EXAMPLES OF PROOFS BY INDUCTION

KEITH CONRAD

1. Introduction

In this handout we illustrate proofs by induction from several areas of mathematics: linear algebra, polynomial algebra, and calculus. Becoming comfortable with induction proofs is almost entirely a matter of having lots of experience.

The first kind of induction argument one usually sees is for summation identities, such as $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. That style of induction proof is *not* how induction is generally used in proofs in mathematics! Two questions naturally arise from this.

(1) Why are students sometimes taught only induction with summation identities, if it's not a typical way induction is often used in proofs?
(2) Why are induction proofs of summation identities bad models for induction elsewhere in mathematics?

I will leave the answer to the first question to your imagination. The answer to the second question is that in most uses of induction, you can't argue by trying to "add something to both sides" like in the proof of a summation identity, because what is being proved isn't an identity, so there aren't "both sides" in the first place. Even identities that are proved by induction can't always proceed by manipulating the previously settled cases *into* the next case like in a summation identity.

The right way to approach an inductive argument is to ask yourself "How can I use the earlier cases to prove the next case" rather than "How can I algebraically manipulate the earlier cases into the next case"? In particular, the inductive step does not usually begin by immediately writing down the earlier case and doing something to it. What normally happens is that the earlier (proved) cases appear somewhere within the inductive step, but it could be in the middle or the end. This will be clearer after you read the proofs below.

Another important idea for creating proofs by induction is to *try out small explicit examples*. Can you get the case $n = 2$ from the case $n = 1$ somehow? Can you get the case $n = 3$ from the case $n = 2$ somehow? If you have no idea how to manufacture the inductive step in general, working out small cases of the inductive step successfully can usually help suggest an outline for a proof of the inductive step in general.

2. Linear Algebra

We begin with an inductive proof of a matrix identity where the "do something to both sides" idea from summation identity proofs works.

Theorem 2.1. *Let A be a square matrix and B be an invertible square matrix of the same size. Then $(BAB^{-1})^n = BA^nB^{-1}$ for all integers $n \geq 0$.*

Proof. We argue by induction on n, the exponent. The result is obvious for $n = 0$, when both sides equal the identity matrix. When $n = 1$, the equation $(BAB^{-1})^1 = BAB^{-1}$ is obvious.

Let's see what happens in the case when $n = 2$ (this is not strictly necessary, but is the kind of work a student should do to discover a proof of the inductive step: try small cases). We have

$$\begin{aligned}(BAB^{-1})^2 &= (BAB^{-1}) \cdot (BAB^{-1}) \\ &= BA(B^{-1}B)AB^{-1} \\ &= BAIAB^{-1} \\ &= BAAB^{-1} \\ &= BA^2B^{-1}.\end{aligned}$$

The way B and B^{-1} cancelled in the middle is the key idea. Let's prove the case $n = 3$ from the case $n = 2$ in the same way: now that we know $(BAB^{-1})^2 = BA^2B^{-1}$,

$$\begin{aligned}(BAB^{-1})^3 &= (BAB^{-1})^2 \cdot (BAB^{-1}) \\ &= BA^2B^{-1}BAB^{-1} \\ &= BA^2(B^{-1}B)AB^{-1} \\ &= BA^2IAB^{-1} \\ &= BA^2AB^{-1} \\ &= BA^3B^{-1}.\end{aligned}$$

Hopefully from these two small cases you already see how the inductive step for any n will work. That general step is what we turn to next.

To prove the inductive step, assume the result is established for exponent n: $(BAB^{-1})^n = BA^nB^{-1}$. Then

$$\begin{aligned}(BAB^{-1})^{n+1} &= (BAB^{-1})^n(BAB^{-1}) \\ &= (BA^nB^{-1}) \cdot (BAB^{-1}) \\ &= BA^n(B^{-1}B)AB^{-1} \\ &= BA^nIAB^{-1} \\ &= BA^n \cdot AB^{-1} \\ &= BA^{n+1}B^{-1}\end{aligned}$$

(We used the inductive hypothesis in the second equation.) Thus, the result is true for exponent $n + 1$ if it is true for exponent n.

Since the base case $n = 1$ is true, and assuming the n-th case is true we showed the $(n + 1)$-th case is true, we conclude that the theorem is true for all integers $n \geq 0$. □

In our next theorem from linear algebra whose proof uses induction, we do not argue in the inductive step from one case directly to the next case. Instead the inductive step has a proof of the next case by reducing ourselves to the setting of the previous case. This reduction idea is extremely important: a lot of proofs by induction follow it.

