Math 79SI Notes

Mason Rogers

5 Mathematical Induction I

5.1 Background

The proof techniques we have developed so far give us an array of tools for proving implications $P \implies Q$. However, in some instances proving one implication is not enough. Sometimes, we are faced with an infinite family of related statements $P_1, P_2, P_3...$ and want to prove them all true. In doing so, we prove all of the P_n by lining them up like dominoes

$$P_1 \implies P_2 \implies P_3 \implies \ldots \implies P_n \implies P_{n+1} \implies \ldots$$

so that knocking down the first one (P_1) makes them all fall.

A classic example is the proof that $1 + 3 + \ldots + 2n - 1 = n^2$ for all $n \in \mathbb{N}$. We aim to prove $P_n \implies P_{n+1}$ for all n, then show that P_1 is true. Let P_n be the statement $1 + 3 + \ldots + 2n - 1 = n^2$ for fixed n. Assuming P_n to be true, we can add 2n + 1 to both sides to obtain $1 + 3 + \ldots + 2n + 1 = n^2 + 2n + 1 = (n + 1)^2$, precisely the statement P_{n+1} . Hence, we proved $P_n \implies P_{n+1}$ for all $n \ge 1$. It then remains to show that P_1 is true, which is easy to check: 1 = 1. From this, we could conclude that P_n is true for all $n \in \mathbb{N}$, which is precisely the claim.

This is the most basic form of mathematical induction and what we will focus on this week. The most immediate application of this technique is in proving that a family of statements holds true for all natural numbers n.

Sometimes, the step of proving $P_n \implies P_{n+1}$ is called the *inductive step*, and the P_1 case is known as the *base case*. As a warning, some arguments require checking multiple base cases rather than just P_1 .¹ For instance, explicit formulas for recursive sequences can often be proven by induction. But if the recurrence depends on the previous k terms of the sequence, all of the first k must be checked. In general, it is important to verify that the cases you have directly checked match the required hypotheses of the inductive step.

Inductive arguments may take many forms while still having the same two principal steps. Sometimes, you may need to assume more than P_n to prove P_{n+1} . Perhaps you need to assume both P_{n-1} and P_n , or even P_k for all $k \leq n$, to prove P_{n+1} . We will also (over this section and the next) see examples of multiple inductions, nested inductions, induction on

¹This is why we write most induction arguments by proving the inductive step *before* checking the base case. When we have already written the inductive step carefully, it is easier to see how many base cases are necessary to 'knock all of the dominoes down', per our analogy. Many authors write the inductive step after the base case, which still results in a valid proof.

geometric constructions, and more. However, the general principle remains the same: make sure that your inductive step reaches all the cases you aim to prove and that your base cases cover all of the necessary inputs to your inductive step. Quoting our domino analogy one last time, make sure that you arrange your dominoes in a way that they will all fall once a certain few are knocked over, then make sure that you knock over those certain few correctly.

Mathematical induction is a powerful technique that manifests in all branches of mathematics. We will begin with a few examples that make induction the clear choice of proof technique, then branch into examples that showcase the beauty and utility of mathematical induction beyond proving formulas.

5.2 Examples

We begin with a classic example of proof by induction to familiarize ourselves with the technique. Let S_n denote the sum of the first *n* natural numbers, so $S_n = 1 + 2 + ... + n = \sum_{i=1}^{n} i$. We wish to find an explicit formula for S_n . Writing out a table of S_n for small *n* gives the following.

n	S_n	n	S_n
1	1	6	21
2	3	$\overline{7}$	28
3	6	8	36
4	10	9	45
5	15	10	55

Either by plotting successive differences of the S_n or by plotting a graph of S_n versus n, a quadratic relationship is suggested. We conjecture that $S_n = an^2 + bn + c$ for some numbers a, b, and c to be found. Substituting S_n and n for n = 1, 2, 3 gives the following system of equations for a, b, and c.

