Lecture 10 - Perspectives on Induction

6.042 - March 13, 2003

In this lecture, we consider mathematical induction from various perspectives. We begin with a review of induction. Then we discuss a key step in every induction proof: proving that proposition $P(n)$ implies proposition $P(n+1)$. Next, we see the role induction plays in Peano's axioms for arithmetic. Finally, we use induction to solve a complicated problem.

1 Review

As a review, the principle of induction is stated and used to prove a simple theorem below.

$$\frac{\begin{array}{l} P(0) \\ \forall n\ P(n) \to P(n+1) \end{array}}{\forall n\ P(n)}$$

Here $P(n)$ is a predicate involving the variable n, and the domain of discourse is $\mathbb{N}$. Induction says that if $P(0)$ is true and $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$, then the predicate $P(n)$ is true for all $n \in \mathbb{N}$. Now let's use induction to prove a theorem.

Theorem 1 *For all $n \in \mathbb{N}$:*

$$\sum_{k=0}^{n} k2^k \quad = \quad (n-1) \cdot 2^{n+1} + 2$$

Proof. The proof is by induction on n. Let $P(n)$ be the proposition that:

$$\sum_{k=0}^{n} k2^k \quad = \quad (n-1) \cdot 2^{n+1} + 2$$

First, we must show that $P(0)$ is true. In this case, the summation on the left is equal to zero, and the expression on the right is equal to $(0-1) \cdot 2^{0+1} + 2 = 0$ as well. Therefore, $P(0)$ holds.

Next, we must show that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. In other words, we must show that $P(n+1)$ is true, assuming that $P(n)$ is true. This can be done as follows:

$$\begin{aligned}\sum_{k=0}^{n+1} k2^k &= \left(\sum_{k=0}^{n} k2^k\right) + (n+1)\cdot 2^{n+1} \\ &= \big((n-1)\cdot 2^{n+1} + 2\big) + (n+1)\cdot 2^{n+1} \\ &= ((n+1)-1)\cdot 2^{(n+1)+1} + 2\end{aligned}$$

In the first step, we break the last term out of the summation. The second step relies on the assumption $P(n)$. The final step uses only algebra. This shows that for all $n \in \mathbb{N}$, $P(n+1)$ is true provided $P(n)$ is true.

Therefore, by the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$, which proves the claim. □

2 Proving an Implication

Suppose that we want to prove an implication, such as $A \to B$. How should we structure such an argument? This is an important question, because this situation arises in every induction proof when we try to show that $P(n) \to P(n+1)$. The truth table for the $\to$ connective gives some insight:

A	B	$A \to B$
F	F	T
F	T	T
T	F	F
T	T	T

Let's try to carefully prove that $A \to B$ is true where A is the proposition that $e^\pi > 23$, and B is the proposition that $2e^\pi > 46$. There are two cases to consider: either A is false or A is true.

- First, suppose that A is false. Then the truth table above says that $A \to B$ is true. There is nothing to be done!
- Now, suppose A is true. The truth table says that $A \to B$ is true only if B is also true. Therefore, *we must show that B is true, supposing that A is true. This can be done as follows:*

$$\begin{aligned}2e^\pi &> 2 \cdot 23 \\ &= 46\end{aligned}$$

The first step uses our supposition that A is true, and the second is simplification.

In either case, $A \to B$ is true, so we are done.

Most of the argument above is boilerplate; that is, the text would be exactly the same if A and B were completely different propositions. The crux of the argument is the italicized portion. So when we are trying to prove $A \to B$, we might as well omit all the boilerplate and just write stuff corresponding to the italicized text; that is, we need only prove that B is true, supposing that A is true. This is precisely what we did in the example induction proof:

> Next, we must show that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. In other words, we must show that $P(n+1)$ is true, assuming that $P(n)$ is true. This can be done as follows...

And this is what you should do in every induction proof: in order to prove $P(n) \to P(n+1)$, assume that $P(n)$ is true and show that $P(n+1)$ is true as a consequence.

3 Peano's Postulates

In the late 1800's, Guiseppe Peano proposed five postulates as a basis for mathematics involving the natural numbers. They are listed below, followed by an explanation.

1. $0 \in \mathbb{N}$
2. $\forall x \; S(x) \in \mathbb{N}$
3. $\forall x \forall y \; S(x) = S(y) \;\to\; x = y$
4. $\neg \exists x \; 0 = S(x)$
5. $\forall A \subseteq \mathbb{N} \; (0 \in A \wedge (x \in A \to S(x) \in A)) \;\to\; A = \mathbb{N}$

The first postulate establishes the number 0. The second asserts that every natural number x has a successor, denoted $S(x)$. The third and fourth postulates rule out the possibility that $\mathbb{N}$ is a finite set of numbers containing a cycle, where each number is succeeded by the next number in the cycle. The last postulate is equivalent to mathematical induction.