Theorem 2.2. *Let A be a square matrix. Eigenvectors for A having distinct eigenvalues are linearly independent: if $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are eigenvectors for A, with $A\mathbf{v}_i = \lambda_i\mathbf{v}_i$ for distinct scalars $\lambda_1, \ldots, \lambda_r$, then $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are linearly independent.*

As a reminder, an eigenvector for A is a nonzero vector $\mathbf{v}$ such that $A\mathbf{v} = \lambda\mathbf{v}$ for some scalar λ.

Proof. We induct on r, the number of eigenvectors. Since a single nonzero vector is a linearly independent set by itself, the theorem is true (and not interesting!) when $r = 1$. Now suppose $r > 1$ and the result has been verified for $r - 1$. That is, assume it is known that *any* $r - 1$ *eigenvectors of* A *with distinct eigenvalues are linearly independent.* That is our inductive hypothesis.

If we are now given r eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_r$ of A with distinct eigenvalues $\lambda_1, \ldots, \lambda_r$, suppose

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r = \mathbf{0} \tag{2.1}$$

for some scalars c_i. We want to prove each c_i is 0. (That is what linear independence means.)

We need to use A somehow. In equation (2.1), apply A to both sides:

$$c_1A(\mathbf{v}_1) + c_2A(\mathbf{v}_2) + \cdots + c_rA(\mathbf{v}_r) = \mathbf{0},$$

so

$$c_1\lambda_1\mathbf{v}_1 + c_2\lambda_2\mathbf{v}_2 + \cdots + c_r\lambda_r\mathbf{v}_r = \mathbf{0}. \tag{2.2}$$

Look closely at (2.1) and (2.2). They both say some linear combination of the $\mathbf{v}_i$'s is equal to $\mathbf{0}$, but they use different-looking systems of coefficients. By a suitable scaling we will be able to make the coefficients of $\mathbf{v}_1$ in (2.1) and (2.2) match, and then subtracting one equation from the other will cancel that term and leave us with $r - 1$ vectors, to which the inductive hypothesis applies.

The coefficients of $\mathbf{v}_1$ in (2.1) and (2.2) are c_1 and $c_1\lambda_1$. So if multiply through (2.1) by λ_1 we get

$$c_1\lambda_1\mathbf{v}_1 + c_2\lambda_1\mathbf{v}_2 + \cdots + c_r\lambda_1\mathbf{v}_r = \mathbf{0}, \tag{2.3}$$

where the coefficient of $\mathbf{v}_1$ is now $c_1\lambda_1$, just like in (2.2). Now subtract (2.3) from (2.2) and the first term is eliminated:

$$c_2(\lambda_2 - \lambda_1)\mathbf{v}_2 + \cdots + c_r(\lambda_r - \lambda_1)\mathbf{v}_r = \mathbf{0}. \tag{2.4}$$

The vectors $\mathbf{v}_2, \ldots, \mathbf{v}_r$ are $r-1$ eigenvectors of A. Their eigenvalues $\lambda_2, \ldots, \lambda_r$ are distinct (by hypothesis), so the inductive hypothesis tells us that $\mathbf{v}_2, \ldots, \mathbf{v}_r$ are linearly independent. Therefore (2.4) tells us that $c_i(\lambda_i - \lambda_1) = 0$ for $i = 2, 3, \ldots, r$. Since the eigenvalues are distinct, $\lambda_i - \lambda_1 \neq 0$ for $i = 2, \ldots, r$, so $c_i = 0$ for $i = 2, 3, \ldots, r$. Feeding this into (2.1) gives us $c_1\mathbf{v}_1 = \mathbf{0}$, so $c_1 = 0$ as well (since $\mathbf{v}_1 \neq \mathbf{0}$). Thus every c_i is 0. □

3. Polynomials

Proofs about polynomials often proceed using induction on the degree. That is, a general theorem about polynomials is proved first for constant polynomials (degree 0), then for linear polynomials (degree 1), then for quadratic polynomials (degree 2), and so on.

Theorem 3.1. *Let $f(x)$ be a nonconstant polynomial with real coefficients and degree d. Then $f(x)$ has at most d real roots.*

We can't replace "at most d real roots" with "exactly d real roots" since there are nonconstant polynomials like $x^2 + 1$ which have no real roots. (Zero roots is at most two roots, so the theorem is true for $x^2 + 1$.)