1	1	- 1	Γ	a		$\begin{bmatrix} 1\\ 3 \end{bmatrix}$	
4	2	1		b	=	3	
9	3	1	L	c		6	

This has the unique solution (a, b, c) = (1/2, 1/2, 0), giving us the suggestion that $S_n = (n^2 + n)/2 = n(n+1)/2$, which we now aim to prove.

Proposition 5.1. $S_n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Proof. We will begin by proving that if the formula holds for n = k then it also holds for n = k + 1. Suppose that $\sum_{i=1}^{k} i = k(k+1)/2$. Adding k + 1 to both sides gives

$$\left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + k + 1.$$

We can pull the k + 1 on the left side into the summation by increasing the upper limit of the summation to k + 1, obtaining

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + k + 1.$$

The left side is now by definition equal to S_{k+1} , so it remains to show that the right side is equal to (k+1)(k+2)/2, i.e. that the formula for S_n holds for n = k+1. We have

$$\frac{k(k+1)}{2} + k + 1 = \frac{k^2 + 3k + 2}{2} = \frac{(k+1)(k+2)}{2},$$

as desired. This completes the proof that if the formula holds for n = k, the formula holds for n = k + 1.

Since we only use each individual case n (and no previous cases) to prove case n + 1, it suffices to check n = 1 as our lone base case. From direct computation, we see that $S_1 = 1$ and that 1(1+1)/2 = 1, so the formula holds when n = 1. Thus, the formula holds for all $n \in \mathbb{N}$, completing the proof.

To put it explicitly in the language of proving an infinite family of statements P_n , let the statement P_n be $S_n = n(n+1)/2$. The proposition is precisely the statement that P_n is true for all $n \in \mathbb{N}$. We then proved that for all $k \ge 1$, $P_k \implies P_{k+1}$, i.e. that if the formula holds for n = k, it also holds for n = k + 1. Then, all that remained to do to conclude that P_n is always true was show that P_1 is true, which was as simple as writing 1 = 2/2.

We now turn to prove a slightly more complicated formula. This time, our argument will require using P_n and P_{n-1} to prove P_{n+1} , so we will have to check 2 base cases.

The Fibonacci sequence, known for its ubiquity in nature² and connection to the Golden Ratio, is an example of a recursively defined sequence, where for all $n \ge 2$, the *n*-th Fibonacci number F_n is given by $F_n = F_{n-1} + F_{n-2}$. By convention, we set $F_0 = 0$ and $F_1 = 1$, so the first few Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, etc. Taking common quotients between terms, it appears that the Fibonacci sequence behaves roughly like a geometric sequence r^n . Since $F_n = F_{n-1} + F_{n-2}$, we expect that such an r would satisfy $r^n = r^{n-1} + r^{n-2}$, or equivalently after dividing through by r^{n-2} , $r^2 - r - 1 = 0$. This gives two possibilities for r:

$$r = \frac{1 + \sqrt{5}}{2} =: \phi \quad \text{or} \quad r = \frac{1 - \sqrt{5}}{2} =: \psi.$$

Neither quite gives the Fibonacci sequence as a geometric series, but a bit of experimentation³ suggests the following proposition.

Proposition 5.2. $F_n = \frac{1}{\sqrt{5}}(\phi^n - \psi^n)$ for all $n \ge 0$.

Since $|\psi| \in (0,1)$, $\psi^n \to 0$ as $n \to \infty$. This explains why $F_n/F_{n-1} \to \phi$ as $n \to \infty$.

Proof. As our inductive step, we will show that if the formula holds for n = k - 1 and n = k then it holds for n = k + 1. Suppose that $F_{k-1} = (\phi^{k-1} - \psi^{k-1})/\sqrt{5}$ and $F_k = (\phi^k - \psi^k)/\sqrt{5}$. Then

$$F_{k+1} = F_k + F_{k-1} = \frac{1}{\sqrt{5}} \left(\phi^k + \phi^{k-1} - (\psi^k + \psi^{k-1}) \right) = \frac{1}{\sqrt{5}} (\phi^{k+1} - \psi^{k+1}),$$

²See Section 5.4 for cool examples!

