MATH 233
Spring 2018
Making Proofs

MAKING PROOFS

Mathematical proofs use logical reasoning. The rules of inference and equivalences that we had seen in logic are the tools that mathematicians (and scientists in general) use to prove assertions. In fact, any reasonable communication use logic.

Therefore as scientists who understand basic mathematical language and write computer programs we should know how to prove things using logical reasoning:

PROOF STRATEGIES

Theorems have a premise and a conclusion. A proof is showing that the conclusion is true when the premise is true. For example : The sum of two odd numbers is even. This theorem can be expressed as a first-order logic sentence as:

$\forall x \ \forall y \ ((\text{odd}(x) \land \text{odd}(y)) \rightarrow \text{even}(x+y))$
domain of x,y : integers

The premise is $\text{odd}(x) \land \text{odd}(y)$, conclusion is $\text{even}(x+y)$.

There are different proof procedures, i.e. sequence of reasoning steps to arrive the desired result. Which strategy to use changes according to theorem. However, such an intuition develops only through making proofs. Different proof techniques are:

1. Direct proofs
2. Proof by contradiction
3. Proof by contraposition
4. Proof by counter example
5. Induction

Now we will look at every proof strategy with an example proof. We will also explain the logic behind the proof strategy.

Direct proofs

This method, starts with the premise and reaches the conclusion with rules of reasoning. Here is a simple example:

$\forall x \ \forall y \ ((\text{odd}(x) \land \text{odd}(y)) \rightarrow \text{even}(x+y))$

domain of x,y : integers

x is odd and y is odd means that they are of the form:
$x = 2n+1$,
$y = 2m+1$
where n,m are integers.

Then, $x + y = 2n+1+2m+1 = 2n+2m+2 = 2.(n+m+1)$
Since the sum is a multiple of 2, it is even.

Proof by contradiction

This method is also called “reduction to the absurd”. This proof assumes that the contrary of the theorem that needs to be proved is true.

Prove that $p \rightarrow q$ (i.e. $p \rightarrow q \equiv 1$)

Contrary theorem : Prove that $p \wedge \neg q \equiv 0$ (Since $\neg (p \rightarrow q) \equiv p \wedge \neg q$ and $\neg 1 \equiv 0$)
i.e. Show that $p \wedge \neg q$ is a contradiction

If the assumption, through rules of reasoning results with a situation that is absurd (contradicts with our basic assumptions) then conclude that the contrary can not be true and hence the theorem is true.

Here is an example :

Every positive integer has a unique factorization (Note: A factorization of an integer is writing the integer as a product of primes. Order does not mater. For example 24 = 2.2.2.3)

Assume that the contrary is true. There is an integer n which has two distinct factorizations.

$$n = \prod_{i=1}^{i=m} p_i = \prod_{j=1}^{j=n} q_j$$

and also assume that all p_i's and q_j's are distinct (in the case that they are not distinct common factors can be eliminated that then the following proof still holds after this elimination). That is to say, $\forall i, \forall j\ p_i \neq q_j$.

Now, $n = p_1.p_2....p_m = q_1.q_2....q_n$
But then $p_1 = (q_1.q_2....q_n) / (p_2....p_m)$
We know that none of p_i divide any q_j since they are all distinct primes. But then, p_1 can not be a whole number. This is an absurd situation. Therefore our assumption that there are two distinct factorizations can not be true. Therefore the theorem is true.

Proof by contraposition

We know that p → q ~ ¬ q → ¬ p. Sometimes for a theorem like p → q, it is easier to prove ¬ q → ¬ p. This proof technique uses this equivalence.

Here is an example:

Prove that if if n is an integer and 3n+2 is odd then n is odd.
∀n, odd(3n+2) → odd(n)
domain of n : integer

Now this first-order logic sentence is equivalent to:
∀n, even(n) → even(3n+2)
domain of n : integer

And this can be proved using “direct proof” strategy.
When n is even, 3n is also even. Adding an even number to and even number results in a even number. Therefore 3n+2 is even.

Proof by counter example

When there is a theorem that has a universal quantifier, showing a counter example, makes this first-order logic sentence false. Thus makes the theorem false.

Example:
All primes are odd.
As a first-order logic sentence this theorem is:
∀n, prime(n) → odd(n)
domain of n : positive integers.

Now, we know that 2 is prime and 2 is not odd. Thus 2 is a counter example and makes our theorem false.

Remark : Theorems are basis of science, science construct models that applies to objects of investigation. The models are successful as long as they can generalize. That is to say, they explain not individual objects but classes of objects. That is to say, they do generalization. When we find a counter example to a scientific theorem, an object which can not be explained by the model at hand, our theorem is not longer valid and so a new theory needs to be found.

A recent example is the atrobiological finding by NASA researchers about the foundations of life. Until two weeks ago (in 2010) scientific world's theory as this: “In order to have life, six basic elements are necessary: C, H, N, O, P, S.” However, in a lake (in USA) with arsenic, some bacteria replaced phospate on the DNA with arsenic. Therefore because of this counter example, this theorem is no longer valid.

Induction

This strategy is used for theorems where there is a simple case (called the base case) and complex cases can be derived from this simple case via recursion. If the theorem is proved for the base case and for the step where next case is derived from the previous case, then all instances would be covered.

$P(1) \wedge (\forall k, P(\text{kth element in the set}) \rightarrow P(\text{element after the kth element})) \equiv \forall k\ P(k)$

Example:
Sum of integers from zero upto n is n(n+1)/2

As a first-order logic sentence:

$$\sum_{i=0}^{i=n} i = (n.(n+1)) / 2$$

Base case:
n = 1. Sum(n) = 1.2/2 = 1

Inductive step:
Assume the assertion holds for k. Show that it holds for k+1.
Theorem holds for k implies that

$$\sum_{i=0}^{i=k} i = (k(k+1)) / 2 \quad (1)$$

Showing that the theorem holds for k+1 is showing that

$$\sum_{i=0}^{i=k+1} i = ((k+1)(k+2)) / 2 \quad (2)$$

Adding k+1 to both sides in (1) gives us

$$\sum_{i=0}^{i=k} i + (k+1) = (k(k+1)) / 2 + (k+1)$$

Rewriting (3) gives us (2)
Remember that we used induction also when we proved theorems about propositional logic formulas.

What is a constructive proof?

“Sometimes an existence proof of $\exists x P(x)$ can be given by finding an element a, called a witness, such that $P(a)$ is true. This type of existence proof is called **constructive**.” [1]

References :

1. Kenneth H. Rosen, Discrete Mathematics and Its Applications, 7th Edition, Mc-Graw Hill, 2007.

2. “Nasa reveals bacteria that can live on arsenic instead of phosphorus,” http://www.guardian.co.uk/science/2010/dec/02/nasa-bacteria-arsenic-phosphorus

3. Stanley Burris, Logic for Mathematics and Computer Science, Prentice Hall, 1998.