Proof. We will argue by induction on the degree d of $f(x)$. Note $d \geq 1$. (Our theorem begins with degree 1, not degree 0.)

A polynomial of degree 1 with real coefficients is of the form $f(x) = ax + b$, where a and b are real and $a \neq 0$. This has exactly one root, namely $-b/a$, and thus *at most* one real root. That settles the theorem for $d = 1$. (Notice we proved the theorem for all polynomials of degree one at the same time.)

Now assume the theorem is known for all polynomials of some degree d with real coeffcients. (This is the inductive hypothesis.) We want to prove the theorem for all polynomials of degree $d + 1$ with real coefficients. (That is the inductive step.)

We consider two cases.

Case 1: The polynomial has no real roots (for instance, $x^2 + 1$ in degree 2). Since there are 0 roots, and $0 \leq d + 1$, the polynomial has at most $d + 1$ real roots.

Case 2: The polynomial has a real root. What we're going to do now (as a method of reducing to an earlier case) is use the root to pull out a linear factor of our polynomial of degree $d + 1$. The complementary factor will have degree d, to which the inductive hypothesis will be applicable.

Write our polynomial of degree $d + 1$ as

$$f(x) = c_{d+1}x^{d+1} + c_d x^d + \cdots + c_1 x + c_0, \tag{3.1}$$

where $c_j \in \mathbf{R}$ and $c_{d+1} \neq 0$. Let r be a real root, so

$$0 = c_{d+1}r^{d+1} + c_d r^d + \cdots + c_1 r + c_0. \tag{3.2}$$

Subtracting (3.2) from (3.1), the terms c_0 cancel and we get

$$f(x) = c_{d+1}(x^{d+1} - r^{d+1}) + c_d(x^d - r^d) + \cdots + c_1(x - r) \tag{3.3}$$

The polynomial formula

$$x^j - r^j = (x - r)(x^{j-1} + rx^{j-2} + \cdots + r^i x^{j-1-i} + \cdots + r^{j-2}x + r^{j-1}).$$

show $x^j - r^j$ is divisible by $x - r$. Write the second factor as $Q_{j,r}(x)$, so

$$x^j - r^j = (x - r)Q_{j,r}(x), \tag{3.4}$$

and substituting (3.4) into (3.3) gives

$$\begin{aligned} f(x) &= \sum_{j=1}^{d+1} c_j(x - r)Q_{j,r}(x) \\ &= (x - r)\sum_{j=1}^{d+1} c_j Q_{j,r}(x) \\ &= (x - r)Q(x), \end{aligned}$$

say. Each $Q_{j,r}(x)$ has real coefficients and all c_j are real, so $Q(x)$ has real coefficients.

Computing the degree of both sides, $\deg f(x) = 1 + \deg Q(x)$, so $\deg Q(x) = d$. We can therefore apply the inductive hypothesis to $Q(x)$: it has at most d real roots. Any root of $f(x)$ is either r or a root of $Q(x)$: if $f(s) = 0$ then $(s - r)Q(s) = 0$, so $s = r$ or $Q(s) = 0$. Since there are at most d real roots of $Q(x)$, tossing r into the list gives us at most $d+1$ real roots of $f(x)$. As $f(x)$ was an arbitrary polynomial of degree $d + 1$ with real coefficients, we have shown all polynomials of degree $d + 1$ with real coefficients have at most $d + 1$ real roots. This completes the proof of the inductive step. □

4. Calculus

We will prove three theorems from calculus using induction. In the first two theorems we will take for granted the product rule. (The proof of the product rule has nothing to do with induction but everything to do with the limit definition of the derivative. This will not be discussed, since this is a handout on induction, not limits.)

Our first inductive proof in calculus is the power rule.

Theorem 4.1. *For $n \geq 1$, $(x^n)' = nx^{n-1}$.*

Proof. We will use the product rule and induction. The case $n = 1$ says $x' = 1$, which can be proved directly from the definition of the derivative as the limit of a Newton quotient. This is left to the reader to check.

