm{Odd}(n) \rightarrow \mathrm{Even}(3n+3)\big)$.

# Another Proof of a Biconditional

Definitions
$\text{Even}(x) \coloneqq \exists k(x = 2k)$
$\text{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

- Prove: For an integer $n$, $3n + 3$ is odd iff $n$ is even.

$\Leftarrow$ Let $n$ be an arbitrary integer. Suppose $n$ is even. Then by definition of even, $n = 2k$ for some integer $k$. Then consider $3n + 3$:

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

Since $k$ is an integer, $3k + 1$ is an integer. So $3n + 3$ is 2 times an integer plus 1. So by definition of odd, $3n + 3$ is odd. Since $n$ was arbitrary, this shows that for all integers $n$ if $n$ is even then $3n + 3$ is odd.

$\Rightarrow$ We prove by contrapositive. Let $n$ be an arbitrary integer. Suppose that $n$ is odd. Then by definition of odd, $n = 2k + 1$ for some integer $k$. Then consider $3n + 3$:

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

Since $k$ is an integer, $3k + 3$ is an integer. So $3n + 3$ is 2 times an integer. So by definition of even, $3n + 3$ is even. Since $n$ was arbitrary, this shows that for all integers $n$, if $n$ is odd then $3n + 3$ is even. Then the contrapositive also holds: for all integers $n$, if $3n + 3$ is odd then $n$ is even.

# Remark: Multiple Biconditionals

- Suppose you wanted to prove $p \leftrightarrow q \leftrightarrow r$.

- How many sub-proofs would you need?
- Could do every pair: $(p \rightarrow q) \wedge (q \rightarrow p) \wedge (q \rightarrow r) \wedge (r \rightarrow q) \wedge (p \rightarrow r) \wedge (r \rightarrow p)$
- But it turns out you only need 3. For instance, $(p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)$
- Any chain of conditional statements work so long as you can follow the chain of implications to get from any statement to any other.

# Proof Strategies So Far

- Direct Proof
- Proof by Contrapositive
- Proof of Biconditional
- Proof by Cases
- Proof of Existence
- Disproof

# Proof by Cases

# Warm Up: Shaking Hands

- Suppose there are six people in a room. Some of them shake hands. Consider the claim:

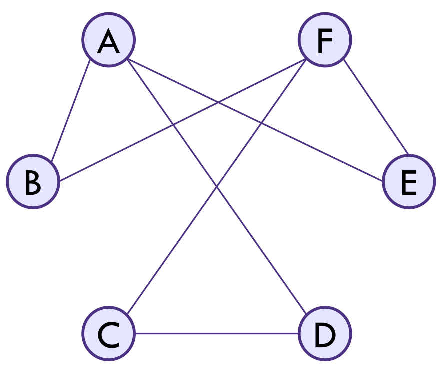
  - There are at least three people who all shook each other's hands, or three people such that no pair of them shook hands.

- Is it true?

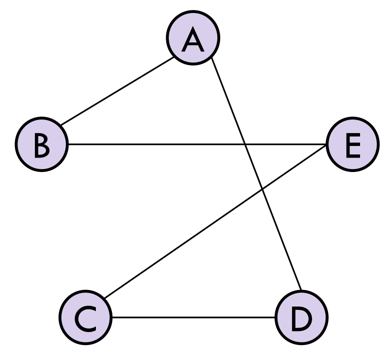
# Warm Up: Shaking Hands

- Suppose there are six people in a room. Some of them shake hands. Consider the claim:

  - There are at least three people who all shook each other's hands, or three people such that no pair of them shook hands.




Not obvious! Doesn't work with 5 people.



- There are six people in a room. Prove that there are at least three people who all shook each other's hands, or three people such that no pair of them shook hands.

Choose one person, call them $A$. Note that $A$ has 5 people around them in the room.

- Case 1: $A$ shook 3 or more of the others' hands. Pick three of them, call them $B$,$C$,$D$. Then if any of $B$, $C$ or $D$ shook hands with each other, we have 3 people who have all shaken hands. If none of $B$, $C$, or $D$ shook hands with each other, then we have 3 people who have not shaken any hands.
- Case 2: $A$ shook 2 or fewer of the others' hands. Pick three of the people $A$ did not shake hands with, and call them $X$, $Y$, $Z$. Then if any of $X$, $Y$, $Z$ also did not shake with each other, we have 3 people who have all not shaken hands. If all of $X$, $Y$, or $Z$ shook hands with each other, then we have 3 people who have all shaken hands.

# Proof by Cases

- Proof by cases is the strategy of:

1. Breaking your assumption(s) into smaller cases.
   Be careful to make sure that your cases cover all of the possible scenarios. It's ok if they have overlap though.

2. Proving that the claim holds in all of these cases.
   Formally: $(P \lor Q) \rightarrow R \equiv (P \rightarrow R) \land (Q \rightarrow R)$.

# 5 numbers: Proof by Cases

- Suppose that $x_1, \dots, x_5$ are real numbers such that $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ and $x_1 + x_2 + x_3 + x_4 + x_5 = 50$. Prove that $x_1 + x_2 \leq 20$.

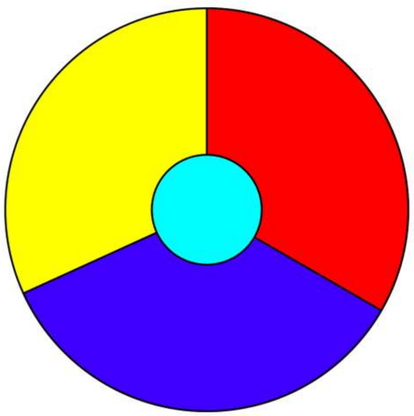
Let $x_1, x_2, x_3, x_4, x_5$ be arbitrary real numbers such that $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ and $x_1 + x_2 + x_3 + x_4 + x_5 = 50$.

