Proofs and Proof Strategies

- Discrete Mathematics (Kenneth Rosen)
  - 8th edition – 1.7-1.8

What is a Proof?

- **Proof**: A valid argument establishing the truth of a mathematical statement.
- Ingredients:
  - Hypotheses (if any)
  - Axioms/Postulates
  - Previously proven theorems
  - Rules of inference
- Two styles:
  - **Formal proofs**: detailed, step-by-step (machine-friendly)
  - **Informal proofs**: concise, human-readable (skipping trivial steps)

Importance of Proofs

- Core to mathematics and computer science:
  - Program correctness
  - Security of operating systems
  - Consistency of system specifications
  - Reasoning in AI
- Essential skill: constructing & understanding proofs.
- *Predicate logic* is an extension of propositional logic that permits concisely reasoning about whole *classes* of entities.

  E.g., “x>y”, “x=5”.
- Such statements are neither true or false unless the values of the variables are not specified. Hence, these aren’t propositions.

Terminology

- **Formally and technically, any statement that can be shown to be true using a valid argument (i.e. a proof) is a theorem.**
- **But in mathematical writing (i.e. papers etc),**
- **Theorem** – important proven statement.
- **Proposition** – “less important” theorem.
- **Lemma** – “theorems” that help proving main theorems.
- **Corollary** – follows directly from a theorem.
- **Conjecture** – statement believed true by some partial evidence, not yet proven. Many times, these conjectures are disproven.
- These aren’t “formal” definitions.

How Theorems Are Stated

- Often implicitly universally quantified:
  - “If $x > y$, then $x^3 > y^3$”
  - Really means: “For all real numbers x, y, if $x > y$ then $x^3 > y^3$.”
- Standard proof structure:
  - Pick an arbitrary element
  - Show property holds for that element
  - Conclude it holds for all

How Theorems Are Stated

- Often implicitly universally quantified:
  - "If $x > y$, then $x^2 > y^2$"
  - Really means: "For all real numbers $x, y > 0$, if $x > y$ then $x^2 > y^2$."
- Hence, make sure that the quantifiers are specified in your theorems.

Methods of Proofs

Strategies for proving theorems:

- **Direct proof**
- **Proof by contraposition**
- **Vacuous proof**
- **Trivial proof**
- **Proof by contradiction**
- **Proof of equivalence**
- **Proof by cases**
- **Counterexamples** (to disprove $\forall$ statements)

Methods of Proofs

Strategies for proving theorems:

- **Direct proof**
- **Proof by contraposition**
- **Vacuous proof**
- **Trivial proof**
- **Proof by contradiction**
- **Proof of equivalence**
- **Proof by cases**
- **Counterexamples** (to disprove ∀ statements)

.

.

.

1.7

1.8

Direct Proof

- To prove q, given p:
  - Assume p is true
  - Show q must be true
- Example:
  If n is odd, then n^2 is odd.
  - Let $n = 2k + 1$, where k is an integer.
  - Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ → odd.

Proof by Contraposition

- $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Assume ¬q, show that p is false.
- Example:
  If 3n+2 is odd, then n is odd.
  - Contrapositive: If n is even, then 3n+2 is even.

Vacuous & Trivial Proofs

- **Vacuous proof**:
  If p is false, then p→q is true.
- Example: Show that the proposition *P*(0) is true, where *P*(*n*) is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.
- "If 0>1, then $0^2 > 0$"
- **Trivial proof**:
  If q is true, then p→q is true regardless of p.

Proof by contradiction.

- **Proofs of Equivalence**
- To prove $p \leftrightarrow q$:
  - Prove both $p \rightarrow q$ and $q \rightarrow p$.
- Example:
  "n odd $\Leftrightarrow n^2$ odd"
  - Forward: Assume n odd, show n^2 is odd
  - Backward: Assume n^2 is odd, show n is odd

Counterexamples

- To disprove $\forall x P(x)$, show one example where $P(x)$ is false.
- Example:
  "Every positive integer is the sum of two squares."
  - Counterexample: 3.

Proof by contradiction.

- Assume statement is false
- Derive a **contradiction** (something and its negation)
- Conclude assumption was wrong → statement true.