To understand the inductive step, first let's check two special cases: the passage from $n = 1$ to $n = 2$ and the passage from $n = 2$ to $n = 3$. Using the product rule on x^2,

$$(x^2)' = (xx)' = xx' + xx' = x + x = 2x.$$

Using the product rule on x^3, written as $x^2 \cdot x$,

$$(x^3)' = (x^2 \cdot x)' = x^2 \cdot x' + x \cdot (x^2)' = x^2 \cdot 1 + x \cdot 2x = x^2 + 2x^2 = 3x^2.$$

Note where the used the formula for $(x^2)'$ in this proof of the formula for $(x^3)'$.

With these special cases in mind, the inductive step in general should make sense: assuming $(x^n)' = nx^{n-1}$, we have by the product rule

$$(x^{n+1})' = (x^n \cdot x)' = x^n \cdot x' + x \cdot (x^n)' = x^n \cdot 1 + x \cdot nx^{n-1} = x^n + nx^n = (n+1)x^n.$$

□

Remark 4.2. Although the power rule is an identity, it *can't* be proved using the simple-minded "do something to both sides" method of induction in proofs of summation identities. Think about it: how are you going to massage both sides of the equation $(x^n)' = nx^{n-1}$ to get $(x^{n+1})'$ on the left side? The exponent appears inside the derivative, so you can't apply some simple operation to $(x^n)'$ to make it $(x^{n+1})'$. You will not get anywhere by starting the inductive step with $(x^n)'$.

What happened instead in the proof is that the product rule lets us write $(x^{n+1})'$ *in terms of* $(x^n)'$, and at that point we can bring in the inductive hypothesis about $(x^n)'$. This is why the right attitude in induction proofs is to ask "How can I use the previous case" instead of "How can I start with the previous case?"

Our next inductive proof in calculus is an example of inducting on the number of terms in a formula.

Theorem 4.3. *For differentiable functions $f_1(x), \ldots, f_n(x)$,*

$$\frac{(f_1(x) \cdots f_n(x))'}{f_1(x) \cdots f_n(x)} = \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)}.$$

Proof. We induct on n, the number of functions.

When $n = 1$, the formula is clear since both sides equal $f_1'(x)/f_1(x)$.

To handle the case $n = 2$, the product rule tells us

$$(f_1(x)f_2(x))' = f_1'(x)f_2(x) + f_1(x)f_2'(x).$$

Divide both sides by $f_1(x)f_2(x)$ and we get the formula we are looking for:

$$\frac{(f_1(x)f_2(x))'}{f_1(x)f_2(x)} = \frac{f_1'(x)f_2(x)}{f_1(x)f_2(x)} + \frac{f_1(x)f_2'(x)}{f_1(x)f_2(x)} = \frac{f_1'(x)}{f_1(x)} + \frac{f_2'(x)}{f_2(x)}.$$

Let's see how to prove the theorem for $n = 3$ by a reduction to the case $n = 2$: we can view a product of three terms $f_1(x)f_2(x)f_3(x)$ as a product of two terms, $(f_1(x)f_2(x))f_3(x)$. By the proved case of (any) two differentiable functions,

$$\begin{aligned}\frac{(f_1(x)f_2(x)f_3(x))'}{f_1(x)f_2(x)f_3(x)} &= \frac{((f_1(x)f_2(x))f_3(x))'}{(f_1(x)f_2(x))f_3(x)} \\ &= \frac{(f_1(x)f_2(x))'}{f_1(x)f_2(x)} + \frac{f_3'(x)}{f_3(x)}.\end{aligned}$$

Again by the case of two differentiable functions,

$$\frac{(f_1(x)f_2(x))'}{f_1(x)f_2(x)} + \frac{f_3'(x)}{f_3(x)} = \frac{f_1'(x)}{f_1(x)} + \frac{f_2'(x)}{f_2(x)} + \frac{f_3'(x)}{f_3(x)}.$$