In Peano's system, the number 3 exists only as $S(S(S(0)))$, the successor of the successor of the successor of 0. Addition is then defined as follows:

$$x + y \;=\; \begin{cases} x \text{ if } y = 0 \\ S(x + z) \text{ if } y = S(z) \end{cases}$$

Using this definition, we can prove that $2 + 2 = 4$. (Woohoo!) Recall that 2 is just shorthand for $S(S(0))$.

$$\begin{aligned} S(S(0)) + S(S(0)) &= S(S(S(0)) + S(0)) \\ &= S(S(S(S(0)) + 0)) \\ &= S(S(S(S(0)))) \end{aligned}$$

The last expression represents the number 4.

3.1 Axiom Systems

Like Euclid's axioms for geometry, Peano's postulates require some tuning to reach modern standards for rigor. For example, nowhere do the postulatees state that $=$ is symmetric or transitive. And the induction axiom quantifies over all *subsets* of the domain of discourse, $\mathbb{N}$; whereas, ordinarily, $\forall x$ means "for all x in the domain of discourse". Furthermore, the induction axiom makes use of sets, which are not defined.

Today, many axiom systems are availabe as foundations for mathematics. The best known is called ZFC, after Zermelo, Fraenkel, and the choice axiom. The ZFC axioms are concerned not with the natural numbers, but with sets. Natural numbers, rational numbers, real numbers and everything else, it turns out, can be defined in terms of sets.

Strangely, the available axiom systems are not quite equivalent; that is, there are some theorems that can be proved from one set of axioms, but not from another. For example, more theorems can be proved from the ZFC axioms than can be proved from Peano's postulates. In particular, Goodstein's Theorem asserts that a certain sequence of natural numbers tends to zero. This theorem can be proved in ZFC, but (provably!) can not be proved from Peano's postulates.

ZFC is sufficient for most mathematics, but there are even more powerful axiom systems. However, with every collection of axioms, there is a latent risk: they may be subtly contradictory; that is, it may be possible to prove both proposition X *and* proposition $\neg X$. This would be a *bad thing*, and the risk of such an inconsistency only increases as the power of the axiom system grows.

No one knows if even the ZFC axioms are consistent. Someone could conceivably find an inconsistency the day before the 6.042 final. Then math would be broken. This might seem absurd, but ZFC itself emerged after traditional set theory collapsed in self-contradiction.

4 The Josephus Problem

Josephus Flavius was a famous Jewish historian of the first century. According to legend, he and some others were trapped in a cave surrounded by Romans. The group resolved that suicide was preferable to capture. So they decided to form a circle and go around it, killing every second person until no one was left. Josephus himself preferred to live. If he could figure out where to stand, then he could be the last one alive, surrender himself to the Romans, and write some more history. For example, suppose that there were a total of 9 people in the cave:

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

Then, according to the rules, people would be killed in the following order: 2, 4, 6, 8, 1, 5, 9, 7, 3. Therefore, Josephus should stand in position 3.

Let $J(n)$ be the position of the last person alive when there are n people in the cave. Our example shows that $J(9) = 3$. What is $J(n)$? That is, where should Josephus stand if there are n people in the cave?

Our solution to this problem involves three steps. First, we build a mathematical model of life and death in the beseiged cave. Then we *guess* a solution to Josephus' problem. Finally, we confirm our guess using mathematical induction.

4.1 A Recurrence Equation

Suppose that there are an even number of people in the cave; that is, suppose $n = 2k$ for some integer k. After one pass around the circle, only k people are left, and person 3 is about to die. The circle looks like this:

$$1\ 3\ 5\ 7\ \ldots\ (2k-1)$$

Now, in effect, we are starting the whole process over again with a circle of k people. The i-th person in the new circle was at position $2i - 1$ in the original circle. We know that the survivor will be the person at position $J(k)$ in the new circle, who was the person at position $2J(k) - 1$ in the original circle. Thus, we have the relation:

$$J(2k) \;=\; 2J(k) - 1$$

Now suppose that there are an odd number of people in the cave; that is, suppose $n = 2k + 1$ for some integer k. After one pass, there are $k + 1$ people left. Then person 1 is killed. At that point, the circle looks like this:

$$3\ 5\ 7\ 9\ \ldots\ (2k+1)$$

Once again, we are effectively starting over with a circle of k people. The i-th person in the new circle was at position $2i+1$ in the original circle. Again, the last survivor will be the person at position $J(k)$, which was the person at position $2J(k)+1$ in the original circle. This gives a second relation:

$$J(2k+1) \;=\; 2J(k)+1$$

As a special case, if there is only one person in the cave, that person is the last one alive; thus, $J(1)=1$. Putting together all these obervations, we have:

$$\begin{aligned} J(1) &= 1 \\ J(2k) &= 2J(k)-1 \qquad (k \geq 1) \\ J(2k+1) &= 2J(k)+1 \qquad (k \geq 1) \end{aligned}$$

We can combine these equations to obtain a recurrence equation for $J(n)$:

$$J(n) \;=\; \begin{cases} 1 & \text{if } n = 1 \\ 2J(n/2)-1 & \text{if } n > 1 \text{ and even} \\ 2J((n-1)/2)+1 & \text{if } n > 1 \text{ and odd} \end{cases}$$

4.2 Guessing an Explicit Formula

Using the recurrence equation, we can easily tabulate values of $J(n)$ for small n:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1	...