Proof Strategy

- Start with direct proof (expand definitions).
- If stuck, try:
  - Contraposition
  - Contradiction
- Consider trivial or vacuous cases.
- For equivalences, break into implications.
- To disprove $\forall$, search for counterexamples.

- Detailed version of Proof by exhaustion and cases.

Motivation

- Not all theorems can be proved by a single argument.
  - Sometimes, we must consider different cases separately.
  - Leads to two important techniques:
    - Exhaustive Proof (Proof by Exhaustion)
    - Proof by Cases

Rule of Inference

- To prove: $(p1 \vee p2 \vee \ldots \vee pn) \rightarrow q$
  - Equivalently prove:
    $(p1 \rightarrow q) \wedge (p2 \rightarrow q) \wedge \ldots \wedge (pn \rightarrow q)$
  - Break down into cases and prove each conditional separately.
  - This is called proof by exhaustion.

Example 1 – Exhaustive Proof

- Prove: $(n+1)^3 \geq 3^n$ for $n \leq 4$.
  - n=1: $8 \geq 3$
  - n=2: $27 \geq 9$
  - n=3: $64 \geq 27$
  - n=4: $125 \geq 81$
  - ☑ True for all four cases.

Example 2 – Exhaustive Proof

- Claim: Only consecutive perfect powers ≤ 100 are 8 and 9.
  - Squares ≤100: 1,4,9,16,25,36,49,64,81,100
  - Cubes ≤100: 1,8,27,64
  - Other powers ≤100: 16,32,64,81 …
  - Only 2^3=8 and 3^2=9 are consecutive perfect powers.

Exhaustive Proof

- Special case of proof by cases (we will see in the next slide).
  - All possible instances are explicitly checked.
  - Works only when the number of possibilities is small.
  - Example: Checking all integers in a finite range.

Proof by Cases

- Generalization of proof by exhaustion.
- What if you don't have only finite possibilities.

- A theorem may involve different scenarios.
  - Divide proof into finitely many cases.
  - Prove theorem separately in each case.
  - Each case may contain infinitely many points, but share some property.
  - Combine results to complete proof.

Proof by Cases

- Generalization of proof by exhaustion.
- What if you don't have only finite possibilities.

- A theorem may involve different scenarios.
  - Divide proof into finitely many cases.
  - Prove theorem separately in each case.
  - Each case may contain infinitely many points, but share some property.
  - Combine results to complete proof.

Formally,

- To prove:
- $\forall x \in D, P(x) \rightarrow Q(x)$

- 1. Divide the domain:
- $D = D_1 \cup D_2 \cup \ldots \cup D_n$

- 2. Prove separately:
- $\forall x \in D_1, P(x) \rightarrow Q(x)$
- $\forall x \in D_2, P(x) \rightarrow Q(x)$
- …
- $\forall x \in D_n, P(x) \rightarrow Q(x)$

- 3. Conclude:
- $\forall x \in D, P(x) \rightarrow Q(x)$

Example.

- Claim:
- $\forall n \in \mathbb{Z}, n^2 \geq n$

- Partition domain:
- - $D_1 = \{0\}$
- - $D_2 = \{n \in \mathbb{Z} \mid n \geq 1\}$
- - $D_3 = \{n \in \mathbb{Z} \mid n \leq -1\}$

- Check cases:
- $\forall n \in D_1, n^2 \geq n$
- $\forall n \in D_2, n^2 \geq n$
- $\forall n \in D_3, n^2 \geq n$

- Therefore:
- $\forall n \in \mathbb{Z}, n^2 \geq n$ ✓

Example 3 – Proof by Cases

- Claim: For any integer n, n^2 ≥ n.
  - Case 1: n=0 → 0^2=0.
  - Case 2: n≥1 → n^2 ≥ n.
  - Case 3: n ≤ -1 → n^2 ≥ 0 > n.
  - ☑ Holds in all cases.

Example 4 – Proof by Cases

- Claim: $|xy| = |x||y|$ for real numbers x,y.
  - Cases:
  - 1. $x \geq 0$, $y \geq 0$
  - 2. $x \geq 0$, $y < 0$
  - 3. $x < 0$, $y \geq 0$
  - 4. $x < 0$, $y < 0$
  - All yield same result. ☑

Without Loss of Generality (WLOG)

- Used to combine symmetric cases.
  - Example: Instead of proving both $(x \geq 0, y < 0)$ and $(x < 0, y \geq 0)$, prove one.
  - Say: 'WLOG, roles are symmetric.'
  - ⚠ Must ensure no loss in generality.