We can apply the same idea for the general proof of the inductive step. Let's assume the theorem is proved for any n differentiable functions. When $f_1(x), \dots, f_{n+1}(x)$ are any $n+1$ differentiable functions, write

$$f_1(x)\cdots f_n(x)f_{n+1}(x) = (f_1(x)\cdots f_n(x))\cdot f_{n+1}(x), \tag{4.1}$$

where the first product on the right contains n functions. Treating $f_1(x)\cdots f_n(x)$ as a single function, we can view the right side of (4.1) as a product of two functions. Then we can use the proved case of the theorem for two functions to simplify the expression with $n+1$ functions before using the inductive hypothesis:

$$\begin{aligned}\frac{(f_1(x)\cdots f_{n+1}(x))'}{f_1(x)\cdots f_{n+1}(x)} &= \frac{((f_1(x)\cdots f_n(x))\cdot f_{n+1}(x))'}{(f_1(x)\cdots f_n(x))\cdot f_{n+1}(x)} \\ &= \frac{(f_1(x)\cdots f_n(x))'}{f_1(x)\cdots f_n(x)} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{(Case of two functions)} \\ &= \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{(by ind. hyp.),}\end{aligned}$$

and this is what we needed to show for $n+1$ functions. □

Remark 4.4. The inductive step of this proof does *not* start with the identity for n functions and do something to both sides in order to get the identity for $n+1$ functions. Instead the inductive step starts off by writing $(f_1(x)\cdots f_{n+1}(x))'/(f_1(x)\cdots f_{n+1}(x))$ *in terms of* $(f_1(x)\cdots f_n(x))'/(f_1(x)\cdots f_n(x))$ and then the inductive hypothesis can be applied.

Our final inductive proof in calculus is a beautiful formula for $n!$ in terms of integrals.

Theorem 4.5 (Euler)**.** *For $n \geq 0$, $\int_0^\infty x^n e^{-x}\,dx = n!$.*

Proof. We argue by induction on n. For $n = 0$,

$$\int_0^\infty e^{-x}\,dx = \lim_{b\to\infty}\int_0^b e^{-x}\,dx = \lim_{b\to\infty}(-e^{-x})\Big|_0^b = \lim_{b\to\infty} -e^{-b} - (-e^{-0}) = 0 - (-1) = 1.$$

Assuming the theorem is proved for some value of n, we prove it for $n+1$ by expressing $\int_0^\infty x^{n+1}e^{-x}\,\mathrm{d}x$ in terms of $\int_0^\infty x^n e^{-x}\,\mathrm{d}x$ using *integration by parts*:

$$\begin{aligned}
\int_0^\infty x^{n+1}e^{-x}\,\mathrm{d}x &= \lim_{b\to\infty}\int_0^b x^{n+1}e^{-x}\,\mathrm{d}x \\
&= \lim_{b\to\infty}\int_0^b u\,\mathrm{d}v \qquad\qquad (u = x^{n+1}, \mathrm{d}v = e^{-x}\,\mathrm{d}x) \\
&= \lim_{b\to\infty}\ uv\Big|_0^b - \int_0^b v\,\mathrm{d}u \qquad\qquad (\mathrm{d}u = (n+1)x^n, v = -e^{-x}) \\
&= \lim_{b\to\infty}\ -\frac{x^{n+1}}{e^x}\Big|_0^b + \int_0^b (n+1)x^n e^{-x}\,\mathrm{d}x \\
&= \lim_{b\to\infty}\left(-\frac{b^{n+1}}{e^b} + 0\right) + (n+1)\int_0^\infty x^n e^{-x}\,\mathrm{d}x.
\end{aligned}$$

Exponentials grow much faster than polynomials, so $b^{n+1}/e^b \to 0$ as $b\to\infty$. Therefore

$$\int_0^\infty x^{n+1}e^{-x}\,\mathrm{d}x = (0+0) + (n+1)\int_0^\infty x^n e^{-x}\,\mathrm{d}x = (n+1)\int_0^\infty x^n e^{-x}\,\mathrm{d}x.$$

By the inductive hypothesis, this last expression is $(n+1)\cdot n! = (n+1)!$. That completes the proof. □

Remark 4.6. The inductive step did *not* start with the equation $\int_0^\infty x^n e^{-x}\,\mathrm{d}x = n!$ and do something to both sides to turn it into the equation $\int_0^\infty x^{n+1}e^{-x}\,\mathrm{d}x = (n+1)!$. Instead we started with the integral $\int_0^\infty x^{n+1}e^{-x}\,\mathrm{d}x$ and rewrote it *in terms of* $\int_0^\infty x^n e^{-x}\,\mathrm{d}x$, at which point we can bring in the inductive hypothesis about $\int_0^\infty x^n e^{-x}\,\mathrm{d}x$.

The key thing to look for when you read a proof by induction is *how* the inductive step uses earlier cases to get the next case. Review each proof again with this in mind. Frequently the inductive step does *not* start with the inductive hypothesis (that is, an earlier case) right away.