Spencer Gordon
Nicholas Lourie

9/13/2012

Introduction to Proofs and Higher Mathematics

(A brief lecture)

Set Theory, Common Notation, and Background:

Definitions:

- **Set** – an unordered collection of objects. Objects in sets are called *elements*.
  - Sets are often denoted by capital letters
  - Example sets include the set of all students in a class, the set of even numbers, the set of a person's family members, etc…
- **Membership** – elements can be members of sets. If 'b' is a member of the set B we denote that as $b \in B$.
- **Ordered Pair** – a pair of objects of the form (a, b), where a and b have a specific order. Given two sets, A and B, the *Cartesian product* of A and B is the set of ordered pairs (a, b), with a from A and b from B, or using standard notation, $a \in A$ and $b \in B$. The Cartesian product is denoted $A \times B$.
- **Function** – an ordered triple (X, Y, F) where X is the domain of the function, Y is the range or codomain of the function, and F is a set of ordered pairs (x, y) with $x \in X$ and $y \in Y$ (x is a member of X and y is a member of Y). $F: X \rightarrow Y$ is read 'F is a function from X to Y', where X is the domain and Y is the codomain. All functions satisfy the condition that each element in the domain maps to only one element in the codomain. Map is a synonym for function.
- **Image** – given any subset 'A' of the domain of a function 'F', the image of A under F is the set of all values 'b' in the codomain of F such that for some $a \in A$, $F(a) = b$.
  - The idea of image is what a set 'looks like' after it has been mapped by a function.
- **Preimage** – given any subset of values 'B' in the codomain of a function 'F', the preimage of B under F is the set of all values 'a' in the domain of F such that for some $b \in B$, $b = F(a)$.
  - Notice that image and preimage are in a sense opposites of each other.
- **Injection** – A function $F: A \rightarrow B$ is called an *injection* if the preimage of every $b \in B$ is a single point.
  - i.e., a function is an injection, also called *one to one*, if every element of the domain is sent to one and only one element of the range or codomain.
- **Surjection** – A function $F: A \rightarrow B$ is called a *surjection* if the image of A under F, (also called simply the image of F) is equal to B.
  - i.e., a function is a surjection, also called *onto*, if every element in the codomain of F has a non-empty preimage, or more intuitively, if F sends at least one element of the domain to every element of the codomain.
- **Bijection** – A function $F: A \rightarrow B$ is called a *bijection* if it is both a surjection and an injection.
  - i.e., a function is a bijection if every element of the codomain has one and only one element that maps to it. Notice that bijections have easily definable inverse functions, namely take every ordered pair (a, b) and just switch the order to produce (b, a). Functions that are not bijections do not have inverses (can you figure out why?)

- An example of a bijection is every time you count something. For example, if you are counting people in a room, you say a number and point to a person. In effect, you are pairing each person with one and only one number, creating a bijection between people and whole numbers.

- **Cardinality** – two sets have the same cardinality if there exists a bijection between them.
  - The cardinality of a set A is denoted |A|
  - Cardinality extends the idea of the number of objects in a set, and for finite sets that is exactly what cardinality is. To motivate this definition, think of the previous example of a bijection. We count objects by creating bijections with subsets of the whole numbers, so if I have the set of people in this room, and I create a bijection with say, the set of numbers from 1 to 20, than I know there are 20 people in the room. The advantage of this definition of cardinality is that it extends to infinite sets and beyond.
- **Common sets**:
  - Certain common sets have reserved bolded letters to represent them. When hand written, it is common for mathematicians to use what is called 'blackboard bold'
  - **R** – the set of real numbers (all numbers representable by finite or infinite decimal expansions)
  - **Q –** the set of rational numbers (or quotients, the set of all fractions)
  - **N –** the set of natural numbers (all whole numbers greater than and including zero)
  - **Z –** the set of all integers (all positive and negative whole numbers and including zero)
  - **Ø –** the *empty set,* or set with no elements

Set and Set Builder Notation

- {} can denote the empty set
- {a, b, c} denotes the set containing exactly the elements a, b, and c.
- { *symbol for a generic element* : *conditions which the element satisfies* }
  - Example: { n ∈ **N** : n is even }, this set is read as follows. The first statement 'n ∈ **N**' means n is a member of the natural numbers, the colon is read as 'such that' and the last statement is a familiar property of some whole numbers. Thus the set is read as, 'the set of all n that are members of the natural numbers such that n is even'; however, usually a mathematician will shorten this to something like 'the set of all natural numbers that are even'.
    - A bar is sometimes used in place of the colon, as in the following example: { p ∈ **N** | p is a prime number } which could be read as 'the set of all p such that p is a prime number'. Notice that the letter p did not have to be used in the set's construction, any letter would have done; however, certain letters are sometimes commonly used for specific meanings in mathematics, and p is often used to denote a prime.

