CMPS 101
Algorithms and Abstract Data Types
Winter 2006

Induction Proofs

Let $P(n)$ be a propositional function of an integer *n*, i.e. *P* is a function whose domain is (some subset of) the set of integers and whose codomain is the set {true, false}. Informally this means $P(n)$ is an assertion whose truth or falsity depends on the integer *n*. *Mathematical Induction* is a proof technique which can be used to prove statements of the form $\forall n \geq n_0 : P(n)$ ("for all *n* greater than or equal to n_0, $P(n)$ is true"). Here n_0 is some fixed integer, and often $n_0 = 1$. Such a proof consists of two steps:

I. **Base Step:** Prove directly that the proposition $P(n_0)$ is true.

IIa. **Induction Step:** Prove $\forall n \geq n_0 : (P(n) \rightarrow P(n+1))$.

To do this pick an arbitrary $n \geq n_0$, and assume for this *n* that $P(n)$ is true. Then show as a consequence that $P(n+1)$ is true. The statement $P(n)$ is often called the *induction hypothesis*, since it is what is assumed in the induction step.

When I and II are complete we conclude that $P(n)$ is true for all $n \geq n_0$. Induction is sometimes explained in terms of a domino analogy. Consider an infinite set of dominos which are lined up and ready to fall. Each domino is labeled by a positive integer, starting with 1 (i.e. $n_0 = 1$). Let $P(n)$ be the assertion: "the *n*th domino falls". First prove $P(1)$, i.e. "the first domino falls", then prove $\forall n \geq 1 : (P(n) \rightarrow P(n+1))$ which says "if any particular domino falls, then the next domino must also fall". When this is done we may conclude $\forall n \geq 1 : P(n)$, "all dominos fall". There are a number of variations on the induction step. The first is just a reparametrization of IIa.

IIb. **Induction Step:** Prove $\forall n > n_0 : (P(n-1) \rightarrow P(n))$

Let $n > n_0$, assume $P(n-1)$ is true, then prove $P(n)$ is true.

Forms **IIa** and **IIb** are said to be based on the *first principle of mathematical induction*. The validity of this principle is proved in the appendix of this handout. Another important variation is called the *second principle of mathematical induction*, or *strong induction*.

IIc. **Induction Step:** Prove $\forall n \geq n_0 : ((\forall k \leq n : P(k)) \rightarrow P(n+1))$

Let $n \geq n_0$, assume that for all *k* in the range $n_0 \leq k \leq n$, $P(k)$ is true. Then prove as a consequence that $P(n+1)$ is true. In this case the term *induction hypothesis* refers to the stronger assumption: $\forall k \leq n : P(k)$.

The strong induction form is often reparameterized as in **IIb**:

IId. **Induction Step:** Prove $\forall n > n_0 : ((\forall k < n : P(k)) \rightarrow P(n))$

Let $n > n_0$, assume for all *k* in the range $n_0 \leq k < n$, that $P(k)$ is true, then prove as a consequence that $P(n)$ is true. In this case the *induction hypothesis* is $\forall k < n : P(k)$.

In terms of the Domino analogy, the strong induction form IId says we must show: (I) the first domino falls, and (II) for any *n*, if all dominos up to but not including the n^{th} domino fall, then the n^{th} domino falls. From (I) and (II) we may conclude that all dominos fall. Strong Induction is most often parameterized as in IId, and form IIc is uncommon. We present here a number of examples of IIa, IIb, and IId.

Example 1 Prove that for all $n \geq 1$:

$$\boxed{\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}}$$

Proof:

Let $P(n)$ be the boxed equation above. We begin the induction at $n_0 = 1$.

I. Base step

Clearly $\sum_{i=1}^{1} i^2 = 1 = \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6}$, showing that $P(1)$ is true.