 $^{^{3}}$ Two standard ways of finding the formula in Proposition 5.2 include finding the eigenvectors of a particular matrix and manipulating a generating function.

where for the last equality we used the fact that ϕ and ψ both satisfy $x^2 = x+1$ and therefore $x^{k+1} = x^k + x^{k-1}$. This is exactly the desired formula $F_{k+1} = (\phi^{k+1} - \psi^{k+1})/\sqrt{5}$, completing our proof of the inductive step.

In our inductive step, we had to assume that the formula held for 2 previous cases. We therefore must check the formula holds for the first 2 cases. Indeed, $(\phi^0 - \psi^0)/\sqrt{5} = 0 = F_0$ and $(\phi^1 - \psi^1)/\sqrt{5} = 1 = F_1$. This completes the proof of the proposition.

To translate once more into our language of proving the family of statements P_n , let P_n be $F_n = (\phi^n - \psi^n)/\sqrt{5}$. For our inductive step, instead of proving $P_n \implies P_{n+1}$ for all n, we proved that P_{n-1} and $P_n \implies P_{n+1}$. This makes our chain of implications look like

 P_0 and $P_1 \implies P_1$ and $P_2 \implies \ldots \implies P_{n-1}$ and $P_n \implies P_n$ and $P_{n+1} \implies \ldots$,

so to prove all of the P_n , we needed to check the base cases of P_0 and P_1 .

Without significantly complicating the technique, we can prove a result invoked during the proof of Proposition 3.4. We claimed that we could factor the polynomial $x^{2n+1} + 1$ as $(x+1)\left(\sum_{i=0}^{2n}(-x)^i\right)$, recalling the familiar example $x^3 + 1 = (x+1)(x^2 - x + 1)$. We aim to prove this inductively.

Proposition 5.3. $x^{2n+1} + 1 = (x+1) \left(\sum_{i=0}^{2n} (-x)^i \right)$ for all $n \in \mathbb{N} \cup \{0\}$.

Proof. Choose n > 0 and suppose that $x^{2n-1} + 1 = (x+1) \left(\sum_{i=0}^{2n-2} (-x)^i \right)$; we aim to show that $x^{2n+1} + 1 = (x+1) \left(\sum_{i=0}^{2n} (-x)^i \right)$. We begin by writing

$$x^{2n+1} + 1 = x^{2n+1} + x^2 - x^2 + 1 = x^2(x^{2n-1} + 1) - x^2 + 1$$

to put the factorization we seek to prove in terms of the one we are assuming.

We invoke our inductive hypothesis to replace the $x^{2n-1} + 1$ term in parentheses, giving

$$x^{2n+1} + 1 = x^2(x+1)\left(\sum_{i=0}^{2n-2} (-x)^i\right) - x^2 + 1.$$

Pulling the x^2 inside the summation amounts to shifting the index up 2, yielding

$$x^{2n+1} + 1 = (x+1)\left(\sum_{i=2}^{2n} (-x)^i\right) - x^2 + 1.$$

To combine terms, we factor the $-x^2 + 1$ as (x + 1)(1 - x) and substitute this to obtain

$$x^{2n+1} + 1 = (x+1)\left(\sum_{i=2}^{2n} (-x)^i\right) + (x+1)(1-x).$$

Lastly, observe that the 1 - x term consists precisely of the i = 0 and i = 1 terms missing from the summation. Rearranging therefore gives

$$x^{2n+1} = (1+x) \left(\sum_{i=0}^{2n} (-x)^i \right),$$

as desired.

Since our argument only depends on the n-1 case being true to prove that the n case is true, we only need to check the n = 0 case. Fortunately, this is immediate as x+1 = (x+1)(1).

The above is a good example of induction being used to prove something other than an explicit formula for a sequence of numbers. In our next example, we use a simple induction to derive an interesting corollary from a more involved direct proof.

We define the binomial coefficient

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

whose name stems from the fact that $\binom{n}{k}$ is the coefficient of x^k in the polynomial $(x+1)^k$. A priori, it is not clear from the given formula that the binomial coefficient is an integer. However, this can be proven by a clever induction argument.⁴ First, we prove that we can write the binomial coefficients $\binom{n+1}{k}$ in terms of the coefficients $\binom{n}{k}$ via what is known as Pascal's triangle formula.

