# Proofs

# Reading

- Malik Magdon-Ismail. Discrete Mathematics and Computing.
  - Chapter 4

# Today

- Proving “IF …, THEN …”
- Proof patterns
  - Direct proof
  - Proof by contraposition
  - Proof by contradiction
- Proofs about sets

# Implications: reasoning in the absence of facts

- Reasoning:
  - It rained last night (fact); the grass is wet ("deduced").
- Reasoning in the absence of facts:
  - IF it rained last night, THEN the grass is wet
- We like to prove such statements even though, at this moment, it is not much use
  - Later, you may learn that it rained last night and infer the grass is wet
- More relevant example from CS:

  IF we can quickly find the largest friend-clique in a friendship network,

  THEN we can quickly determine how to assign non-conflicting frequencies to radio stations using a minimum number of frequencies

# Implications, cont'd

- Mathematical example, quadratic formula:
- IF $ax^2 + bx + c = 0$ AND $a \neq 0$, THEN

$$x = \frac{-b+\sqrt{b^2-4ac}}{2a} \text{ or } x = \frac{-b-\sqrt{b^2-4ac}}{2a}$$

# Proving an implication

- IF $x$ and $y$ are rational, THEN $x + y$ is rational
  – What are the predicates $p$ and $q$?

$$p = x \text{ and } y \text{ are rational}$$
$$q = x + y \text{ is rational}$$

  – Formally, we write this as

$$\forall (x, y) \in \mathbb{Q}^2 : (x + y) \in \mathbb{Q}$$

  – i.e., $P(x, y) = (x + y) \in \mathbb{Q}$

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| F | F | T |
| F | T | T |
| T | F | F |
| T | T | T |

- *Proof:*
  – We must show that the row $p = T, q = F$ cannot happen
  – Let's see what happens if $p = T$, i.e., $(x, y) \in \mathbb{Q}^2$

$x = \frac{a}{b}, y = \frac{c}{d}$, where $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{N}$

  - What is $x + y$?

$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Is that number rational?

  – Yes, $ad + bc \in \mathbb{Z}, bd \in \mathbb{N}$

  - i.e., $q = T$ (the row $p = T, q = F$ cannot happen!) QED.

# Template for direct proof of an implication $p \to q$

Rensselaer

- *Proof*. We prove the implication using a direct proof.
  1. Start by assuming that the statement claimed in $p$ is T
  2. Restate your assumption in mathematical terms
  3. Use mathematical and logical derivations to relate your assumption to $q$
  4. Argue that you have shown that $q$ must be T
  5. End by concluding that $q$ is T

# Formal proof example

- *Theorem:* If $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$
- *Proof*. We prove the theorem using a direct proof.
  1. Assume that $x, y \in \mathbb{Q}$, that is $x$ and $y$ are rational
  2. Then there are integers $a, c$ and natural numbers $b, d$ such that $x = a/b$ and $y = c/d$
     - (because this is what it means for $x$ and $y$ to be rational)
  3. Then $x + y = (ad + bc)/bd$
     - (high-school algebra)
  4. Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, $(ad + bc)/bd$ is rational
  5. Thus, we conclude (from steps 3 and 4) that $x + y \in \mathbb{Q}$

# A proof is a mathematical essay

Rensselaer

- A proof must be well written
  - The goal of a proof is to convince a reader of a theorem
  - A badly written proof that leaves a reader with some doubts has failed

# Steps for Writing Readable Proofs

1. **State your strategy**.
   - Start with proof type.
   - Structure long proofs into parts and tie up the parts at the end.
   - Readers must have no doubts.
2. **The proof should have a logical flow**.
   - It is difficult to follow movies that jump between story lines or back and forth in time.
   - A reader follows a proof linearly, from beginning to end.
3. **Keep it simple**.
   - Make the idea at the heart of your proof clear.
   - Avoid excessive symbols and unnecessary notation.
4. **Justify your steps**.
   - The reader must have no doubts.
   - Avoid phrases like "It's obvious that . . . " If it is so obvious, explain.
5. **End your proof.** Explain why what you set out to show is true.
6. **Read your proof.** Finally, check correctness; edit; simplify

