CSCI 2200
FOUNDATIONS OF COMPUTER SCIENCE

David Goldschmidt
goldsd3@rpi.edu
Fall 2022

A DIRECT PROOF OF AN IMPLICATION

Given a claim in the form $p \rightarrow q$, we can consider using a *direct proof* as follows…

Proof. We prove the implication using a direct proof.

1. Start by assuming that the statement claimed in p is true
2. Restate your assumption in mathematical terms, as necessary
3. Use mathematical and logical derivations to relate your above assumptions to q
4. Argue that you have shown that q must be true
5. End by concluding that q is true ■

A DIRECT PROOF OF AN IMPLICATION – EXAMPLE

Prove the following claim: if $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$

Proof. We prove the implication using a direct proof.

1. Assume that $x, y \in \mathbb{Q}$, i.e., x and y are rational.
2. Then, by definition, there are integers a, c and natural numbers b, d such that $x = a/b$ and $y = c/d$.
3. Then $x + y = (ad + bc)/bd$.
4. Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, $(ad + bc)/bd$ is rational (by definition).
5. Thus, we conclude from steps 3 and 4 that $x + y \in \mathbb{Q}$. ■

We made no assumptions about x…

…therefore, we proved $\forall x : P(x)$

PROVE USING A DIRECT PROOF…

Given $x \in \mathbb{R}$; claim $P(x)$: if $\underbrace{4^x - 1 \text{ is divisible by } 3}_{p}$, then $\underbrace{4^{x+1} - 1 \text{ is divisible by } 3}_{q}$

Proof. We prove the claim using a direct proof.

1. Assume that p is true, i.e., $4^x - 1$ is divisible by 3.
2. This means that $4^x - 1 = 3k$ for an integer k; from this, $4^x = 3k + 1$.
3. Since $4^{x+1} = 4 \cdot 4^x$, we have $4^{x+1} = 4 \cdot (3k + 1) = 12k + 4$.

   Therefore, $4^{x+1} - 1 = 12k + 3 = 3 \cdot (4k + 1)$, which is a multiple of 3.
4. Since $4^{x+1} - 1$ is a multiple of 3, we have shown that $4^{x+1} - 1$ is divisible by 3.
5. Therefore, the statement claimed in q is true. ∎

DISPROVING AN IMPLICATION

To prove that an implication is false, we need only find one counter-example

claim $P(x)$: if $\underbrace{x^2 > y^2}_{p}$, then $\underbrace{x > y}_{q}$

p	q	$p \rightarrow q$
F	**F**	**T**
F	**T**	**T**
T	**F**	**F**
T	**T**	**T**

One counter-example is $x = -10$ and $y = 9$

A counter-example shows p to be **T** and q to be **F**…

…which cannot occur for $p \rightarrow q$

Therefore, one counter-example is sufficient to disprove the implication

PROVING AN IMPLICATION

Note that we only have proven that the implication is true!

…we have said nothing about n here

Can we prove the **implication** that if n^2 is even, n is even ~~(for $n \in \mathbb{Z}$)~~?

p : n^2 is even

q : n is even

$p \to q$: if n^2 is even, n is even

p	q	$p \to q$
F	**F**	**T**
F	**T**	**T**
T	**F**	**F**
T	**T**	**T**

Can we prove that the **F** row **cannot** occur?

In this row, q is **F**, so n is odd, i.e., $n = 2k + 1$

From this, $n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$, which means n^2 is odd, i.e., p must be **F**

The highlighted row **cannot** occur—therefore, $p \to q$ is always **T**

A CONTRAPOSITION PROOF OF AN IMPLICATION

Given a claim in the form $p \to q$, we can consider using *contraposition* as follows…

Proof. We prove the implication using contraposition.

1. Start by assuming that the statement claimed in q is false
2. Restate your assumption in mathematical terms, as necessary
3. Use mathematical and logical derivations to relate your above assumptions to p
4. Argue that you have shown that p must be false
5. End by concluding that p is false ■

Note that this is still a direct proof…

PROOF BY CONTRAPOSITION – EXAMPLE

Note that this is still a direct proof…

…because we prove $\neg q \rightarrow \neg p$

Given claim $P(x)$: if $\underbrace{x^2 \text{ is even}}_{p}$, then $\underbrace{x \text{ is even}}_{q}$

Proof. We prove the claim using contraposition.

1. Assume that x is odd (i.e., that q is false).
2. Since x is odd, $x = 2k + 1$ for some $k \in \mathbb{Z}$.
3. Then, $x^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$, which is 1 plus an even number.
4. Since x^2 is 1 plus a multiple of 2, we know x^2 is odd (i.e., p must be false).
5. Thus, we have shown that x^2 is odd (i.e., that p is false when q is false) and $P(x)$ is true. ∎

PROOF BY CONTRAPOSITION – EXAMPLE

Note that this is still a direct proof…

…because we prove $\neg q \rightarrow \neg p$

Given claim $P(x)$: if $\underbrace{x^2 \text{ is even}}_{p}$, then $\underbrace{x \text{ is even}}_{q}$

Proof. We prove the claim using contraposition.