Proposition 5.4. $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ for all $k \in \{1, \ldots, n\}$ and all $n \in \mathbb{N}$.

Proof. This is a proof by computation, where we simply match denominators and rearrange as follows:

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!}$$
$$= \frac{n!k}{k!(n-k+1)!} + \frac{n!(n-k+1)}{k!(n-k+1)!}$$
$$= \frac{n!(n+1)!}{k!(n-k+1)!}$$
$$= \frac{(n+1)!}{k!(n-k+1)!} = \binom{n+1}{k}$$

Now, we know that we can write $\binom{n+1}{k}$ in terms of the binomial coefficients $\binom{n}{k}$ and $\binom{n}{k-1}$. This gives the following corollary.

Corollary 5.5. $\binom{n}{k}$ is an integer for all $k \in \{0, \ldots, n\}$ and all $n \in \mathbb{N}$.

Proof. First, observe that $\binom{n}{0}$ and $\binom{n}{n}$ are both 1 for all $n \in \mathbb{N}$, as can be verified by direct computation. They are thus integers, and we reduce to proving that $\binom{n}{k}$ is an integer for $k \in \{1, \ldots, n-1\}$ and all $n \in \mathbb{N}$. By Proposition 5.4, these coefficients can be expressed as a sum of binomial coefficients with a lower n. This proves the inductive step: if $\binom{n}{k} \in \mathbb{Z}$ for all $k \in \{1, \ldots, n-1\}$ then $\binom{n+1}{k} \in \mathbb{Z}$ for all $k \in \{1, \ldots, n\}$.

We are left to check the base case n = 1. Indeed, both $\binom{1}{0}$ and $\binom{1}{1}$ equal 1 and so are integers, completing the proof.

⁴Another way to prove that $\binom{n}{k}$ is an integer for $0 \le k \le n$ is to prove that it *counts* something; more on this in the next section.

We can also use induction to evaluate certain sums of binomial coefficients.⁵ For example, we have:

Proposition 5.6. $\sum_{k=0}^{n} \binom{n}{k} = 2^{n}$ for all $n \in \mathbb{N}$.

Proof. For the inductive step, suppose $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. We aim to show that $\sum_{k=0}^{n+1} \binom{n+1}{k} = 2^{n+1}$. By Pascal's triangle formula, we have

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \binom{n+1}{0} + \binom{n+1}{n+1} + \sum_{k=1}^n \binom{n+1}{k}$$
$$= 2 + \sum_{k=1}^n \left(\binom{n}{k-1} + \binom{n}{k} \right).$$

Observe that by shifting the index k, we have that $\sum_{k=1}^{n} \binom{n}{k-1} = \sum_{k=0}^{n-1} \binom{n}{k}$, which in turn equals $\sum_{k=0}^{n} \binom{n}{k} - 1$. Likewise, $\sum_{k=1}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} - 1$. Substituting this into the above yields

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = 2 + 2\sum_{k=0}^{n} \binom{n}{k} - 2 = 2\sum_{k=0}^{n} \binom{n}{k}.$$

By the inductive hypothesis, we then have that $\sum_{k=0}^{n+1} \binom{n+1}{k} = 2 \cdot 2^n = 2^{n+1}$, as desired.

We now check the base case n = 1. Via direct computation, we see that $\sum_{k=0}^{1} {1 \choose k} = 1 + 1 = 2^{1}$. This concludes the proof.

The intuition for this result follows from the computation of the cardinality of the powerset of a finite set. See Exercise 7 for more details.

We now conclude the first induction section with one more algebraic induction example: the arithmetic mean/geometric mean (AM-GM) inequality. For this example, however, the induction does *not* proceed as $P_1 \implies P_2 \implies P_3 \dots$ In addition to being a useful result in analysis, the proof of this theorem is a gateway into the world of more advanced inductive arguments.