# Example: direct proof

- *Theorem*: Let $x$ be any real number, i.e., $x \in \mathbb{R}$. IF $4^x - 1$ is divisible by 3, THEN $4^{x+1} - 1$ is divisible by 3.
- What are the predicates $p$ and $q$?

$$p = 4^x - 1 \text{ is divisible by 3}$$
$$q = 4^{x+1} - 1 \text{ is divisible by 3}$$

# Example: direct proof

- *Theorem*: Let $x$ be any real number, i.e., $x \in \mathbb{R}$. IF $4^x - 1$ is divisible by 3, THEN $4^{x+1} - 1$ is divisible by 3.
- *Proof*: We prove the claim using a direct proof.
  1. Assume that $p$ is T, that is $4^x - 1$ is divisible by 3.
  2. This means that $4^x - 1 = 3k$ for an integer $k$, or that
     $$4^x = 3k + 1$$
  3. Observe that $4^{x+1} = 4 \times 4^x$. Using $4^x = 3k + 1$,
     $$4^{x+1} = 4(3k + 1) = 12k + 4$$
  4. Therefore
     $$\begin{aligned} 4^{x+1} - 1 &= 12k + 3 \\ &= 3(4k + 1) \end{aligned}$$
     is a multiple of 3 ($4k + 1$ is an integer)
  5. Since $4^{x+1} - 1$ is a multiple of 3, we have shown that $4^{x+1} - 1$ is divisible by 3
  6. Therefore, the statement claimed in $q$ is T
- **Question:** Is $4^x - 1$ divisible by 3?

# We made no assumptions about $x$!

- $P(x)$: "IF $4^x - 1$ is divisible by 3, THEN $4^{x+1} - 1$ is divisible by 3"
- Since we made no assumptions about $x$, we proved:

$$\forall x \in \mathbb{R}: P(x)$$

- **Exercise**:
- *Prove*: For all pairs of odd integers $m, n$, the sum $m + n$ is an even integer

~~1. $m = 2k + 1$ for some $k \in \mathbb{Z}$~~

~~2. $n = 2p + 1$ for some $p \in \mathbb{Z}$~~

~~3. $m + n = 2(p + k + 1)$~~

~~4. Why is this sufficient proof?~~

# Disproving an Implication

Rensselaer

- IF $x^2 > y^2$, THEN $x > y$
  - What are $p$ and $q$?

$$p = (x^2 > y^2)$$
$$q = (x > y)$$

- Is this statement true or false?
- False!
- Counter example: $x = -8, y = -4$

$$p: 64 = x^2 > y^2 = 16$$
$$q: -8 = x < y = -4$$

- The row $p$ = T, $q$ = F has occurred!
- **A single counter-example suffices to disprove an implication**

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| F | F | T |
| F | T | T |
| T | F | F |
| T | T | T |

# Contraposition

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| F | F | T |
| F | T | T |
| T | F | F |
| T | T | T |

- IF $x^2$ is even, THEN $x$ is even
  - What are $p$ and $q$?

$$p = (x^2 \text{ is even})$$
$$q = (x \text{ is even})$$

- *Proof*: We must show that the row $p$ = T, $q$ = F can't happen
- Let us see what happens if $q$ = F
  - If $x$ is odd, $x = 2k + 1$
  - Then $x^2 = 4k^2 + 4k + 1$
  - i.e., $x^2 = 2(2k^2 + 2k) + 1$ ($x^2$ is odd!)
- That means $p$ is F
  - The row $p$ = T, $q$ = F *cannot* occur!
  - The implication is proved

# Template: Contraposition Proof of an Implication $p \rightarrow q$

- *Proof*. We prove the theorem using contraposition.
  1. Start by assuming that the statement claimed in $q$ is F.
  2. Restate your assumption in mathematical terms.
  3. Use mathematical and logical derivations to relate your assumption to $p$.
  4. Argue that you have shown that $p$ must be F.
  5. End by concluding that $p$ is F.