Assume that x is odd.

Since x is odd, $x = 2k + 1$ for some $k \in \mathbb{Z}$.

Then, $x^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$, which is 1 plus an even number.

Since x^2 is 1 plus a multiple of 2, we know x^2 is odd.

Thus, we have shown that x^2 is odd and $P(x)$ is true. ∎

EQUIVALENCE AND CONTRAPOSITION

Since $\neg q \rightarrow \neg p$ and $p \rightarrow q$ are logically equivalent, proving one proves the other!

From our truth tables showing logical equivalence…

$$p \rightarrow q \overset{\text{eqv}}{\equiv} \neg p \vee q \overset{\text{eqv}}{\equiv} \neg q \rightarrow \neg p$$

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \vee q$	$\neg q \rightarrow \neg p$
F	F	T	T	T	T	T
F	T	T	F	T	T	T
T	F	F	T	F	F	F
T	T	F	F	T	T	T

equivalent statements

PROOF BY CONTRAPOSITION – EXAMPLE

Given claim Q(x,y): if $\underbrace{x, y > 0 \text{ and } x{\cdot}y > 100}_{p}$, then $\underbrace{x > 10 \text{ or } y > 10}_{q}$

The contrapositive statement is…

…if $x \leq 10$ and $y \leq 10$, then one of x,y is not positive or $x{\cdot}y \leq 100$

Proof. We prove the claim using contraposition.

Assume that $x \leq 10$ and $y \leq 10$.

Case 1. Either x or y is not positive.

Case 2. Both x and y are positive, so under our assumption, we have $0 < x, y \leq 10$. In this case, $x{\cdot}y \leq (10 \times 10)$ or simply $x{\cdot}y \leq 100$.

Thus, we have shown that claim Q(x,y) is true. ■

EQUIVALENCE IS STRONGER THAN IMPLICATION

Claims sometimes involve equivalence between propositions p and q…

p IF AND ONLY IF q e.g., sets A and B are equal IF AND ONLY IF both $A \subseteq B$ and $B \subseteq A$

In such compound statements, either p and q are both true or they are both false…

$$(p \to q) \land (q \to p) \overset{\text{eqv}}{\equiv} p \leftrightarrow q$$

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$
F	F	T	T	T
F	T	T	F	F
T	F	F	T	F
T	T	T	T	T

prove each of these separately…

How do we prove an IF AND ONLY IF claim?

We prove both implications…

PROVING EQUIVALENCE (IFF) – EXAMPLE

Given claim $P(x)$: $\underbrace{\text{integer } x \text{ is divisible by } 3}_{p}$ IF AND ONLY IF $\underbrace{x^2 \text{ is divisible by } 3}_{q}$

Proof. We prove the claim by proving each implication (i.e., $p \to q$ and $q \to p$).

(i) We use a direct proof to prove that if x is divisible by 3, then x^2 is divisible by 3.

Assume x is divisible by 3, so $x = 3k$ for some $k \in \mathbb{Z}$.

Squaring both sides, $x^2 = 9k^2 = 3{\cdot}(3k^2)$, which is also a multiple of 3.

Thus, x^2 is divisible by 3, as was to be shown.

PROVING EQUIVALENCE (IFF) – EXAMPLE

Given claim $P(x)$: $\underbrace{\text{integer } x \text{ is divisible by } 3}_{p}$ IF AND ONLY IF $\underbrace{x^2 \text{ is divisible by } 3}_{q}$

(ii) We use contraposition to prove that if x^2 is divisible by 3, then x is divisible by 3.

Assume x is not divisible by 3. There are two cases for x…

Case 1. $x = 3k + 1$.

Case 2. $x = 3k + 2$.

PROVING EQUIVALENCE (IFF) – EXAMPLE

Given claim $P(x)$: $\underbrace{\text{integer } x \text{ is divisible by } 3}_{p}$ IF AND ONLY IF $\underbrace{x^2 \text{ is divisible by } 3}_{q}$

(ii) We use contraposition to prove that if x^2 is divisible by 3, then x is divisible by 3.

Assume x is not divisible by 3. There are two cases for x…

Case 1. $x = 3k + 1$. Here, $x^2 = 3k(3k + 2) + 1$, so 1 more than a multiple of 3.

Case 2. $x = 3k + 2$. Here, $x^2 = 3(3k^2 + 4k + 1) + 1$, so also 1 more than a multiple of 3.

In both cases, we have shown that x^2 is not divisible by 3, as was to be shown. ■

Given claim $P(x)$: integer x is divisible by 3 IF AND ONLY IF x^2 is divisible by 3

Proof. We prove the claim by proving each implication.

