8 Proof mechanics: Simplifying the goal[9]

We've now seen many examples of simple proofs for universal principles about sets and functions. The details of the proofs differ, but all proofs share some basic common features. In this section we provide a systematic look at the techniques used to build a proof.

At any point in a proof, there is an active scenario (with active objects and active assumptions) and a goal. When trying to make further progress, you should generally *focus on the goal*, rather than on the scenario. There are two basic ways to make progress:

Approach 1: If the form of the goal is a *compound assertion*, use the *top-level logical structure* of the goal to modify both the active scenario and the goal.

Approach 2: Replace the goal G by another goal G' that implies G. This does not change the scenario.

Doing proofs involves a combination of technical skill and creativity. The skill comes in following the rules of proof correctly, and understanding how to properly work with the mathematical objects and assertions in the scenario. The creativity comes in because as you do proofs, there are choices to make. Sometimes these choices are clear, but often they rely on the mathematicians imagination and ingenuity. As we discuss the proof techniques below, we'll highlight the places where the mathematician is required to use creativity.

8.1 Modifying the goal 1. Use the top-level logical structure of the goal to modify the proof task

If the current goal is a compound assertion, then depending on the top-level structure, we can modify the scenario and the goal. If the top-level structure of the assertion is $\neg A$, where A is a compound assertion, then $\neg A$ has a logical equivalent whose top-level structure is not negation. Apply this equivalent first. Otherwise, we can apply the methods below. All of these methods are easy to apply except the case that the goal has the form "There exists $x \in T$ such that $A(x)$".

Current goal: For all $x \in T$, $A(x)$.

Add to scenario : Suppose x is an arbitrary member of T. (Introduce object x)

New goal : Prove $A(x)$.

Current goal: Prove: If A then B.

Technique 1. Direct.

Add to scenario : Assume A.

[9] 2-11-2015.

New goal : Prove B.

Technique 2. Contrapositive

Add to scenario : Assume B is false.

New goal : Prove that A is false.

Remark 8.1. These two proof techniques tell us that when proving $A \implies B$ we can start by assuming A or by assuming $\neg B$. However, you may not assume B, you must *prove* it!

Current goal: Prove: A or B.

Technique 1. **Add to scenario** : Assume B is false.

New goal : Prove A

Technique 2. **Add to scenario** : Assume A is false.

New goal : Prove B.

Current goal: A and B. Split the goal into two goals and prove each separately.

First goal : Prove A

Second goal : Prove B

Current goal: A if and only if B. Split into two goals and prove each separately. Technique 1. Split into two parts.

First goal : Prove if A then B.

Second goal : Prove if B then A.

Technique 2. Introduce an intermediate assertion.

Introduce an additional assertion C. (The choice of C requires ingenuity.)

First goal : Prove $A \iff C$.

Second goal : Prove $B \iff C$.

Current goal: There exists $x \in T$ such that $A(x)$.

Add to scenario: Provide "instructions" for constructing a specific object. Prove that these instructions produce an object in T. Add this object to the scenario with the instructions "Let x be the constructed object".

New goal: Prove that the constructed x satisfies $A(x)$.

All of the modifications to the scenario and goal described above are straightforward to carry out, *except* the case that the current goal is an existential assertion "There exists $x \in T$ such that $A(x)$". In that case, the modification of the scenario requires the proof-writer to provide instructions for constructing $x \in T$. These instructions are specific to the current scenario, and may require considerable cleverness and creativity.

Approach 2. Replacing the goal by another goal that implies it. In the first approach, we modified goals based on the logical structure of the goal. As usual, when we focus on logical structure, the meaning of the assertion is not important, just how its put together.

In the second approach, we modify the goal based on the actual meaning of G. Such a goal can be found in a few ways.

The goal G' is obtained by applying a definition For example, suppose your goal is to prove that $A \subseteq B$, where A and B are sets in the current scenario. Using the definition of "$A \subseteq B$" we replace the goal by "For all $x \in A$, we have $x \in B$."

As another example, G is "n is composite" where n is a positive integer in your current scenario. Using the deifinition of *composite* integer we can replace the goal by "There are two positive integers less than n whose product is n" or "There is a positive integer k larger than 1 such that n/k is a positive integer greater than 1."