IIa. Induction Step

Let $n \geq 1$ and assume $P(n)$ is true. That is, for this particular value of *n*, the boxed equation holds. Then

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \qquad \text{(by the induction hypothesis)} \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(n+1) \cdot [(n+1)+1] \cdot [2(n+1)+1]}{6} \qquad \text{(by some algebra)}
\end{aligned}$$

showing that $P(n+1)$ is true.

We conclude that $P(n)$ is true for all $n \geq 1$. ///

One should always state explicitly what is being assumed in the induction step (i.e. what is the induction hypothesis.) One should also make note of the point in the proof at which the induction hypothesis is used.

Example 2 Let $x \in R$ and $x \neq 1$. Show that for all $n \geq 0$:

$$\boxed{\sum_{i=1}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}}$$

Proof:

Here we will use form IIb. Again let $P(n)$ be the boxed equation. We begin the induction at $n_0 = 0$.

I. Base step

$\sum_{i=0}^{0} x^i = x^0 = 1 = \frac{x-1}{x-1}$, showing that $P(1)$ is true.

IIb. Induction Step

Let $n > 0$ and assume that $P(n-1)$ is true, i.e. assume for this particular *n* that: $\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x-1}$.

Then

$$\begin{aligned} \sum_{i=0}^{n} x^i &= \sum_{i=0}^{n-1} x^i + x^n \\ &= \frac{x^n - 1}{x-1} + x^n \qquad \text{(by induction hypothesis)} \\ &= \frac{x^{n+1} - 1}{x-1}, \end{aligned}$$

showing that $P(n)$ is true.

Steps I and II prove that $P(n)$ holds for all $n \geq 0$. ///

Exercise Prove that for all $n \geq 1$: $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2} \right)^2$. Do this using both forms **I**Ia and IIb.

Often the propositional function $P(n)$ is not a formula, but some assertion concerning other types of mathematical structures. Recall that a *graph G* consists of a set *V* of vertices, and a set *E* of edges. Each edge joins two (not necessarily distinct) vertices which we call it's *ends*. Two vertices that are joined by an edge are said to be *adjacent*, and an edge is said to be *incident* with it's two ends. A *path* in *G* is a sequence of adjacent vertices, all of which are distinct, except possibly the first and last. A *cycle* in *G* is a closed path, i.e. one in which the initial and terminal vertices are identical. A graph *G* is said to be *connected* if any two vertices are joined by a path. *G* is called *acyclic* if it contains no cycles. A graph *T* is called a *tree* if it is both connected and acyclic. The following example uses the strong induction IId.

Example 3 Let $n \geq 1$ and suppose *T* is a tree on *n* vertices. Prove that *T* necessarily has $n-1$ edges.

Proof:
Let $P(n)$ be the statement: if *T* is a tree on *n* vertices, then *T* contains $n-1$ edges. We begin at $n_0 = 1$.

I. Base step
If *T* has just one vertex then, being acyclic, it can have no edges, whence $P(1)$ holds.

IId. Induction Step (Strong Induction)
Let $n > 1$ and assume for all *k* in the range $1 \leq k < n$, that $P(k)$ is true. That is, for any such *k*, all trees on *k* vertices contain $k-1$ edges. Now let *T* be a tree on *n* vertices. Pick any edge *e* in *T* and remove it. The removal of *e* splits *T* into two subtrees, each having fewer than *n* vertices. Say the two subtrees have k_1 and k_2 vertices respectively. Since no vertices were removed we must have $k_1 + k_2 = n$. Then by our inductive hypothesis these two subtrees have $k_1 - 1$ and $k_2 - 1$ edges respectively. Upon replacing the edge *e* we see that *T* must contain a total of

$$(k_1 - 1) + (k_2 - 1) + 1 = k_1 + k_2 - 1 = n - 1$$

edges.

The result now follows for all trees by the second principle of mathematical induction. ///

There are many other variations on the induction technique. Occasionally we must use *double induction*, which involves a modification of both the base and induction steps.

Base Step: Prove $P(n_0)$ and $P(n_0+1)$.

