EE360C: Algorithms

Proofs

Pedro Santacruz

Department of Electrical and Computer Engineering
University of Texas at Austin

Spring 2014

A PROOF

- a statement is either *true* or *false*.
    - $1 = 0$ is *false*
    - $\exists t : \cos(t) = t$ is *true*
    - $\forall a, b, c, n : (n > 2) \wedge (a^n + b^n = c^n) \Rightarrow a = b = c = 0$ is true (though it's difficult to prove)
- some statements may be true or false depending on the values assigned to variables:
    - $3x = 5$
    - $x^2 + y^2 - 4xy > 0$

A mathematical proof is a "convincing" argument expressed in the language of mathematics

- it should contain enough detail to convince someone with reasonable background in the subject

Some Terminology

- *Definition*: an unambiguous explanation of terms
- *Proposition*: a statement that is claimed to be true
- *Theorem*: a major result
- *Lemma*: a minor result; often used on the way to proving a theorem
- *Corollary*: something that follows from something just proved
- *Axioms*: basic assumptions or truths

Terminology (cont.)

A theorem can be reduced to stating "if A then B." The following are all equivalent:

- If A is true then B is true
- A implies B
- $A \Rightarrow B$
- B only if A
- A is sufficient for B
- B is true whenever A is true

The Forward-Backward Method

A good technique to approaching a proof is to work from both directions. Start by first writing both the statements A and B. In the forward direction: "given A, what else do I know?" In the backward direction: "how would I show B?"

Example: If a right triangle xyz with sides of length x and y and a hypotenuse of length z has area $z^2/4$, then the triangle xyz is isosceles.

The Forward-Backward Method (cont.)

Example: If a right triangle xyz with sides of length x and y and a hypotenuse of length z has area $z^2/4$, then the triangle xyz is isosceles.

A	right triangle xyz has area $z^2/4$
A1	$xy/2 = z^2/4$ (area = 1/2 base $\times$ height)
A2	$x^2 + y^2 = z^2$ (Pythagorean theorem)
A3	$(x^2 + y^2)/4 = xy/2$ (substituting for z^2)
A4	$(x^2 + y^2) = 2xy$ (multiplying through by 4)
A5	$x^2 - 2xy + y^2 = 0$ (rearranging)
A6	$(x - y)^2 = 0$ (factoring)
B2	$(x - y) = 0$
B1	$x = y$
B	triangle xyz is isosceles

The Forward-Backward Method (cont.)

Example: If a right triangle xyz with sides of length x and y and a hypotenuse of length z has area $z^2/4$, then the triangle xyz is isosceles.

A condensed version of the entire proof: "From the hypothesis and the definition of the area of a triangle, $xy/2 = z^2/4$. By Pythagoras, $x^2 + y^2 = z^2$. On substituting $x^2 + y^2$ for z^2, we obtain $(x - y)^2 = 0$. Hence $x = y$ and the triangle is isosceles.

Proof Tools

Part of our proof is just algebraic manipulation. But other pieces also drew upon external information (e.g., the definition of isosceles triangle, the theorem stating the area of a triangle, the Pythagorean theorem).

In general, a proof will draw upon definitions, axioms, and previously proven theorems. Be careful to avoid a circular proof (i.e., where a step in your proof relies on the theorem you're trying to prove).

Truth Tables

Notations

- $A \Rightarrow B$: "implies"
- $\overline{B} \Rightarrow \overline{A}$: "contrapositive"
- $B \Rightarrow A$: "converse"
- $\overline{A} \Rightarrow \overline{B}$: "inverse"
- $A \Leftrightarrow B$: "equivalence" or "if-and-only-if" or "iff"

A	B	$\overline{A}$	$\overline{B}$	$A \Rightarrow B$	$\overline{B} \Rightarrow \overline{A}$	$B \Rightarrow A$	$\overline{A} \Rightarrow \overline{B}$	$A \Leftrightarrow B$
F	F	T	T	T	T	T	T	T
F	T	T	F	T	T	F	F	F
T	F	F	T	F	F	T	T	F
T	T	F	F	T	T	T	T	T

Quantifiers

- $\exists$: there exists an object with a certain property such that something happens
- $\forall$: for all objects with a certain property, something happens

Specialization

- x' has a certain property
- $\forall x$ with a certain property, something happens
- the something happens for x'

Choose

- $\forall x$ with a certain property, something happens.
- Let x' be such that the certain property holds
- something happens for x'

An Example

If s and t are rational numbers and $t \neq 0$, then s/t is rational.