(i) We use a direct proof to prove that if x is divisible by 3, then x^2 is divisible by 3.

Assume x is divisible by 3, so $x = 3k$ for some $k \in \mathbb{Z}$.

Squaring both sides, $x^2 = 9k^2 = 3 \cdot (3k^2)$, which is also a multiple of 3.

Thus, x^2 is divisible by 3, as was to be shown.

(ii) We use contraposition to prove that if x^2 is divisible by 3, then x is divisible by 3.

Assume x is <u>not</u> divisible by 3. There are two cases for x…

Case 1. $x = 3k + 1$. Here, $x^2 = 3k(3k + 2) + 1$, so 1 more than a multiple of 3.

Case 2. $x = 3k + 2$. Here, $x^2 = 3(3k^2 + 4k + 1) + 1$,
so also 1 more than a multiple of 3.

In both cases, we have shown that x^2 is <u>not</u> divisible by 3, as was to be shown. ■

USING EQUIVALENCE FOR DEFINITIONS

The IF AND ONLY IF connector is often used for definitions…

Set Equality (for two sets *A* and *B*):
$A = B$ IF AND ONLY IF both $A \subseteq B$ and $B \subseteq A$

Prove these equivalences…

Parallel Line Segments
Two line segments on a plane are parallel to one another
IF AND ONLY IF
extending both line segments to infinity in both directions causes
no intersections between the two lines

PROOF BY CONTRADICTION

Given any claim p, we can always use proof by *contradiction* to prove p…

Proof. We prove the claim by contradiction.

1. Start by assuming that the statement claimed in p is false.
2. Restate your assumption in mathematical terms, as necessary.
3. Use mathematical and logical derivations to derive a conflicting truth, i.e., a contradiction that must be false.
4. End by concluding that the assumption in step 1 is false, so p must be true. ■

PROOF BY CONTRADICTION – EXAMPLE

Given a and b are integers. Prove the claim p that $a^2 - 4b \neq 2$.

Proof. We prove the claim by contradiction.

Assume that $a^2 - 4b = 2$ (i.e., that p is false).

Rearrange to get $a^2 = 4b + 2$, then $a^2 = 2(2b + 1)$, which means a^2 is even.

If a^2 is even, then a is even, which means $a = 2k$ for integer k.

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

Whoops! The LHS is even and the RHS is odd—conflicting truths—a contradiction!

Thus, we have proven that $a^2 - 4b \neq 2$ (i.e., p must be true). ■

PROOF BY CONTRADICTION – EXAMPLE

Given a and b are integers. Prove the claim p that $a^2 - 4b \neq 2$.

Proof. We prove the claim by contradiction.

Assume that $a^2 - 4b = 2$.

Rearrange to get $a^2 = 4b + 2$, then $a^2 = 2(2b + 1)$, which means a^2 is even.

If a^2 is even, then a is even, which means $a = 2k$ for integer k.

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

The LHS is even and the RHS is odd—a contradiction!

Thus, we have proven that $a^2 - 4b \neq 2$. ■

PROOF BY CONTRADICTION

Can you prove the following claims by contradiction?

Claim 1. Let $m, n \in \mathbb{Z}$. Prove that $21m + 9n \neq 1$.

Claim 2. Let x, y be positive real numbers. Prove that $x + y \geq 2\sqrt{xy}$

Claim 3. Let $m, n \in \mathbb{Z}$ with $m^2 + n^2$ divisible by 4. Then m and n are not both odd.

Proof by contradiction is powerful—and the starting assumption gives you a lot to work with!

WHICH PROOF TECHNIQUE SHOULD YOU USE?

Proof Method	Situation
Direct proof	Appears clear how result follows from assumption
Contraposition	Appears clear how if result is **F**, the assumption will be **F**
Show a counter-example	Disprove an implication
Show an example	Prove something exists $\exists$
Contradiction	Prove something does not exist
Contradiction	Prove something is unique
Show for general object	Prove something is true for <u>all</u> objects
Show a counter-example	Disprove something is true for <u>all</u> objects

EXERCISE 4.8

Determine which proof technique to use for each claim…

…you do no need to prove each claim yet

(a) There is no real x for which $x^2 < 0$

(b) If n^2 is odd, then n is odd

(c) If n is odd, then n^2 is odd

(d) Not every natural number is a square

(e) The product of two rational numbers is rational

(f) The product of two odd numbers can never be even

(g) There does <u>not</u> exist a rational number equal to $\sqrt{6}$

(h) At least one number in a set of numbers is as large (or larger) than the average

WHAT NEXT…?

Problem Set 2 will be posted by Monday—due at recitations on September 21

Homework 2 will be posted on Tuesday—due by 11:59PM on September 29

Problem Set 3 will be posted by next Monday—due at recitations on September 28

Email me extra-time accommodations ASAP

Practice! Tinker! Practice! Tinker! Practice! Tinker! Practice! Tinker! Practice