Induction Step: Prove $\forall n \geq (n_0+2) : (P(n-2) \wedge P(n-1) \rightarrow P(n))$.

When this is accomplished we may conclude $\forall n \geq n_0 : P(n)$. In terms of our domino analogy we prove that: (I) the first two dominos fall, and (II) if any two consecutive dominos fall, then the very next domino falls. From this we deduce that all dominos fall. The next example uses the Fibonacci numbers F_n which are defined by the recurrence

$$F_n = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F_{n-1} + F_{n-2} & \text{if } n \geq 2 \end{cases}$$

i.e. each term is the sum of the previous two. Using this recurrence, the first few terms of the sequence are readily computed as $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, \ldots$ etc.

Example 4 Let $a = \dfrac{1+\sqrt{5}}{2}$, and $b = \dfrac{1-\sqrt{5}}{2}$. Prove that for all $n \geq 0$, $\boxed{F_n = \dfrac{1}{\sqrt{5}}\left[a^n - b^n\right].}$

Proof:
Let $P(n)$ denote the boxed equation above.

I. Base Step

Observe that $P(0)$ and $P(1)$ are true since $\dfrac{1}{\sqrt{5}}\left[a^0 - b^0\right] = 0 = F_0$ and $\dfrac{1}{\sqrt{5}}\left[a^1 - b^1\right] = 1 = F_1$.

II. Induction Step (Double Induction)

Let $n \geq 2$ and assume that both $P(n-2)$ and $P(n-1)$ are true, i.e. we assume for this *n*

$$F_{n-2} = \frac{1}{\sqrt{5}}\left[a^{n-2} - b^{n-2}\right] \quad \text{and} \quad F_{n-1} = \frac{1}{\sqrt{5}}\left[a^{n-1} - b^{n-1}\right].$$

The induction hypothesis yields

$$F_n = F_{n-1} + F_{n-2} = \frac{1}{\sqrt{5}}\left[a^{n-2}(a+1) - b^{n-2}(b+1)\right].$$

One checks that *a* and *b* are roots of the quadratic equation $x^2 - x - 1 = 0$, whence $a^2 = a+1$, and $b^2 = b+1$. Therefore

$$F_n = \frac{1}{\sqrt{5}}\left[a^{n-2} \cdot a^2 - b^{n-2} \cdot b^2\right] = \frac{1}{\sqrt{5}}\left[a^n - b^n\right],$$

showing that $P(n)$ is true.

Together (I) and (II) imply that $F_n = \dfrac{1}{\sqrt{5}}\left[a^n - b^n\right]$ for all $n \geq 0$. ///

Often the proposition to be proved is an inequality, as the next example illustrates.

Example 5 Define $T(n)$ for $n \in Z^+$ by the recurrence

$$T(n) = \begin{cases} 0 & \text{if } n = 1 \\ T(\lfloor n/2 \rfloor) + 1 & \text{if } n \geq 2 \end{cases}$$

Prove that for all $n \geq 1$, $\boxed{T(n) \leq \lg(n)}$ (which implies $T(n) = O(\lg n)$.)

Proof:
Let $P(n)$ be the boxed inequality above.

I. Base Step
The inequality $T(1) \leq \lg(1)$ reduces to simply $0 \leq 0$, which is obviously true, so $P(1)$ holds.

IId. Induction Step (Strong Induction)
Let $n > 1$ and assume for all k in the range $1 \leq k < n$ that $P(k)$ is true, i.e. $T(k) \leq \lg(k)$. In particular $T(\lfloor n/2 \rfloor) \leq \lg \lfloor n/2 \rfloor$ when $k = \lfloor n/2 \rfloor$. Therefore

$$\begin{aligned} T(n) &= T(\lfloor n/2 \rfloor) + 1 && \text{(by the recurrence for } T(n)\text{)} \\ &\leq \lg \lfloor n/2 \rfloor + 1 && \text{(by the induction hypothesis)} \\ &\leq \lg(n/2) + 1 && \text{(since } \lfloor x \rfloor \leq x \text{ for any } x\text{)} \\ &\leq \lg(n) - \lg(2) + 1 \\ &= \lg(n), \end{aligned}$$

showing that $P(n)$ is true.