The goal G' is obtained by applying a known theorem. For example, Suppose our current scenario includes a function f and the goal is "f is a bijection". Theorem 7.21 tells us that a function is a bijection if and only if it is invertible. So we could change the goal to "f is invertible". Then using the definition of invertible, we can change our goal further to "f has a left-inverse and a right-inverse".

Dreaming up a new goal. This is where mathematics gets really creative. We have a mathematical scenario and a conclusion G that we're trying to prove. The mathematician tries to imagine: what would help me prove goal G? She uses all of her mathematical knowledge and experience, and also considers different examples of the scenario, and uses all she knows to try to figure out how to reach goal G. If she's lucky and skillful, she comes up with an idea: Here's another goal G'. I think I can prove G' and I think that goal G' has something to do with G. If I can prove both of the following:

1. G' implies G.
2. G' is true.

then G will follow.

For example, our scenario has a function $f : \mathbb{R} \longrightarrow \mathbb{R}$ that is given by $f(x) = x^3 - 6x^2 + 10x + 7$ and we want to show that this function is one-to-one. The mathematician may remember that derivatives tell us useful things about functions, and after trying some examples may come up with the following alternative approach:

1. Prove that if $g : \mathbb{R} \longrightarrow \mathbb{R}$ is any function for which the derivative is defined and positive for all x, then g is one-to-one.
2. Prove that the derivative of the given function f is defined and positive for all x.

Notice that the new goal, which talks about the derivative of f, seems completely different than the old goal, and requires the mathematician to use knowledge and imagination to discover.

8.2 Three other proof techniques.

There are three other approaches to proofs: *proof by contradiction*, *proof by cases* and *proof by mathematical induction*. Examples of the first two were given in the previous section. Here we'll briefly discuss each of them.

Proof by Contradiction. A scenario is said to be *contradictory* of there are no feasiable instances. For example: if x is a real number, the assertions $x > 9$ and $x < 7$ are contradictory.

Suppose that we have a particular scenario and our goal is to prove A. This is the same as proving that for the given scenario, it is impossible that A is false. . One approach to doing that is to assume that "A is false" and see what happens. If we can deduce two contradictory conclusions, we conclude that assuming "A is false" leads to a contradictory scenario. Therefore A must be true.

Current goal. Prove A

> **Add to scenario** A is false.
>
> **New goal** Derive two assertions that contradict each other.

Here's a famous example:

Theorem 8.1. *There are infinitely many primes.*

Proof. Suppose for contradiction that there are finitely many primes. Then there is a largest prime p. Let $m = p!$, which is the product of all the numbers from 1 up to p and let $n = 1 + m$. Let D be the set of divisors of n that are bigger than 1. D is nonempty (since $n \in D$). Let q be smallest member of D. Then q has no divisors other than itself or 1 (otherwise such a divisor would be a smaller member of D). So q is a prime, and so must be less than or equal to p. Since $q \leq p$ and m is the product of all positive integers up to p, q is a divisor of m. But then q is a divisor of both m and n which means that both $\frac{n}{q}$ and $\frac{m}{q}$ are integers, which means that $\frac{n}{q} - \frac{m}{q} = \frac{1}{q}$ is an integer. But $q > 1$ so this is impossible. So we have a contradiction, and so our assumption that there are finitely many primes is wrong. □

Proof by cases There is a particular approach to modifying the goal that involves breaking the goal into multiple parts and proving each part separately.

Proof by cases, first form Suppose our goal is to prove A. Let B be any other assertion. We do two separate subproofs:

Subproof one First case.

> **Add to scenario** Assume B
>
> **New goal** Prove A

Subproof two Second case.

Add to scenario Assume $\neg B$

New goal Prove A

This two part process proves "if B is true then A is true, and also if B is false then A is true". Since in every instance of the current scenario, one of B and $\neg B$ is true, we can conclude that A is true.