Theorem 5.7. Let $n \ge 2$ be a natural number and let x_1, \ldots, x_n be nonnegative real numbers. Then their *arithmetic mean* is greater than or equal to their *geometric mean*, i.e.

$$\frac{x_1 + \dots + x_n}{n} \ge \sqrt[n]{x_1 \cdots x_n}.$$

Let's unpack what this means for the case n = 2. We claim that for $x, y \ge 0$, their arithmetic mean (x + y)/2 is at least their geometric mean \sqrt{xy} . We know that $0 \le (\sqrt{x} + \sqrt{y})^2 = x + 2\sqrt{xy} + y$, and rearranging gives

$$\frac{x+y}{2} \ge \sqrt{xy} \tag{1}$$

as desired.

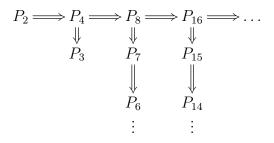
⁵This is the binomial formula for $(x + y)^n$ with x = y = 1. More on the general binomial formula later.

Proof. The fact that we are proving a statement for a finite collection $\{x_n\}$ with varying size may make you think to induct on n, the size of the collection. However, a few minutes of trying to prove the n + 1 case from the n case may be enough to convince yourself that straightforward induction does not quite fit the problem.

Instead, we use the following strategy for our inductive step.

- 1. Assume that the AM-GM inequality holds for 2 numbers and for n numbers, then prove that it holds for 2n numbers.
- 2. Assume that the AM-GM inequality holds for n numbers, then prove that it holds for n-1 numbers.

To see why this is a sufficient inductive step, let P_n be the statement 'the AM-GM inequality holds for *n* nonnegative real numbers'. Observe that if we complete steps 1 and 2, we will have the following implications in place:



It is clear from the diagram that P_n is hit by some chain of implications starting with P_2 for all n > 2. Thus, after completing the above inductive step, it will only remain to prove that P_2 holds.

Step 1: Suppose that the AM-GM inequality is valid for a collection of n nonnegative real numbers, and let x_1, \ldots, x_{2n} be a collection of 2n nonnegative real numbers. We begin by writing

$$\frac{x_1 + \ldots + x_{2n}}{2n} = \frac{1}{2} \left(\frac{x_1 + \ldots + x_n}{n} + \frac{x_{n+1} + \ldots + x_{2n}}{n} \right).$$

In other words, we have shown that the arithmetic mean of the 2n numbers is the arithmetic mean of the arithmetic means of the first n and the last n of them. Applying the assumed case of the AM-GM inequality for n numbers twice, we obtain

$$\frac{x_1 + \ldots + x_{2n}}{2n} \ge \frac{1}{2} \left(\sqrt[n]{x_1 \cdots x_n} + \sqrt[n]{x_{n+1} \cdots x_{2n}} \right).$$

Because the geometric mean of n nonnegative real numbers is itself a nonnegative real number, we can apply the (also assumed) n = 2 case of the AM-GM inequality to see that

$$\frac{x_1 + \dots + x_{2n}}{2n} \ge \sqrt{\sqrt[n]{x_1 \cdots x_n} \sqrt[n]{x_{n+1} \cdots x_{2n}}} = \sqrt[2n]{x_1 \cdots x_{2n}},$$

which is exactly the desired 2n case of the AM-GM inequality!

We see now that moving from n to 2n rather than from n to n + 1 allowed for the necessary consolidation of the two *n*-th roots into the geometric mean of all 2n numbers. This concludes step 1, so we now move to step 2.

Step 2: Suppose that the AM-GM inequality holds for a collection of n nonnegative real numbers, and let x_1, \ldots, x_{n-1} be a collection of n-1 nonnegative real numbers. Let $\alpha = (x_1 + \ldots + x_{n-1})/(n-1)$, the arithmetic mean of the x_n , itself a nonnegative real number. Observe that

$$\alpha = \frac{x_1 + \ldots + x_{n-1} + \alpha}{n}$$

so the arithmetic mean of the x_n is unchanged by adding α to the collection. Now we have a collection of n nonnegative real numbers to which we can apply the AM-GM inequality to obtain

$$\alpha \ge \sqrt[n]{x_1 \cdots x_{n-1} \cdot \alpha}$$

Since all quantities are nonnegative, we can raise both sides to the n-th power without altering the inequality, giving

$$\alpha^n \ge x_1 \cdots x_{n-1} \cdot \alpha.$$

Dividing by α and taking the (n-1)-th root on both sides gives

$$\frac{x_1 + \dots + x_{n-1}}{n-1} = \alpha \ge \sqrt[n-1]{x_1 \cdots x_{n-1}},$$

completing the proof of step 2!