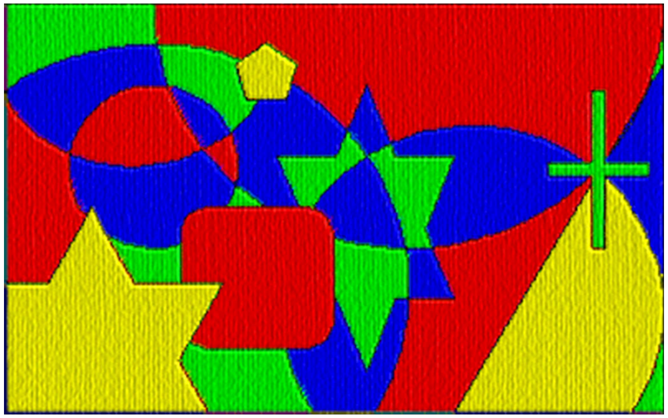
Case 1: $x_2 \leq 10$. Then since $x_1 \leq x_2, x_1 \leq 10$. So $x_1 + x_2 \leq 20$, as desired.
Case 2: $x_2 > 10$. Then since $x_3, x_4, x_5 \geq x_2$, we have that $x_3 > 10, x_4 > 10, x_5 > 10$. So $x_3 + x_4 + x_5 > 30$. Thus $x_1 + x_2 < 20$, as desired.

- Since $x_1, \dots, x_5$ were arbitrary, the claim holds.

# Four Color Theorem: Proof by Cases

- **Theorem** (Four Color): Any plane surface with regions in it can be colored in four colors or less. Two regions that have a common border must not get the same color.





- The first proof had 1,936 cases. The shortest known proof today has over 600 cases.

# Existence Proof

# Existence Proof

- To prove $\exists x \, \mathrm{P}(x)$, we give one example of $x$ in the domain that makes $\mathrm{P}(x)$ true.

# Existence Proof

- There is some prime number $p$ such that $p + 6$ and $p + 8$ are also prime.

- $\exists p\big(\mathrm{Prime}(p) \wedge \mathrm{Prime}(p + 6) \wedge \mathrm{Prime}(p + 8)\big)$

- Consider $p = 5$. Then $p + 6 = 11$ is also prime, as is $p + 8 = 13$.

# When are Existence Proofs often helpful?

- To disprove a claim, we prove the negation of the claim.

- Existence proofs are often helpful to disprove “for all” claims.

- Another term for this is giving a counterexample.

# Counterexamples

- A single example can't *prove* a ∀ statement.

- A single counterexample can *disprove* a ∀ statement.
- For example, to disprove "all professors like pizza", you must find a professor who does not like pizza.

- In formal logic:
- $\neg\forall x\big(\mathrm{P}(x) \rightarrow \mathrm{Q}(x)\big) \equiv \neg\forall x\big(\neg\mathrm{P}(x) \vee \mathrm{Q}(x)\big)$ Law of Implication
- $\equiv \exists x\neg\big(\neg\mathrm{P}(x) \vee \mathrm{Q}(x)\big)$ DeMorgan's Law for Quantifiers
- $\equiv \exists x\big(\mathrm{P}(x) \wedge \neg\mathrm{Q}(x)\big)$ DeMorgan's Law

# Counterexamples

For all real numbers $a, b, c,$ if $|a + c| = |b + c|$, then $|a| = |b|$.

This claim is false. Disprove!

Consider $a = -6, b = 4, c = 1$. Certainly $|a| \neq |b|$. Observe that:
$|a + c| = |-6 + 1| = |-5| = 5$

$|b + c| = |4 + 1| = |5| = 5$

So this is a counterexample to the claim.

# Counterexamples

You are given $1¢$, $5¢$, $10¢$, $12¢$ and $25¢$ coins.

Your boss says to make change with the least amount of coins, first use as many $25¢$ coins that will fit, then $12¢$ coins, then $10¢$, then $5¢$, then $1¢$ cent.

Disprove this with a counterexample.

Consider making $21¢$ of change. Your boss's strategy would involve using $12¢$, $5¢$, $1¢$, $1¢$, $1¢$, $1¢$ coins, i.e. 6 coins. However you can make this much change using only 3 coins: $10¢$, $10¢$, $1¢$.

# Prove or Disprove

# Prove or Disprove

- In practice, we don't usually know if a claim is true or false beforehand
- We want to prove the statement if it's true, and disprove it if it's false.
- Strategy:
    - Play around with many examples in an attempt to show that the claim is false
    - If the claim is false, hopefully you'll find a counterexample
    - If the claim is true, you'll gain intuition for why from the examples

# Prove or Disprove

Identify if the following claims are true or false, and then prove or disprove.

1. For all positive integers $n$, $n^2 + 3n + 1$ is always prime.
   False: e.g. $n = 6$ gives $36 + 18 + 1 = 55$.

2. For all positive integers $n$, the sum $1 + 2 + \cdots + n$ is equal to $\frac{n(n+1)}{2}$.
   True. Hint to prove: regroup $1 + 2 + \cdots + n - 1 + n$ into pairs $(1 + n) + (2 + (n - 1)) + \cdots$

3. For every real number $n$, $n^2 \geq n$.
   False: e.g. $n = \frac{1}{2}$, since $\frac{1}{4} < \frac{1}{2}$.

4. For an integer $n$, $3n^2 + n + 10$ is always even.
   True. Hint to prove: break into the cases that $n$ is even and $n$ is false.