# Example Contraposition Proof of an Implication $\boldsymbol{p \rightarrow q}$

- *Theorem*: If $x^2$ is even, then $x$ is even.
- *Proof*:
  1. Assume $x$ is odd
  2. Then $x = 2k + 1$ for some $k \in \mathbb{Z}$ (definition of what it means for $x$ to be odd)
  3. Then $x^2 = 2(2k^2 + 2k) + 1$ (high-school algebra)
  4. Which means $x^2$ is 1 plus a multiple of 2, and hence is odd
  5. We have shown that $x^2$ is odd, concluding the proof. QED.
- **Exercise**: Prove: IF $x$ is irrational, THEN $\sqrt{x}$ is irrational

# Equivalence: … IF AND ONLY IF …

- $p$ and $q$ are equivalent means they are either both T or both F
- We write ($p$ IF AND ONLY IF $q$) or $(p \leftrightarrow q)$
- You are a US citizen if and only if you were born on US soil
  - (This is not an equivalence according to current US law)
- Sets $A$ and $B$ are equal if and only if $A \subseteq B$ and $B \subseteq A$
- Integer $x$ is divisible by 3 if and only if $x^2$ is divisible by 3
- To prove $p \leftrightarrow q$ is T, you must prove:
  - Row $p$ = *T*, $q$ = *F* cannot occur: that is $p \rightarrow q$
  - Row $p$ = *F*, $q$ = *T* cannot occur: that is $q \rightarrow p$

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| F | F | T |
| F | T | F |
| T | F | F |
| T | T | T |

# Integer $x$ is divisible by 3 IF AND ONLY IF $x^2$ is divisible by 3

- What are $p$ and $q$?

$$p = (x \text{ is divisible by 3})$$
$$q = (x^2 \text{ is divisible by 3})$$

- *Proof*. The proof has two main steps (one for each implication):

1. Prove $p \rightarrow q$: IF $x$ is divisible by 3 THEN $x^2$ is divisible by 3
   - We use a direct proof
   - Assume $x$ is divisible by 3, so $x = 3k$ for some $k \in \mathbb{Z}$
   - Then $x^2 = 9k^2$
   - i.e., $x^2 = 3 \times (3k^2)$, so it is divisible by 3

# Integer $x$ is divisible by 3 IF AND ONLY IF $x^2$ is divisible by 3

- What are $p$ and $q$?

$$p = (x \text{ is divisible by 3})$$
$$q = (x^2 \text{ is divisible by 3})$$

- *Proof*. The proof has two main steps (one for each implication):

2. Prove $q \to p$: IF $x^2$ is divisible by 3 THEN $x$ is divisible by 3
   - We use contraposition. Assume $x$ is **not** divisible by 3. Then there are 2 cases:
   - Case 1: $x = 3k + 1$
     - i.e., $x^2 = 9k^2 + 6k + 1 = 3k(3k + 2) + 1$
     - (still not a multiple of 3)
   - Case 2: $x = 3k + 2$
     - i.e., $x^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$
     - (still not a multiple of 3)
   - In both cases $x^2$ is not divisible by 3. QED.

# …IF AND ONLY IF… Proofs

- IF AND ONLY IF proof contains the proofs of *two* implications
- Each implication may need to be proved differently

# Contradictions

- Example contradictions

$$1 = 2$$
$$n^2 < n \text{ (for integer } n\text{)}$$
$$|x| < x$$
$$p \wedge \neg p$$

- Contradictions are **FISHY**. In mathematics you cannot derive contradictions.
- **Principle of Contradiction:** If you derive something **FISHY**, something's wrong with your derivation.