Our proof is thus contingent upon the n = 2 case of the AM-GM inequality. But we discussed after stating the general theorem that this amounts to statement $(\sqrt{x} + \sqrt{y})^2 \ge 0$, arriving at equation (1). We are thus finished the entire proof of the AM-GM inequality. \Box

The AM-GM inequality is just the beginning of using induction to prove complicated chains of implications and provides a hint to the power of the technique. Next week, we will focus on more intricate induction arguments, including some cases in which induction may not initially seem like a viable strategy. We will also examine a few proofs of the fundamental theorem of arithmetic which have been withheld until now.

5.3 Exercises

- 1. For $z \in \mathbb{C}$, let \overline{z} denote the complex conjugate of z. For $z_1, \ldots, z_n \in \mathbb{C}$, prove that
 - (a) $\overline{z_1 + \ldots + z_n} = \overline{z}_1 + \ldots + \overline{z}_n$ and (b) $\overline{z_1 \cdots z_n} = \overline{z}_1 \cdots \overline{z}_n$.
- 2. For $b_1, \ldots, b_n \in \mathbb{N}$ and $z \in \mathbb{C}$, prove the sum/product formula for exponents: $z^{b_1 + \ldots + b_n} = z^{b_1} \cdots z^{b_n}$.
- 3. For differentiable functions f and g, the product rule gives (fg)' = f'g + g'f. For n differentiable functions f_i , what is the derivative of $\prod_{i=1}^n f_i$?
- 4. Find an explicit cubic polynomial formula in n for computing $A_n = \sum_{i=1}^n i^2$ as in the lead-up to Proposition 5.1. Use mathematical induction to prove that your formula holds for all $n \in \mathbb{N}$.

- 5. Find an explicit quartic polynomial formula in n for computing $B_n = \sum_{i=1}^n i^3$ as in the lead-up to Proposition 5.1. Use mathematical induction to prove that your formula holds for all $n \in \mathbb{N}$.
- 6. Prove that for all $n \in \mathbb{N}$, $x^n 1 = (x 1) \left(\sum_{i=0}^{n-1} x^i \right)$.
- 7. Let S be a finite set with n elements. Prove that the set of all subsets of S, referred to as the *powerset* of S and denoted $\mathcal{P}(S)$,⁶ has 2ⁿ elements. Does this match your intuition?
- 8. Google the game 'towers of Hanoi', and use induction on n to prove that for a setup with n disks on 3 pegs, the game can be completed in $2^n 1$ moves.
- 9. Using the limit definition of the derivative

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

and the binomial theorem, prove directly (without induction) that $\frac{d}{dx}(x^n) = nx^{n-1}$. Now prove the same statement by induction in another way, using only the product rule and the fact that the derivative of a constant function is 0.

10. Google 'arithmetic mean-geometric mean inequality' and read a proof different to the one given in this section. How do the two arguments differ? How are they similar?

5.4 Further Reading

CPZ Chapter 6.2	Another explanation of mathematical induction with exer-		
	cises		
"Fibonacci Numbers and	Examples manifestations of the Fibonacci sequence in na-		
Nature" by Dr. Ron Knott	ture both coincidental and not		
	www.maths.surrey.ac.uk/hosted-		
	sites/R.Knott/Fibonacci/fibnat.html		

⁶Note that the powerset includes S itself and the *empty set* with no elements, denoted \emptyset . For example, let $S = \{A, B\}$. Then $\mathcal{P}(S) = \{\emptyset, \{A\}, \{B\}, \{A, B\}\}$.