Introduction to proofs, Proof methods and strategies

S. Abu Diab

Mathematics Department
American University of Beirut

October 4, 2010

Outline

Motivation

Man has always made claims about all that surrounds him (people, nature, oneself,...)
But not all of these claims come to work when implemented.
In fact, we are "bombarded" with claims in our everyday life.
Advertisements, conversations, television shows, ... all present opinions that need to be checked and can not be taken for granted.

We have seen that

Logic (from Classical Greek logos ($\lambda\acute{o}\gamma o\varsigma$)) is the study of the principles of valid inference and demonstration.

- Mathematical proofs use the rules of logical deduction that grew out of the work of Aristotle around 350 BC.
- We follow these rules instinctively.
- We understand them even when we do not say them.
- But they are formulated as a set of rules.
- This is how you check your reasoning!!

Axiom

An axiom or postulate is a statement that is assumed to be true. (based on underlying assumptions about mathematical structures)

Theorem

A theorem is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered somewhat important.

Proof

A proof is a sequence of statements that uses the rules of inference to reach the conclusion of the theorem.

Or

Proof

A proof is a valid argument that establishes the truth of a mathematical statement.

Lemma

A lemma is a simple theorem used in the proof of other theorems.

Proposition

A proposition is a theorem that can be proved in few statements.

Corollary

A corollary is a proposition that can be proved directly from a given theorem.

Conjecture

A conjecture is a statement whose truth value is unknown.

"tout droit" start from the given and reach the conclusion.

Example 1:
Show that if n is an odd integer then n^2 is an odd integer.

Indirect = Not direct :)

Indirect Proofs

- Proofs by contraposition

Indirect = Not direct :)

Indirect Proofs

- Proofs by contraposition
- Proofs by contradiction

Proof by contraposition: Instead of proving that p implies q, we prove that $\neg q$ implies $\neg p$.

Example 2:
Show that if n is an integer and n^2 is odd then n is odd.

Proof by contradiction: We suppose that what you want to reach is false and get a contradiction.

Example 3:
Show that $\sqrt{2}$ is irrational.

Proving an equivalence: two implications

Counterexamples: to prove that a statement of the form $\forall x\, P(x)$ is FALSE.

You always need a starting point for your proof. To begin a direct proof for an implication, you can start with the hypotheses. Using the hypotheses, together with axioms and known theorems, you can construct a proof by a sequence of steps that leads to the conclusion. This type of reasoning, called forward reasoning is the most common way to reach relatively simple results.
Similarly, with indirect proofs you will start with the negation of your conclusion and using a sequence of steps reach the negation of your assumption.

However, it may be sometimes helpful to use backward reasoning. This means that we find a new conclusion that will lead to the original one and try to prove this new conclusion.

Example 4:
Show that the arithmetic mean of two different positive real numbers is always greater than their geometric mean, i.e., for any $a,\ b \in \mathbb{R}$

$$\frac{a+b}{2} > \sqrt{ab}$$

If you think you know this, try showing that if a and b are distinct positive numbers, and $A = \frac{a+b}{2}$, $B = \sqrt{ab}$, then we have this inequality

$$B < \frac{(a-b)^2}{8(A-B)} < A$$

We consider all possible cases and prove each one alone.

Example 5:
Show that if $|xy| = |x|\,|y|$ for any two real numbers x and y.

Exhausting cases means you consider all possible single examples.

Euclid showed that there are infinitely many primes by supposing that there are only finitely many primes p_1, p_2,..., p_n. Then, considering the number $p_1 p_2 p_3 ... p_n + 1$. This is not divisible by any of the existing primes. Thus, it must be a prime.

Example 6:
Adapt Euclid's proof that there are infinitely many primes to show that there are infinitely many primes of the form $4k + 3$ where k is a nonnegative integer.

This is when you show that $\exists x\, P(x)$.

A proof is constructive if you construct the answer. For instance, you show that $\exists x\, P(x)$by finding this x. Otherwise, it is nonconstructive.

Refer to page 91

Many other strategies exist. In fact, it is hard to track the creative process in an individual's mind!

- As you noticed, you can never do a proof if you do not know the definitions.
- Keep in mind the different ideas that are used in doing a proof.
- Always try to establish a link between your hypothesis and your conclusion. This link will be the bridge that you will use to reach the end result.

- When you want to prove a statement, be aware of the psychological factor. You can never achieve something if in your mind you believe that you can not do it.
-
- In proving non obvious statements, there is a creative factor sometimes.

K. H. Rosen.
Discrete Mathematics and its Applications.
McGraw-Hill, 5th edition, 2003.