Therefore $T(n) \leq \lg(n)$ for all $n \geq 1$ as claimed. ///

Exercise Define $S(n)$ for $n \in Z^+$ by the recurrence

$$S(n) = \begin{cases} 0 & \text{if } n = 1 \\ S(\lceil n/2 \rceil) + 1 & \text{if } n \geq 2 \end{cases}$$

Prove that for all $n \geq 1$: $S(n) \geq \lg(n)$ (whence $S(n) = \Omega(\lg n)$.)

Induction Fallacies
The next few examples illustrate some pitfalls in constructing induction proofs. The result in Example A below was proved correctly in Example 3. We give an invalid proof of the same fact which illustrates an argument some authors have called the "induction trap".

Example A For all $n \geq 1$, if *T* is a tree on *n* vertices then *T* has $n - 1$ edges.

Proof: (Invalid)
Base Step: If $n = 1$ then *T* has no edges, being acyclic.
Induction Step: Let $n \geq 1$ and let *T* be a tree on *n* vertices. Assume that *T* has $n - 1$ edges. Add a new vertex and join it to *T* with a new edge. The resulting graph has $n + 1$ vertices and *n* edges (and is clearly

a tree since connectedness is maintained and no cycles were created.) By the principle of mathematical induction, all trees on n vertices have $n-1$ edges. □

Let us first observe that this argument does not follow the induction paradigm. In this example $P(n)$ is of the form $A(n) \to B(n)$ where $A(n)$ is the statement "T is a tree on n vertices", and $B(n)$ is "T has $n-1$ edges". The induction step should therefore be to prove, for all $n \geq 1$, $P(n) \to P(n+1)$. That is

$$(A(n) \to B(n)) \to (A(n+1) \to B(n+1)).$$

To prove this we should assume $A(n) \to B(n)$, then assume $A(n+1)$, then show as a consequence that $B(n+1)$ is true. In other words we should:

- Assume all trees on n vertices have $n-1$ edges
- Assume T has $n+1$ vertices
- Show as a consequence that T has n edges

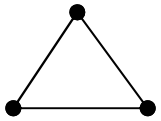
The above argument did not follow this format however. Instead the arguer does the following.

- Assume T has n vertices
- Assume T has $n-1$ edges
- Construct a new tree from T having $n+1$ vertices and n edges

Therefore the above argument was not a proof by induction. Some students would nevertheless hold that the above argument is still valid, even though it is not a true induction proof. The next example shows convincingly that it cannot be valid. First we introduce a few more definitions related to graphs. A graph G is called *simple* if it contains no *loops* (i.e. edges whose end vertices are identical) and no *multiple edges* (i.e. pairs of edges with the same end vertices).

Example B For all $n \geq 1$, if G is a simple graph on n vertices, then G has $n-1$ edges. (False!)

We notice right away that the above statement is false since the graph below provides an elementary counter-example. But consider the following "proof" in light of Example A.



Proof: (Invalid)
Base Step: If $n = 1$ then G has no edges, being simple.
Induction Step: Let $n \geq 1$ and let G be a simple graph on n vertices. Assume that G has $n-1$ edges. Add a new vertex and join it to G with a new edge. The resulting graph has $n+1$ vertices and n edges (and is clearly simple since no loops or multiple edges were created.) By the principle of mathematical induction, all simple graphs on n vertices have $n-1$ edges. □

Observe that Example B follows the format of Example A word for word. Thus if A is valid, so must B be valid. But the assertion "proved" in B is false! Therefore B cannot be a valid argument, and so neither is A. Another fallacy comes about by not proving the induction step for all $n \geq n_0$.