The pattern in this table suggests an explicit formula for $J(n)$. In general, as n increases, the value of $J(n)$ bounces up and down. Looking more closely, we see that each time n reaches a power of two, the value of $J(n)$ drops to 1. As n increases further, $J(n)$ begins counting up through the odd integers: 1, 3, 5, 7, ... until n reaches the next power of two. Thus, the value of $J(n)$ is determined by the distance between n and the largest power of two less than n. In particular, if we let $n = 2^m + r$ (where 2^m is the largest power of two less than n), then we can express $J(n)$ as follows:

$$\begin{aligned} J(n) &= J(2^m + r) \\ &= 2r+1 \qquad\qquad (\text{where } 0 \leq r < 2^m) \end{aligned}$$

Let's try to rewrite the right side of this equation purely in terms of n. In doing so, we'll use some notation that may be unfamiliar. Let $\lfloor x \rfloor$ be the largest integer smaller than x. (This is called the "floor of x".) For example, $\lfloor \pi \rfloor = 3$. Also, we'll use $\lg x$ to denote the base-two logarithm of x. For example, $\lg 64 = 6$, since $2^6 = 64$.

In these terms, if $n = 2^m + r$, then $m = \lfloor \lg n \rfloor$ and $r = n - 2^m$. Therefore, we have:

$$\begin{aligned} J(n) &= 2r + 1 \\ &= 2(n - 2^m) + 1 \\ &= 2(n - 2^{\lfloor \lg n \rfloor}) + 1 \end{aligned}$$

Now we have an explicit formula for $J(n)$! We can compute, for example:

$$\begin{aligned} J(97) &= 2(97 - 2^{\lfloor \lg 97 \rfloor}) - 1 \\ &= 2(97 - 64) - 1 \\ &= 67 \end{aligned}$$

But is this answer correct? We based our formula for $J(n)$ on an apparent pattern in a table with only sixteen entries; we have no assurance that that pattern continues. How can we tell whether our formula is correct in general?

4.3 Verifying the Formula by Induction

We can use induction to prove that our explicit formula for $J(n)$ is correct; that is, that it is consistent with the recurrence equation:

$$J(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2J(n/2) - 1 & \text{if } n > 1 \text{ and even} \\ 2J((n-1)/2) + 1 & \text{if } n > 1 \text{ and odd} \end{cases}$$

There will be two cases to consider in the inductive step, because the recurrence equation itself differentiates between even and odd n.

Claim 2 *For all $n \geq 1$:*

$$J(n) = 2(n - 2^{\lfloor \lg n \rfloor}) + 1$$

Proof. The proof is by strong induction on n. Let $P(n)$ be the proposition that:

$$J(n) \;=\; 2(n - 2^{\lfloor \lg n \rfloor}) + 1$$

First, we must prove $P(1)$. In this case, the left side of the equation is $J(1) = 1$, and the right side is $2(1 - 2^{\lfloor \lg 1 \rfloor}) + 1 = 1$ as well. Therefore, equality holds, and so $P(1)$ is true.

Next, we must show that $P(1) \wedge \ldots \wedge P(n-1)$ implies $P(n)$, for each $n > 1$. Assume that propositions $P(1), \ldots, P(n-1)$ are all true.

We consider two cases. If n is even, then we have:

$$\begin{aligned} J(n) &= 2J\left(\frac{n}{2}\right) - 1 \\ &= 2\left(2\left(\frac{n}{2} - 2^{\lfloor \lg(n/2) \rfloor}\right) + 1\right) - 1 \\ &= 2\left(n - 2 \cdot 2^{\lfloor (\lg n) - 1 \rfloor} + 1\right) - 1 \\ &= 2\left(n - 2^{\lfloor \lg n \rfloor}\right) + 1 \end{aligned}$$

The first step uses the recurrence equation for $J(n)$. The second step uses the assumption that proposition $P(n/2)$ is true. The last two steps are simplifications. We conclude that $P(n)$ holds.

On the other hand, if n is odd, then we have:

$$\begin{aligned} J(n) &= 2J\left(\frac{n-1}{2}\right) + 1 \\ &= 2\left(2\left(\frac{n-1}{2} - 2^{\lfloor \lg((n-1)/2) \rfloor}\right) + 1\right) + 1 \\ &= 2\left((n-1) - 2 \cdot 2^{\lfloor (\lg(n-1)) - 1 \rfloor} + 1\right) + 1 \\ &= 2(n - 2^{\lfloor \lg(n-1) \rfloor}) + 1 \\ &= 2(n - 2^{\lfloor \lg n \rfloor}) + 1 \end{aligned}$$

The first step uses the recurrence equation for $J(n)$. The second uses the proposition $P((n-1)/2)$, which we assume to be true. The next two steps are simplifications. In the final step, we use the fact that $\lfloor \lg x \rfloor = \lfloor \lg(x-1) \rfloor$ when x is an odd number greater than one. Again, we conclude that $P(n)$ holds.

Therefore, the proposition $P(n)$ is true for all $n \geq 1$ by strong induction. □