Example 7 – WLOG + Proof by Cases

- Claim: If xy and x+y are even, then x,y are even.
  - Assume WLOG x odd.
  - Case 1: y even → x+y odd ✕ contradiction.
  - Case 2: y odd → xy odd ✕ contradiction.
  - Thus, both must be even. ☑

Common Errors

- ❌ Checking only examples (not all cases).
  - ❌ Missing a case (e.g., forgetting x=0).
  - ❌ Incorrect use of WLOG.
  - Example: Claim 'x^2 always positive' missed case x=0.

What is an Existence Proof?

- Many theorems assert the existence of an object.
- General form: $\exists x\, P(x)$.Existence proof = proof of $\exists x\, P(x)$.
- Two types:
  - Constructive: find a witness a such that P(a) holds.
  - Nonconstructive: show $\exists x\, P(x)$ without explicitly finding a.

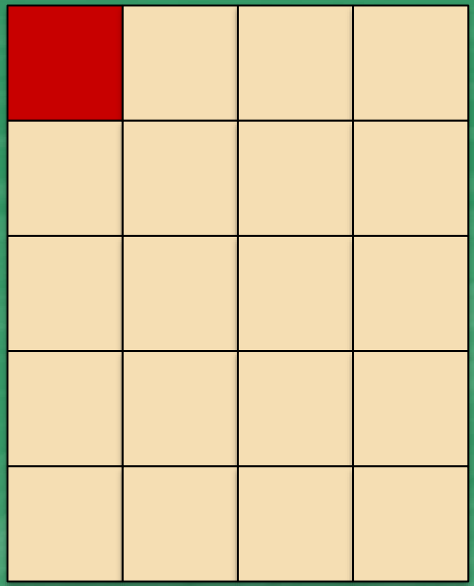
Constructive Proof (Example)

- Provide an explicit example (witness).
- Example 10:
  Show there exists a positive integer expressible as sum of cubes in two ways.
  - **$1729 = 10^3 + 9^3 = 12^3 + 1^3$**
- Famous anecdote: Hardy & Ramanujan ("taxicab number").

Non Constructive Proof

- Game of Chomp.

Chomp Game



- Chomp is a two-player game played on an $m \times n$ grid of cookies.
- Players take turns eating a cookie and all cookies in the rectangle from that cookie to the top-left corner. That is, all the cookies to the below and the right of the chosen cookie.
- The player who is forced to eat the cookie at position (1,1) i.e. top-left, loses.
- Goal: Prove the first player has a winning strategy without specifying the moves.

Game Termination (No Draw)

- Each move removes at least one cookie from the $m \times n$ grid.

- Maximum number of moves: $m \times n$.

- The game always ends (no draws possible) because the grid is finite.

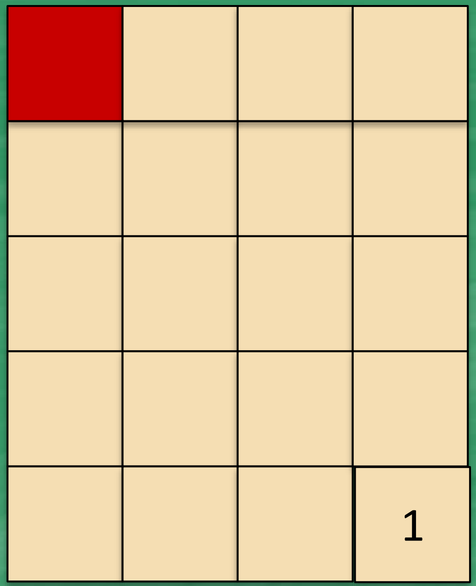
First Player’s Initial Move

- Suppose the first player eats only the cookie at the bottom-right corner, position (*m, n*).
- This move leads to two possibilities:
  - This is the first move of a winning strategy for the first player. That is, the best move that makes it a winner.
  - The second player can respond with a move that starts a winning strategy for them. Which means that second player is the winner.

Second Possibility: Strategy Stealing.