Example C All horses are of the same color.

Proof: (Invalid)
We prove that for all $n \geq 1$: if *S* is a set of *n* horses, then all horses in *S* have the same color. The result follows on letting *S* be the set of all horses. Let $P(n)$ be the boxed statement, and proceed by induction on *n*.

Base Step: Let $n = 1$. Obviously if *S* is a set consisting of just one horse, then all horses in *S* must have the same color. Thus $P(1)$ is true.
Induction Step: Let $n > 1$ and assume that in any set of *n* horses, all horses are of the same color. Let *S* be a set of $n+1$ horses, say $S = \{h_1, h_2, h_3, \ldots, h_{n+1}\}$. Then the sets

$$S' = \{h_2, h_3, \ldots, h_{n+1}\} = S - \{h_1\}$$

and

$$S'' = \{h_1, h_3, \ldots, h_{n+1}\} = S - \{h_2\}$$

each contain exactly *n* horses, and so by the induction hypothesis all horses in S' are of one color, and likewise for S''. Observe that $h_3 \in S' \cap S''$ and that h_3 can have only one color. Therefore the color of the horses in S' is identical to that of the horses in S''. (Note $n > 1 \Rightarrow n \geq 2 \Rightarrow n+1 \geq 3$, so there is in fact a third horse, and he can have only one color.) Since $S = S' \cup S''$ it follows that all horses in *S* are of the same color. Thus $P(n+1)$ is true, showing that $P(n) \rightarrow P(n+1)$ for all $n > 1$. The result now follows by induction. □

Obviously the proposition being proved is false, so there is something wrong with the proof, but what? The base step is certainly correct, and the induction step, as stated, is also correct. The problem is that the induction step was not quantified properly. We should have proved $\forall n \geq 1 : P(n) \rightarrow P(n+1)$ Instead we proved (correctly) that $\forall n > 1 : P(n) \rightarrow P(n+1)$. Indeed it is true that $P(2) \rightarrow P(3)$, $P(3) \rightarrow P(4)$, and $P(4) \rightarrow P(5)$, etc.., but we never proved (and it is false that) $P(1) \rightarrow P(2)$. In terms of the domino analogy, it is as if the first domino falls; and if any domino indexed 2 or above were to fall, then the next domino would fall; but the first domino is not sufficient to topple the second domino, and hence no domino other than the first actually falls.

Appendix: Proof of the first principle of mathematical induction (form IIb).
We prove for any propositional function $P(n)$ defined on the positive integers Z^+, that

$$[P(1) \wedge (\forall n > 1 : P(n-1) \rightarrow P(n))] \rightarrow \forall n \geq 1 : P(n)$$

is a tautology. The proof is based on the *well ordering property* of the positive integers which says: *Any non-empty set of positive integers contains a least element.* We assume this property without proof.

Proof:
Assume that the statements $P(1)$ and $\forall n > 1 : P(n-1) \rightarrow P(n)$ are true. Let $S = \{n \in Z^+ : P(n) \text{ is false}\}$. It will be sufficient to show that $S = \varnothing$, for then $P(n)$ is true for all $n \geq 1$. Assume, to get a contradiction, that $S \neq \varnothing$. Then *S* contains a smallest element *m* by the well ordering property. Since $P(1)$ is true, $1 \notin S$ and so $m \neq 1$. Therefore $m > 1$, and $m - 1 \geq 1$. Since *m* is the smallest element in *S*,

we have $m-1 \notin S$, whence $P(m-1)$ is true. By setting $n = m$ in the statement $\forall n > 1 : P(n-1) \rightarrow P(n)$ we have $P(m-1) \rightarrow P(m)$, and since $P(m-1)$ is true, we conclude that $P(m)$ is also true . Thus $m \notin S$, contradicting the very definition of *m* as the smallest element *in S*. This contradiction shows that our assumption was false, and therefore $S = \varnothing$ as required. ///