# Contradictions, cont'd

- Look at this argument
  1. Assume $\sqrt{2}$ is rational.
  2. This means $\sqrt{2} = a_*/b_*$
     - Here $b_*$ is the smallest denominator (well-ordering)
  3. That is, $a_*$ and $b_*$ cannot have 2 as a common factor
  4. We have: $2 = a_*^2/b_*^2$
     - i.e., $a_*^2 = 2b_*^2$ is even
     - i.e., $a_* = 2k$ is even [we proved this]
  5. Therefore, $4k^2 = 2b_*^2$, so $b_*^2 = 2k^2$
     - Hence $b_*$ is even
  6. Hence, $a_*$ and $b_*$ are both divisible by 2. **(FISHY)**
- What could possibly be wrong with this derivation? It must be step 1

# Template: Proof by Contradiction $p$ is T

- You can use contradiction to prove *anything*
  - Start by assuming it's false.
- Powerful because the starting assumption gives you something to work with
- *Proof*.
  1. To derive a contradiction, assume that $p$ is F
  2. Restate your assumption in mathematical terms
  3. Derive a **FISHY** statement – a contradiction that must be false
  4. Therefore, the assumption in step 1 is false, and $p$ is T

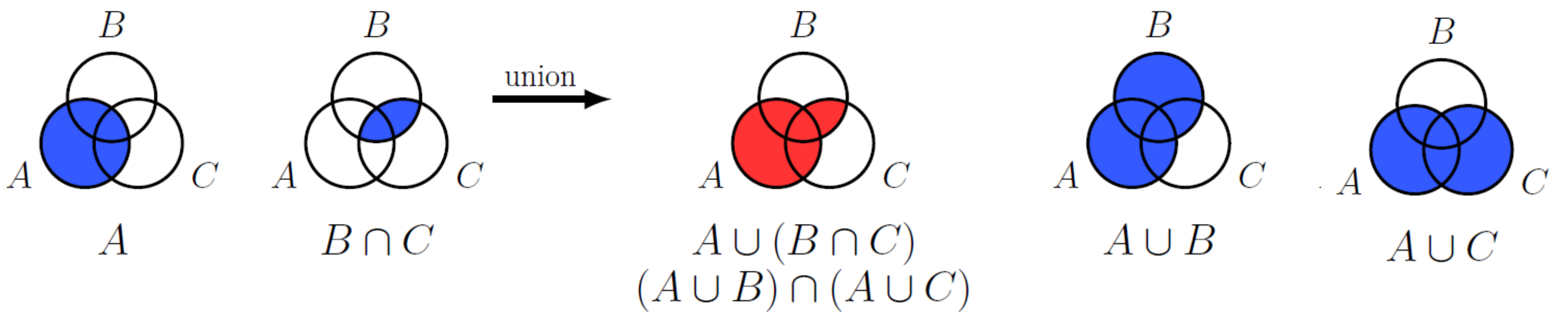
# Template: Proof by Contradiction $p$ is T, cont'd

Rensselaer

- **DANGER**: Be especially careful in contradiction proofs! Any small mistake can easily lead to a contradiction and a false sense that you proved your claim.
- **Exercise**: Let $a, b$ be integers. Prove that $a^2 - 4b \neq 2$.

# Proofs about Sets

- Venn diagram proofs:
  - E.g., $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$




- Formal proofs:
  - One set is a subset of another, $A \subseteq B$:
    - $x \in A \rightarrow x \in B$
  - One set is a not a subset of another, $A \nsubseteq B$:
    - $\exists x \in A: x \notin B$
  - Two sets are equal, $A = B$:
    - $x \in A \leftrightarrow x \in B$

# Proofs about Sets, Exercise

- $A = \{multiples\ of\ 2\}$
- $B = \{multiples\ of\ 9\}$
- $C = \{multiples\ of\ 6\}$
- Prove that $A \cap B \subseteq C$
- What is common about the elements of $A$ and $B$?

# Picking a Proof Template

- Clear how result follows from assumption
  - **Direct proof**
- Clear that if result is false, the assumption is false
  - **Contraposition**
- Prove something exists
  - **Show an example**
- Prove something does not exist
  - **Contradiction**
- Prove something is unique
  - **Contradiction**
- Prove something is *not true* for *all* objects
  - **Show a counter-example**
- Show something is *true* for *all* objects
  - **Show for general object**

# Practice

- Exercise 4.8