Announcements

• Homework 2 is due Thursday, Feb. 12 at 10am in class.
  • Please print out the assignment and use it as a cover sheet when you turn in your homework.

• Homework 1 will be returned in recitation this week.

• Solutions to some of last week’s recitation questions are posted on the web site.

• Change in TA office hours.
  • Jai will have office hours Monday 3pm – 5pm instead of 2pm – 4pm.
Translating to Predicate Logic

I(x) denotes “x has an Internet connection”
C(x,y) denotes “x and y have chatted over the Internet”

Translate: Sanjay has chatted with everyone except Joseph
The Uniqueness Quantifiers

- $\exists!x \ P(x)$ means that $P(x)$ is true for exactly one element in the domain.

- Do we need this quantifier?
- Can we write a logically equivalent statement to $\exists!x \ P(x)$ without it?
MATHEMATICAL PROOFS
Valid Arguments vs. Mathematical Proofs

• The valid arguments we just did are examples of **formal proofs**.
  • Each statement follows logically from preceding statements.
  • Only one rule of inference is used per step.
• Formal proofs can be extremely long and hard to follow (for humans).

• Proofs of mathematical theorems for human consumption are often **informal proofs**.
  • *though people often call these proofs “formal proofs”
• In informal proofs: more than one rule of inference may be used per step, steps may be skipped, premises (axioms) may not be clearly identified.
• Informal proofs must still be logically correct.
Definitions

- A **theorem** is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - axioms (statements which are given as true)
  - rules of inference

- A **lemma** is a 'helping theorem' or a result which is needed to prove a theorem.

- A **corollary** is a result which follows directly from a theorem.

- Less important theorems are sometimes called **propositions**.
  - Even less important theorems are sometimes called **claims**.
Definitions (cont.)

• A **conjecture** is a statement that is being proposed to be true.
  • It may turn out to be false.
  • Once a proof of a conjecture is found, it becomes a theorem.

• Goldbach’s conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.
  • Proposed in 1742 and still an open problem.

• Fermat’s conjecture: The equation $x^n + y^n = z^n$, where $x$, $y$, $z$, and $n$ are integers, has no non-zero solution for $n>2$.
  • Conjectured in 1637.
  • Successful proof published in 1995 by Andrew Wiles.
  • “Fermat’s Last Theorem”
Forms of Theorems

• Many theorems assert that a property holds for all elements in a domain such as the integers or the real numbers.
  • “If \( x > y \), where \( x \) and \( y \) are positive integers, then \( x^2 > y^2 \)”

• To state this precisely requires universal quantifiers, but they are often omitted.
  • “For all positive integers \( x \) and \( y \), if \( x > y \), then \( x^2 > y^2 \).”
Proving Theorems

• Many theorems have the form: \( \forall x(P(x) \rightarrow Q(x)) \)

• To prove them, we show that, where \( c \) is an arbitrary element of the domain, \( P(c) \rightarrow Q(c) \)

• By **universal generalization** the truth of the original formula follows.

• So, we must prove something of the form: \( p \rightarrow q \)
Direct Proof of Conditional Statement

- Direct Proof: To prove $p \rightarrow q$ is true:
  - Assume that $p$ is true.
  - Use rules of inference, axioms, and logical equivalences to show that $q$ must also be true.
Example of a Direct Proof

Give a direct proof of the theorem “If \( n \) is an odd integer, then \( n^2 \) is odd.”

We will need these definitions in our proofs.

- An integer \( n \) is **even** if there exists an integer \( k \) such that \( n = 2k \).
- An integer \( n \) is **odd** if there exists an integer \( k \) such that \( n = 2k + 1 \).

- An integer is either even or odd (never both nor neither).
• Give a direct proof of the theorem:
  “If $n$ is an odd number, then $n^2$ is odd.”
• Give a direct proof of the theorem
  “The sum of two odd numbers is an even number.”
Proof By Contraposition

• Proof by Contraposition: To prove \( p \rightarrow q \) is true,
  • Assume \( \neg q \)
  • Show \( \neg p \) is also true.

• This is sometimes called an indirect proof method.

• If we give a direct proof of \( \neg q \rightarrow \neg p \), then we have a proof of \( p \rightarrow q \).
  • Why does this work?
Give a proof by contraposition that for any integer $n$, if $n^2$ is odd, then $n$ is odd.
Prove by contraposition that if $n$ is an integer and $n^3 + 5$ is odd, then $n$ is even.
Proof by Contradiction

Proof by Contradiction: (AKA *reductio ad absurdum*):
- Suppose we want to prove that a proposition $p$ is true.
- First, assume that $p$ is false ($\neg p$ is true).
- Then, show that $\neg p$ implies a contradiction, i.e.,
  $$\neg p \rightarrow (r \land \neg r)$$
  for some proposition $r$.

- This means that $\neg p \rightarrow F$ is true.
- It follows that the contrapositive $T \rightarrow p$ is true.
- Therefore, $p$ is true.
Example Proof by Contradiction

• Prove that the following theorem: “The difference between any rational number and any irrational number is irrational.”

• A real number $r$ is **rational** if there exist integers $p$ and $q$ with $q \neq 0$ such that $r = p/q$. A number that is not rational is called **irrational**.
• Theorem: The difference between any rational number and any irrational number is irrational.
Theorems that are Biconditional Statements

• To prove a theorem that is a biconditional statement, i.e., a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

• Example Theorem: “If $n$ is an integer, then $n$ is odd if and only if $n^2$ is odd.”
  • Must prove both:
    If $n$ is odd, then $n^2$ is odd.
    If $n^2$ is odd, then $n$ is odd.

• Can use different proof methods for each conditional statement.
Good Problems to Review

• Section 1.7: 1, 5, 7, 9, 11, 13