7 Proof mechanics: Simplifying the goal[8]

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

You have a universal principle to prove. You set up the inifial proof task whose scenario is the hypothesis of the principle being proved, and whose goal is the conclusion of the principle being proved.

The key to getting started on almost any proof is to *focus on the goal*, rather than on the scenario. The initial steps of the proof are generally focused around *simplifying the goal.* The aim is to transform the goal into an atomic assertion (without "and", "or", "if-then", "if and only if" or quantifiers containing no specialized terminology.

There are two basic ways to make progress:

Approach 1: Replace the goal G by another goal G' that implies G. This does not change the scenario. If we prove G', it follow that G is also true.

Approach 2. Use the top-level logical structure of the goal to modify the proof task.

Approach 1. Replacing the goal G by another goal G' that implies G. There are a few different ways to do this.

The goal G' is logically equivalent to or logically stronger than the goal G For example, suppose our scenario involves real numbers x and y (with some assumptions) and our goal is to show "$x^2 - x \leq y^3$ or $x \geq 1$ holds" If we represent $x^2 - x \leq y^3$ by A and $x \geq 1$ by B, we have $A \vee B$ which is logically equivalent to $\neg B \implies A$. Therefore we can replace our goal by "if $x < 1$ then $x^2 - x \leq y^3$".

As another example, suppose that the scenario includes two sets A and B and the goal is to show "It is not the case that $A \subseteq B$ or $B \subseteq A$". This is logically equivalent to "A is not a subset of B and B is not a subset of A"

The goal G' is obtained by substituting a definition in for terminology appearing in G 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."

[8] 2-11-2015. ©2015 by Michael E. Saks

The goal G' is obtained by combining a known theorem with G For example, Suppose our current scenario includes a function f and the goal is "f is a bijection". Theorem 6.18 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".

Approach 2. 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.
>
> **New goal** : Prove B.

Technique 2. Contrapositive

> **Add to scenario** : Assume B if false.
>
> **New goal** : Prove that A is false.

Current goal: Prove: A or B, which is logically equivalent to $\neg B \implies A$.

Technique 1. Direct

> **Add to scenario** : Assume B is false.
>
> **New goal** : Prove A

Technique 2. Contrapositive.

> **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.

> **First goal** : Prove if A then B.
>
> **Second goal** : Prove if B then A.

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.

There are three other approaches to proofs: *proof by contradiction*, *proof by cases* and *proof by induction.* We'll summarize these here, and discuss them in more detail later.

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 the the negation of A is contadicts this scenario. 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 7.1. *There are infinitely many primes.*

Proof. Suppose for contradiction that there are finitely many primes. Then it is possible to form a list consisting of all the primes. Let p_1, p_2,...,p_k be such a list. Let m be the product of all the p_j 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 p be smallest member of D. Then p has no divisors other than itself or 1 (otherwise such a divisor would be a smaller member of D). So p is a prime, and so is on the list of primes. Since m is the product of the list of primes, p is a divisor of m. Also p is a divisor of n. Then n/p is an integer and m/p is an integer. Then $n/p - m/p$ is an integer, but $n/p - m/p = 1/p$ which is not an integer. So we have a contradiction, and so our assumptino 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!

Proof by cases, second form Suppose our goal is to prove A. Suppose that B_1, ...,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 quite important, and will be explained in detail Section **??**. Here we summarize it. 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 from some set
- Any type that is *well-quasi ordered.* (Don't worry about what this is now; it will be explained later.)

The principle of mathematical induction says:

> Suppose you are proving an assertion of the form "$\forall x \in T, C(x)$". Following the usual method for universal statements, we write "Suppose x is an arbitrary member of T. We must prove $C(x)$." The principle of mathematical induction (PMI) says that we are allowed to make the following assumption "for free". "We assume that for any y 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 "shorter 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 an optional section later. But 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 7.2. *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. □