Applying this method requires choosing the assertion B. The proof-writer is free to choose B, since the logic works for any choice of B. What is a good choice of B? Using this method splits the proof into two parts. In each part we add an additional assumption to the scenario, either B or $\neg B$. What we hope is that in each case, adding the additional assumption will make what we want easier to prove. If it doesn't seem to make things easier to prove in both cases, then we made a bad choice of B! Finding a good choice of B, that makes things easier to prove in both cases, is another major place for mathematical creativity.

Proof by cases, second form Suppose our goal is to prove A. Suppose that $B_1, \ldots, B_k$ are a list of assertions. We do k separate subproofs one for each B_i, and one additional subproof.

Subproof i Prove that if B_i is true then so is A

Add to scenario Assume B_i

New goal Prove A

One additional subproof.

Prove that at least one of the B_i is true.

Add to scenario $\neg B_1, \ldots, \neg B_{k-1}$

New goal Prove B_k.

Principle of mathematical induction. This principle is enormously important, and will be explained in detail Section **??**. Here we will introduce it.

Remark 8.2. **A caution to the reader.** You may have seen mathematical induction before, and you may think you already know it. Mathematical induction comes in many forms, and the form usually taught in elementary classes has limited usefulness. Furthermore, when students try to apply this form in more complex situations, it leads them to make serious errors. The form of mathematical induction taught in these notes will probably be different than what you learned before, and is intended to prepare you to use induction properly in complex mathematical situations. So *you should forget everything you think you know about induction, and learn it as presented here.* Later on, we'll relate the form of induction presented here to the more elementary forms of induction usually taught in elementary classes.

This principle of mathematical induction is a general principle for mathematical proofs that can be used *whenever you are proving a universal assertion*, provided that the type of the universal object in the principle is one of the following types:

- Nonnegative integers (or a subset of the nonnegative integers)
- Finite subsets of some set
- Lists with entries taken from some set.
- Any type that is *well-founded.* (Don't worry about what this is now; it will be explained in Section **??**.)

Here is the Principle of Mathematical Induction (PMI):

> Suppose you are proving a universal assertion: "$\forall x \in T, C(x)$". As usual, we start "Suppose x is an arbitrary member of T. We must prove $C(x)$." If T is one of the above types, we are permitted to make the following assumption:
>
> > "We assume that for any $y \in T$ that is smaller than x, $C(y)$ holds".
>
> This assumption is called the *induction assumption.* (Note: If the type T is positive integers, then "smaller than" means "less than". If it is finite subsets, "smaller than" means "having smaller size than" and if it is lists it means "of smaller length than".) We may use this assumption freely in our proof. If we are able to prove $C(x)$ while using this assumption, then this provides a proof of "$\forall x \in T, C(x)$".

There are two questions you should have when first seeing the principle of mathematical induction:

- Why are we allowed to make this assumption?
- How is this assumption useful in proving things?

The answer to the first question will be discussed in Section **??**. For now, you don't need to worry about this. The important thing to know is that mathematicians have determined that the principle of mathematical induction is "sound" which means that you can not prove something that's false using it. So if you manage to prove something using induction you can be assured that it really is true!

The principle of induction looks suspiciously like we are assuming what we are trying to prove, but we are not. In our proof we are trying to prove $C(x)$ for a specific x of T. We are not allowed to assume $C(x)$! We are only allowed to prove $C(y)$ for y smaller than x.

Here's a simple example of a proof by induction:

Theorem 8.2. *For every positive integer $n \geq 2$, there exists a list of primes whose product is n.*

Proof. Suppose n is a positive integer greater than 2. We must show that there is a list of primes whose product is n. By induction, we may assume that if m is an integer smaller than n and greater than 2, then there is a list of primes whose product is m,

We divide into two cases, depending on whether n is prime or n is not prime.

Case 1. Assume n is prime. Then the list (n) is the desired list.
Case 2. Assume n is not prime. Then there are two integers greater than 1, call them a and b such that $n = ab$. Necessariliy a and b are both less than n. So using the inductive assumption, there is a list r of primes whose product is a and a list s of primes whose product is b. Consider the list $r * s$ obtained by concatenating r and s. Then $r * s$ consists only of primes, and the product of the entries is equal to the product of entries in r (which is a) times the product of the entries in s (which is b) which is $ab = n$. So $r * s$ is the desired list. □