Strong induction

Margaret M. Fleck

7 October 2009

This lecture presents proofs by "strong" induction, a slight variant on normal mathematical induction.

1 Announcements

We aren't quite finished grading the midterm, but expect results very soon (e.g. later today, I hope).

Our course policy says that we don't accept last homeworks. We aren't really strict about stuff that's a couple minutes late but, due to the issues with the dropboxes and my being sick last week and unable to watch the boxes carefully, we've accepted a few homeworks that probably came in later in the day. Starting this week, we plan to crack down on the (very small number) of folks who are pushing their luck (and don't have special circumstances and an official excuse).

Aside from the obvious issues created if homeworks are turned in after the solutions are posted, it's not good for you to get behind. This just results in difficulty preparing for exams/quizzes and work piling up at the end of the term. Cut your losses and turn in what you've got by the deadline.

2 A geometrical example

As a warm-up, let's see another example of the basic induction outline, this time on a geometrical application. *Tiling* some area of space with a certain type of puzzle piece means that you fit the puzzle pieces onto that area of space exactly, with no overlaps or missing areas. A right triomino is a 2-by-2 square minus one of the four squares. (See pictures in Rosen pp. 277-278.) I then claim that

Claim 1 *For any positive integer n, a $2^n \times 2^n$ checkerboard with any one square removed can be tiled using right triominoes.*

> Proof: by induction on n.
>
> Base: Suppose $n = 1$. Then our $2^n \times 2^n$ checkerboard with one square remove is exactly one right triomino.
>
> Induction: Suppose that the claim is true for some integer k. That is a $2^k \times 2^k$ checkerboard with any one square removed can be tiled using right triominoes.
>
> Suppose we have a $2^{k+1} \times 2^{k+1}$ checkerboard C with any one square removed. We can divide C into four $2^k \times 2^k$ sub-checkerboards P, Q, R, and S. One of these sub-checkerboards is already missing a square. Suppose without loss of generality that this one is S. Place a single right triomino in the middle of C so it covers one square on each of P, Q, and R.
>
> Now look at the areas remaining to be covered. In each of the sub-checkerboards, exactly one square is missing (S) or already covered (P, Q, and R). So, by our inductive hypothesis, each of these sub-checkerboards minus one square can be tiled with right triominoes. Combining these four tilings with the triomino we put in the middle, we get a tiling for the whole of the larger checkerboard C. This is what we needed to construct.

3 Strong induction

The inductive proofs you've seen so far have had the following outline:

Proof: We will show $P(n)$ is true for all n, using induction on n.

Base: We need to show that $P(1)$ is true.

Induction: Suppose that $P(k)$ is true, for some integer k. We need to show that $P(k+1)$ is true.

Think about building facts incrementally up from the base case to $P(k)$. Induction proves $P(k)$ by first proving $P(i)$ for every i from 1 up through $k-1$. So, by the time we've proved $P(k)$, we've also proved all these other statements. For some proofs, it's very helpful to use the fact that P is true for all these smaller values, in addition to the fact that it's true for k. This method is called "strong" induction.

A proof by strong induction looks like this:

Proof: We will show $P(n)$ is true for all n, using induction on n.

Base: We need to show that $P(1)$ is true.

Induction: Suppose that $P(n)$ is true for $n = 1 \ldots k$. We need to show that $P(k+1)$ is true.

The only new feature about this proof is that, superficially, we are assuming slightly more in the hypothesis of the inductive step. The difference is actually only superficial, and the two proof techniques are equivalent. However, this difference does make some proofs much easier to write.

4 Postage example

Strong induction is useful when the result for $n = k-1$ depends on the result for some smaller value of n, but it's not the immediately previous value (k). Here's a classic example:

Claim 2 *Every amount of postage that is at least 12 cents can be made from 4-cent and 5-cent stamps.*

For example, 12 cents uses three 4-cent stamps. 13 cents of postage uses two 4-cent stamps plus a 5-cent stamp. 14 uses one 4-cent stamp plus two 5-cent stamps. If you experiment with small values, you quickly realize that the formula for making k cents of postage depends on the one for making $k-4$ cents of postage. That is, you take the stamps for $k-4$ cents and add another 4-cent stamp. We can make this into an inductive proof as follows:

> Proof: by induction on the amount of postage.
>
> Base: If the postage is 12 cents, we can make it with three 4-cent stamps. If the postage is 13 cents, we can make it with two 4-cent stamps. plus a 5-cent stamp. If it is 14, we use one 4-cent stamp plus two 5-cent stamps. If it is 15, we use three 5-cent stamps.
>
> Induction: Suppose that we have show how to construct postage for every value from 12 up through k. We need to show how to construct $k+1$ cents of postage. Since we've already proved base cases up through 15 cents, we'll assume that $k+1 \geq 16$.
>
> Since $k+1 \geq 16$, $(k+1)-4 \geq 12$. So by the inductive hypothesis, we can construct postage for $(k+1)-4$ cents using m 4-cent stamps and n 5-cent stamps, for some natural numbers m and n. In other words $(k+1)-4) = 4m+5n$.
>
> But then $k+1 = 4(m+1)+5n$. So we can construct $k+1$ cents of postage using $m+1$ 4-cent stamps and n 5-cent stamps, which is what we needed to show.

Notice that we needed to directly prove four base cases, since we needed to reach back four integers in our inductive step. It's not always obvious how many base cases are needed until you work out the details of your inductive step.

5 Nim

In the parlour game Nim, there are two players and two piles of matches. At each turn, a player removes some (non-zero) number of matches from one of the piles. The player who removes the last match wins.[1]

[1] Or, in some variations, loses. There seem to be several variations of this game.

Claim 3 *If the two piles contain the same number of matches at the start of the game, then the second player can always win.*

Here's a winning strategy for the second player. Suppose your opponent removes m matches from one pile. In your next move, you remove m matches from the other pile, thus evening up the piles. Let's prove that this strategy works.

> Proof by induction on the number of matches (n) in each pile.
>
> Base: If both piles contain 1 match, the first player has only one possible move: remove the last match from one pile. The second player can then remove the last match from the other pile and thereby win.
>
> Induction: Suppose that the second player can win any game that starts with two piles of n matches, where n is any value from 1 through k. We need to show that this is true if $n = k + 1$.
>
> So, suppose that both piles contain $k + 1$ matches. A legal move by the first player involves removing j matches from one pile, where $1 \leq j \leq k + 1$. The piles then contain $k + 1$ matches and $k + 1 - j$ matches.
>
> The second player can now remove j matches from the other pile. This leaves us with two piles of $k+1-j$ matches. If $j = k+1$, then the second player wins. If $j < k + 1$, then we're now effectively at the start of a game with $k + 1 - j$ matches in each pile. Since $j \geq 1$, $k + 1 - j \leq k$. So, by the induction hypothesis, we know that the second player can finish the rest of the game with a win.

The induction step in this proof uses the fact that our claim $P(n)$ is true for a smaller value of n. But since we can't control how many matches the first player removes, we don't know how far back we have look in the sequence of earlier results $P(1) \ldots P(k)$. Our previous proof about postage can be rewritten so as to avoid strong induction. It's less clear how to rewrite proofs like this Nim example.

6 Prime factorization

The "Fundamental Theorem of Arithmetic" from lecture 8 (section 3.4) states that every positive integer n, $n \geq 2$, can be expressed as the product of one or more prime numbers. Let's prove that this is true.

Recall that a number n is prime if its only positive factors are one and n. n is composite if it's not prime. Since a factor of a number must be no larger than the number itself, this means that a composite number n always has a factor larger than 1 but smaller than n. This, in turn, means that we can write n as ab, where a and b are both larger than 1 but smaller than n.[2]

> Proof by induction on n.
>
> Base: 2 can be written as the product of a single prime number, 2.
>
> Induction: Suppose that every integer between 2 and k can be written as the product of one or more primes. We need to show that $k+1$ can be written as a product of primes. There are two cases:
>
> Case 1: $k+1$ is prime. Then it is the product of one prime, i.e. itself.
>
> Case 2: $k+1$ is composite. Then $k+1$ can be written as ab, where a and b are integers such that a and b lie in the range $[2, k]$. By the induction hypothesis, a can be written as a product of primes $p_1 p_2 \ldots p_i$ and b can be written as a product of primes $q_1 q_2 \ldots q_j$. So then $k+1$ can be written as the product of primes $p_1 p_2 \ldots p_i q_1 q_2 \ldots q_j$.
>
> In both cases $k+1$ can be written as a product of primes, which is what we needed to show.

Again, the inductive step needed to reach back some number of steps in our sequence of results, but we couldn't control how far back we needed to go.

[2] We'll leave the details of proving this as an exercise for the reader.