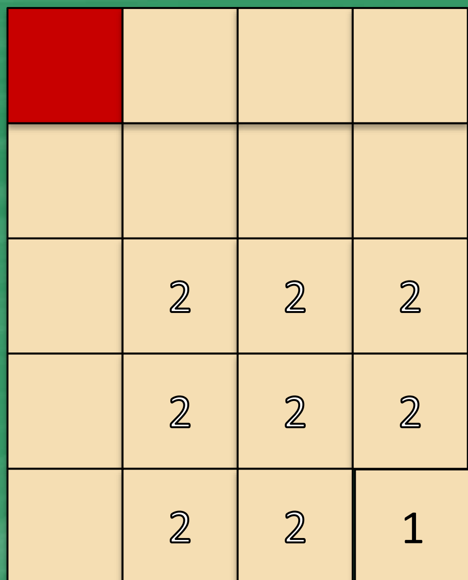
- If the second player has a winning move after the first player eats (*m, n*), call this move *M*.
- Move *M* must be a valid first move in the original $m \times n$ grid (since it removes cookies connected to the top-left).
- Instead of eating (*m, n*), the first player could have played move *M*.

First Player’s Initial Move



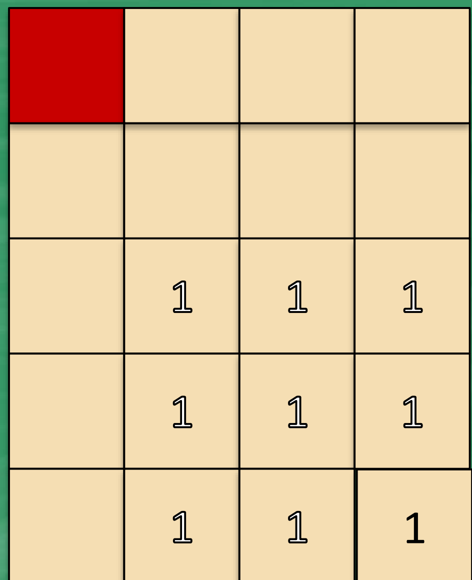
Either this is the best strategy for player I

Player II can win by the next move



That is, the first move of the player I leads to its loss.

But Player I can just imitate this in the first move



Hence, Player I can steal the strategy.

Hence, first player can always win.

- If move *M* starts a winning strategy for the second player, the first player can adopt *M* as their first move.
- By following the winning strategy that *M* initiates, the first player ensures a win.
- Thus, the first player always has a winning strategy, either by eating (*m*, *n*) or by choosing *M*.

Nonconstructive Existence Proof

- Nonconstructive Existence Proof
- This proof shows a winning strategy exists for the first player without specifying the moves.
- It is a **nonconstructive existence proof** because it does not provide an explicit strategy.
- No general winning strategy is known for all rectangular grids.

Uniqueness Proofs

- Theorems may assert the existence of exactly one element with a property.
- General form: $\exists x\, P(x)$ and $\forall y(y \neq x \rightarrow \neg P(y))$
- Two components: Existence + Uniqueness

Structure

- Existence: Show at least one element exists.
- Uniqueness: Suppose x and y both satisfy P. Prove x = y.

Example (Existence)

- Claim: If $a, b \in \mathbb{R}$, $a \neq 0$, then $\exists!\, r \in \mathbb{R}$ such that $ar + b = 0$.

- Existence:
- Let $r = -b/a$.
- Check: $a(-b/a) + b = -b + b = 0$.
  ☑ A solution exists.

Example (Uniqueness)

- Suppose $r = -b/a$ and s is another solution.

- Then $ar + b = as + b \rightarrow ar = as$.
- Divide by a ($\neq 0$): $r = s$.
- ☑ The solution is unique.

Summary

- Uniqueness proofs = Existence + Uniqueness.
- Symbolically:
  $\exists!x\, P(x) \equiv \exists x\, (P(x) \wedge \forall y (y \neq x \rightarrow \neg P(y)))$.
- Example: $ar + b = 0$ ($a \neq 0$) has exactly one solution.

Strategies for Proofs

- Try both Forward and Backward Reasoning.
- Try to adapt the existing proofs of similar theorems.
- If you believe that a statement is wrong, try looking for counter examples.
  Try some small counter examples first.
- Also make use of your intuition (which lead you to believe why the conjecture is wrong) to construct the example.