Reminders

- Homework #2 is due **today**
  - Email me if you are using your free late
- Homework #3 will be out today / tomorrow morning
  - I will send an announcement on Piazza when it is available
  - Will cover proofs (we should cover enough today)

Things to clarify

- Order matters with nesting
  - For any natural number n, there is a natural number s such that $s = n^2$
- How do you make your truth tables?
  - Count the number of rows needed (2^n)
  - Half must be True, half must be False
  - Must account for every combination
  - (Also, binary addition, if you know it)

Rules of Inference

p $p \to q$ ------------ $\therefore q$	Modus ponens	$p \to q$ $q \to r$ ------------ $\therefore p \to r$	Hypothetical syllogism	$p \lor q$ $\neg p \lor r$ ------------ $\therefore q \lor r$	Resolution
$\neg q$ $p \to q$ ------------ $\therefore \neg p$	Modus tollens	$p \lor q$ $\neg p$ ------------ $\therefore q$	Disjunctive syllogism	p q ------------ $\therefore p \land q$	Conjunction

CMSC 203: Lecture 5

Proofs

What is a Proof?

- Valid argument that establishes truth of mathematical statement
- Uses ingredients and rules of inference
- Establishes truth of statement being proved in final step
- Can be formal or informal
  - **Formal**: Long; every step is stated and explained
  - **Informal**: Designed for humans; may skip steps, axioms assumed, rules not explicitly stated

But Whyyyyyy?

- Many applications to computer science
  - Verifying computer programs
  - Establishing security (such as in an OS)
  - Inferences in Artificial Intelligence
  - Showing system specifications are consistent
  - Understanding correctness of algorithms (even ones you create!)

Definitions

- **Theorem**: Statement that can be shown to be true
  - In math, reserved for “important” statements
- **Propositions**: A theorem (but perhaps less important)
- **Proof**: Valid argument that establishes truth of theorem
- **Axioms**: Statements assumed to be true
  - For example, axioms of real numbers
  - May be stated using primitive terms (no definitions)

More Definitions

- **Lemma**: Less important theorem used in steps to a complicated theorem
- **Corollary**: Statement that can be established directly from theorem
- **Conjecture**: Statement proposed to be true
  - Becomes a theorem if proven true

Proof Methods

- A collection of different techniques
- Pick one to use to make a proof
- Only use known axioms, definitions, and theorems
- Do not assume anything that is not an axiom
- Universal quantifier is assumed

Direct Proof

- Demonstrate $p \rightarrow q$ using sequences of steps
  - Assume *p* is true
  - Use rules of inference (axioms, definitions, theorems)
  - Final step shows *q* is true
  - This shows *p* is never true when *q* is false
- Straight-forward
- *Example from book*: "If n is an odd integer, then n^2 is odd"

Indirect Proof

- Do not start with premise and end with conclusion
- Useful for when there is no clear steps to follow from $P(x)$ to $Q(x)$
- Several methods exist to help us with this

Proof by Contraposition

- $p \rightarrow q$ is equivalent to **contrapositive**: $\neg q \rightarrow \neg p$
- We can prove p → q by showing $\neg q \rightarrow \neg p$ is true
- Start with ¬q, use axioms/definitions/theorems/rules of inference, end with ¬p
- *Example from book*: If integer $3n + 2$ is odd, then n is odd

Proof by Contradiction

- Find contradiction q such that $\neg p \rightarrow q$
  - Since q is false, but $\neg p \rightarrow q$ is true, $\neg p$ is false
  - $r \wedge \neg r$ is a contradiction, so show $\neg p \rightarrow (r \wedge \neg r)$
- *Example from book*: "Show that at least four of any 22 days must fall on the same day of the week"

Review of Fallacies

- Affirming the consequent (*abductive reasoning*)
  - If q and $p \rightarrow$ q, then p
  - Eg: If Bill Gates owns Fort Knox, then he is rich. Bill Gates is rich. Therefore, he owns Fort Knox.
- Denying the antecedent (*inverse error*)
  - If $\neg p$ and $p \rightarrow q$, then $\neg q$
  - If Queen Elizabeth is an American citizen, then she is a human being. Queen Elizabeth is not an American citizen. Therefore, Queen Elizabeth is not a human being.
- Circular reasoning
  - Prove something is true by assuming it is true

Some Flawed Logic

- $1 = 2$
  - Provable using direct proof
- If n^2 is positive, then n is positive
  - Provable by axiom that if *n* is positive, n^2 is positive
- If n is not positive then n^2 is not positive
  - Provable by being negative of same axiom

Exhaustive Proof

- Prove statement is true by examining every possible example
- Only possible when dealing with finite solutions
- Only plausible if written with a program (unless very small)
- *Example from book*: Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.

Proof by Cases

- Must cover all possible cases that arise
- Useful if you can individually split *p* into disjunctions
  - $(p_1 \vee p_2 \vee p_3 \vee \ldots) \rightarrow q$
- Takes form of:
  - $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge \ldots$
- *Example from book*: Prove that if n is an integer, then $n^2 \geq n$

Existence Proof

- Useful if theorem is of form $\exists x P(x)$
- **Constructive:** Prove an element *a* exists as a witness
  - You are producing a solution
  - *Example from book*: “There exists a positive integer that can be written as the sum of cubes of positive integers in two different ways.”
  - $1729 = 10^3 + 9^3 = 12^3 + 1^3$

Existence Proof

- **Nonconstructive**: Do not produce a witness
  - You are proving using another proof methd
  - Must show that some solution *must* exist
  - Proof by contradiction, for example
  - *Example from book*: “Show that there exist irrational numbers *x* and *y* such that x^y is rational”

Uniqueness Proof

- Useful if theorem asserts unique element with property
  - Exactly **one** element in a set with property
- Two steps
  - **Existence**: Show an element x exists with property
  - **Uniqueness**: Show that if $y \neq x$, y does not have property (and if y does have property, $y = x$)
- *Example from book*: If a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$

Summary of Proofs

- **Direct Proof**
- Indirect Proof
  - **Contrapositive**
  - **Contradiction**
  - Exhaustive Proof
  - Proof by Cases
  - Existence
  - Uniqueness