A	s and t are rational and $t \neq 0$
A1	$\exists$ integers $p, q, q \neq 0$ such that $s = p/q$
A2	Let a, b be integers such that $b \neq 0$ and $s = a/b$
A3	$\exists$ integers $p, q, q \neq 0$ such that $t = p/q$
A4	Let c, d be integers such that $d \neq 0$ and $t = c/d$
A5	$t \neq 0 \Rightarrow c \neq 0$
A6	$\frac{s}{t} = \frac{a/b}{c/d} = \frac{ad}{bc}$
A7	Let $p = ad$ and $q = bc$
B2	$bc \neq 0$, $\frac{s}{t} = \frac{ad}{bc}$
B1	$\exists$ integers $p, q, q \neq 0$ such that $s/t = p/q$
B	s/t is rational

Another Example

- *Def:* $f : S \to T$ is onto iff $\forall t \in T, \exists s \in S : f(s) = t$
- *Def:* Let $f : X \to Y$ and $g : Y \to Z$ be functions, then $g \bullet f : X \to Z$ is the function such that $(g \bullet f)(x) = g(f(x))$
- *Proposition:* if $f : X \to Y$ is onto and $g : Y \to Z$ is onto, then $g \bullet f : X \to Z$ is onto.

A	$f : X \to Y, g : Y \to Z$ are onto
A1	Let $c \in Z$
A2	$\forall z \in Z, \exists y \in Y$ such that $g(y) = z$
A3	$\exists y \in Y$ such that $g(y) = c$
A4	Let b be such a y: $b \in Y, g(b) = c$
A5	$\forall y \in Y, \exists x \in X$ such that $f(x) = y$
A6	$\exists x \in X$ such that $f(x) = b$
A7	Let a be such an x: $a \in X, f(a) = b$
A8	Let x of **[B2]** be a
A9	$(g \bullet f)(a) = g(f(a)) = g(b) = c$
B3	$(g \bullet f)(a) = c$
B2	$\exists x \in X$ such that $(g \bullet f)(x) = c$
B1	$\forall z \in Z, \exists x \in X$ such that $(g \bullet f)(x) = z$
B	$g \bullet f : X \to Z$ is onto
QED	(quod erat demonstrandum)

Proof by Contradiction

In a proof by contradiction, we assume that the negation of our proposition is true and show that it leads to a contradictory statement.

An Example

Theorem: There are infinitely many prime numbers.
Proof: Suppose there is a finite number of prime numbers. Then you can list them in order: $p_1, p_2, \ldots, p_n$. Consider the number $q = p_1 p_2 \ldots p_n + 1$. The number q is either prime or composite. If we divide any of the listed primes p_i into q, there would be a remainder of 1. Thus q cannot be composite. Therefore q is a prime number that is not listed among the primes listed above, contradicting the assumption that our list $p_1, p_2, \ldots, p_n$ lists all of the prime numbers.

Proof by Induction

Three simple steps to an inductive proof:

- Start with verifying the *base case*.
- Then assume the n^{th} case.
- And use that to prove the $(n+1)^{st}$ case.

An Example

Prove that $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

- **Base case**: show it's true for $n = 0$: $0 = \frac{0(0+1)}{2}$
- **Inductive step**: show that if it holds for n then it holds for $n+1$. That is, use: $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ to show that: $0 + 1 + 2 + \cdots + (n+1) = \frac{(n+1)((n+1)+1)}{2}$
- Substituting in the right hand side of the equation for the sum to n to most of the left hand side of the equation for the sum to $n+1$ gives us:

$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)((n+1)+1)}{2}$$

which is true.

Another Induction Example

Prove that the sum of the first n odd positive integers is n^2.

- **Base case**: the sum of the first one odd positive integers is 1^2. This is true since the sum of the first odd positive integer is 1.
- **Inductive step**: show that if it holds for n, then it holds for $n+1$. If the proposition is true for n, then $1+3+5+\cdots+(2n-1)=n^2$. Then we must show that $1+3+5+\cdots+(2n-1)+(2n+1)=(n+1)^2$. We can prove this algebraically.

One More Induction Example

Prove that if S is a finite set with n elements, then S has 2^n subsets.

- **Base case**: a set S of size 0 has one subset (the empty set); $2^0 = 1$.
- **Inductive step**: assume that every set with n elements has 2^n subsets. Prove that by adding one element to the set S, we increase the number of subsets to 2^{n+1}. Let T be a set with $n+1$ elements. Then it is possible to express $T = S \cup \{a\}$ where a is one of the elements of T and $S = T - \{a\}$. The subsets of T can be obtained by the following. For each subset X of S, there are exactly two subsets of T, namely X and $X \cup \{a\}$. Since there are 2^n subsets of S, there are 2×2^n subsets of T, which is 2^{n+1}.

Questions

?