- How would you express the image of a set A under a function F in this notation? How would you express the preimage of a set B under F in this notation?

Common Abbreviations and Symbols

- s.t. – such that
- iff – if and only if
- QED - *quod erat demonstrandum*, generally written at the end of larger or more involved proofs.
- ■ - Often written to signify the end of shorter proofs.
- ∀ - for all
- ∃ - there exists
- ∄ - there does not exist
- ∈ - is a member of
- ∃! - Exists a unique
- ∴ - Therefore
- → - implies
- ↔ - if and only if

For more see http://en.wikipedia.org/wiki/List_of_mathematical_symbols

Basic Proof Techniques:

Proof begins with understanding

Backward/Forward

- Write out all definitions and given information
- Combine given information to draw new conclusions (this process is going forwards)
- Look at target statement you wish to prove
- Consider what other statements might directly imply it (this process is going backwards)

Contradiction

- Rather than proving a statement, assume its logical opposite or negation.
- Using your assumed truth of the logical opposite, show that either it leads to an implication which contradicts itself or that the logical opposite is not true.

Contrapositive

- The statement "If 'a' then 'b'" is logically equivalent to the statement "if not 'b' then not 'a'", which is known as the contrapositive of the initial statement.
- Sometimes it is easier to prove a statement's contrapositive rather than the statement itself.

Counter Example

- If a statement makes a claim about all members of a set, it is enough to disprove the statement by finding a single member of the set which contradicts it.

Induction

- Proof by induction can be reduced to two steps.
  - Prove that the statement holds for the base case or n = 1
  - Prove that given the statement holds for some arbitrary number n, it also holds for (n + 1).
- Proof by induction can be interpreted in a number of ways. Daniel Solow in his book "How to Read and Do Proofs" draws an analogy between proof by induction and making a 'proof machine'.

Common Patterns of Proof:

Proving uniqueness

- Assume that another object exists sharing the properties of the supposed unique object, and then prove that the two must be equal or the same.

Example Proof: The additive identity of the integers, 0, is unique.

Proving a statement for every member of a set

- Take an arbitrary member of the set, and prove that the statement holds for it. The key idea here is that proving a statement for *any* arbitrary member of a set is the same as proving it for *every* member of the set (as long as the properties you use hold for every member of the set).

Example Proof: Prove every even number is the sum of two odds.

Proving A is a subset of B

- This statement is really equivalent to the statement that every member of A is a member of B, which is simply proving a statement about every member of A. Thus, take an arbitrary member of A and prove that it must be a member of B.

Example Proof: Prove the multiples of 12 are a subset of the multiples of 3.

Proving set equality

- To prove A = B, first prove that the set A is a subset of B, and then prove that the set B is a subset of A. Equivalently, prove every member of A is a member of B and every member of B is a member of A.

- The idea of proving set equality is that sets are completely defined by their elements, so if two sets have all the same elements, they must be the same sets.

Example: Prove that { x | x = 12n, n ∈ **N** } = { x | x = 3n, n ∈ **N** } ∩ { x | x = 4n, n ∈ **N** }

Some Interesting Examples:

Prove that root two is irrational

Can easily be proven using proof by contradiction

Assume $\sqrt{2}$ is rational. Then for some integers a and b we have $\sqrt{2}$ = a/b, such that a and b have no common divisors, or equivalently that the fraction is reduced. This implies $a^2/b^2 = 2$, or $a^2 = 2b^2$. This implies that a^2 is even, so a must be even. Since a is an even integer, there must be some integer such that a = 2i. Thus $(2i)^2 = 2b^2$ or $4i^2 = 2b^2$. From this we know that $b^2 = 2i^2$, so b is even. If b is even and a is even, then the fraction a/b is not fully reduced. This is a contradiction, therefore no such a and b can exist, so $\sqrt{2}$ must be irrational.

(In this proof the fact that if a^2 is even and a is an integer, then a must be even was used twice, can you prove this? Can you write this proof and the proof that the square root of two is irrational using symbols instead of words?)

Proof of infinite primes

Assume there is a complete list of primes arranged by size, P_1, …, P_n . Consider the number $P = P_1*P_2*…*P_n + 1$. P is not divisible by any number on the list of primes, therefore either P is prime, or there exists a prime number smaller than P which is not on the list. This contradicts the assumption that the list contains all prime numbers; therefore no such list can exist.

Sources

Parts of this talk have been adapted from Daniel Solow's "How to Read and Do Proofs"