COMP 182 Algorithmic Thinking

Proofs

Luay Nakhleh
Computer Science
Rice University

Reading Material

- Chapter 1, Section 3, 6, 7, 8

Propositional Equivalences

- The compound propositions p and q are called logically equivalent, denoted by $p \equiv q$, if $p \leftrightarrow q$ is a tautology.
- One way to determine whether two compound propositions are equivalent is to use a truth table.
- Examples:
  - $\neg(p \lor q) \equiv \neg p \land \neg q$.
  - $p \rightarrow q \equiv \neg p \lor q$.
  - $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$.

Propositional Equivalences

Equivalence	***Name***
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

$$p \rightarrow q \equiv \neg p \vee q$$
$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$
$$p \vee q \equiv \neg p \rightarrow q$$
$$p \wedge q \equiv \neg(p \rightarrow \neg q)$$
$$\neg(p \rightarrow q) \equiv p \wedge \neg q$$
$$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$$
$$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$$
$$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$$
$$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$$

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$
$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$
$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$
$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

Propositional Equivalences

- Prove that $\neg(p \to q) \equiv p \wedge \neg q$.
  - Proof 1: by using a truth table.
  - Proof 2: by using logical identities:

Propositional Equivalences

- Prove that $\neg(p \to q) \equiv p \wedge \neg q$.
  - Proof 1: by using a truth table.
  - Proof 2: by using logical identities:

$\neg(p \to q) \equiv \neg(\neg p \vee q)$ by a previous example

$\equiv \neg(\neg p) \wedge \neg q$ by De Morgan law

$\equiv p \wedge \neg q$ by the double negation law

Propositional Equivalences

- Prove that $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$.

Rules of Inference

- Proofs are valid arguments that establish the truth of mathematical statements.
- By an argument, we mean a sequence of statements that end with a conclusion.
- By valid, we mean that the conclusion, or final statement of the argument, must follow from the truth of the preceding statements, or premises, of the argument.
- Let's look at this issue more formally.

Rules of Inference

- An argument in propositional logic is a sequence of propositions.
- All but the final proposition in the argument are called premises and the final proposition is called the conclusion.
- An argument is valid if the truth of all its premises implies the conclusion is true.
- An argument form in propositional logic is a sequence of compound propositions involving propositional variables.
- An argument form is valid if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Rules of Inference

Rule of Inference	***Tautology***	***Name***
p $p \to q$ $\therefore\ q$	$(p \land (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore\ \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore\ p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ $\therefore\ q$	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
p $\therefore\ p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\therefore\ p$	$(p \land q) \to p$	Simplification
p q $\therefore\ p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$ $\neg p \lor r$ $\therefore\ q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

Rules of Inference

- Show that that hypotheses $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $p \vee s$.

Rules of Inference

Rule of Inference	***Name***
$\forall x P(x)$ $\therefore\ P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore\ \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore\ P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore\ \exists x P(x)$	Existential generalization

Rules of Inference

- Use rules of inference to show that if $\forall x(P(x) \lor Q(x))$, $\forall x(\neg Q(x) \lor S(x))$, $\forall x(R(x) \to \neg S(x))$, and $\exists x \neg P(x)$ are all true, then $\exists x \neg R(x)$ is true.

Introduction to Proofs

- A <u>theorem</u> is a statement that can be shown to be true.
- We demonstrate that a theorem is true with a <u>proof</u>.
- A proof is a valid argument that establishes the truth of a theorem.
- The statements used in a proof can include <u>axioms</u> (or <u>postulates</u>), which are statements we assume to be true.

Introduction to Proofs

- Examples of axioms for real numbers:
  - For all real numbers x and y, x+y is a real number (closure under addition).
  - For all real numbers x and y, xy is a real number (closure under multiplication).
  - For every real number x, x+0=0+x=x.
  - ...

Introduction to Proofs

- A less important theorem that is helpful in the proof of other results is called a lemma.
- A corollary is a theorem that can be established directly from a theorem that has been proved.
- A conjecture is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.
- When a proof of a conjecture is found, the conjecture becomes a theorem.

Introduction to Proofs: Direct Proofs

- A direct proof of a conditional statement $p \to q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.

Introduction to Proofs: Direct Proofs

- Definition: The Integer n is even if there exists an integer k such that n=2k, and n is odd if there exists an integer k such that n=2k+1.
- Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."
- Give a direct proof of the theorem "if m and n are both perfect squares, then nm is also a perfect square." (An integer j is a perfect square if there is an integer k such that $j=k^2$.)

Introduction to Proofs: Proof by Contraposition

- Attempts at direct proofs often reach dead ends.
- We need other methods of proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$.
- Proofs of theorems of this type that are not direct proofs are called <u>indirect proofs</u>.
- An extremely useful type of indirect proofs is known as proof by contraposition.
- Such proofs make use of the fact that $p \rightarrow q$ is equivalent to $\neg q \rightarrow \neg p$.
- We take $\neg q$ as a hypothesis, and show that $\neg p$ must follow.

Introduction to Proofs: Proof by Contraposition

- Prove that if n is an integer and 3n+2 is odd, then n is odd.
- Prove that if n=ab, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Introduction to Proofs: Vacuous and Trivial Proofs

- We can quickly prove that a conditional statement $p \rightarrow q$ is true when we know that p is false, because $p \rightarrow q$ must be true when p is false.
- Consequently, if we can show that p is false, then we have a proof, called a vacuous proof, of the conditional statement $p \rightarrow q$.
- 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.
- A proof of $p \rightarrow q$ that uses the fact that q is true is called a trivial proof.
- Trivial proofs are often important when special cases of theorems are proved.
- Example: Let P(n) be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all integers. Show that P(0) is true.

Introduction to Proofs: Proof by Contradiction

- Suppose we want to prove that a statement p is true.
- Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true.
- Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.
- The question is: How can we find a contradiction q that might help us prove that p is true in this way?

Introduction to Proofs: Proof by Contradiction

- Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r.
- Proofs of this type are called proofs by contradiction, which is another type of indirect proofs.
- Example: Prove that the square root of 2 is irrational.
- Example: Show that at least four of any 22 days must fall on the same day of the week.
- Example: Prove that if 3n+2 is odd, then n is odd.

Introduction to Proofs: Proof by Contradiction

- Recall that to show that a statement of the form $\forall x P(x)$ is false, we need only find a counterexample, that is, an example x for which P(x) is false.
- Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Proof Techniques

- Some theorems can be proved by examining a relatively small number of examples.
- Such proofs are called exhaustive proofs, because these proofs proceed by exhausting all possibilities.
- Prove that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 4$.
- Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.

Proof Techniques

- To write an exhaustive proof it must be possible to list all instances to check.
- A type of exhaustive proofs that does not explicitly check all instances is <u>proof by cases</u>.
- A proof by cases must cover all possible cases (as opposed to instances) that arise in a theorem.
- Prove that if n is an integer, than $n^2 \geq n$.

Proof Techniques

- Many theorems are assertions that objects of a particular type exist.
- A theorem of this type is a proposition of the form $\exists x P(x)$, where P is a predicate.
- A proof of a proposition of the form $\exists x P(x)$ is called an existence proof.
- There are several ways to prove a theorem of this type.
- A constructive proof simply finds an element a such that P(a) is true.
- Not all existence proofs are constructive though.

Proof Techniques

- Show that there exists a prime number greater than 10.
- Show that there exist irrational numbers x and y such that x^y is rational.

Questions?