CSE 102
Introduction to Analysis of Algorithms
Induction Proofs

Let $P(n)$ be a propositional function, i.e. P is a function whose domain is (some subset of) the set of integers and whose codomain is the set $\{\text{true}, \text{false}\}$. Informally, this means $P(n)$ is a sentence, statement, or assertion whose truth or falsity depends on the integer n. *Mathematical Induction* is a method for proving 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"), where n_0 is a fixed integer. A proof by Mathematical Induction contains 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 that are lined up and ready to fall. Each domino is labeled by a positive integer, starting with n_0. (Often $n_0 = 1$, which we assume here for the sake of definiteness). 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 re-parametrization 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*, and is illustrated below.

IIc. **Induction Step:** Prove $\forall n \geq n_0 : \big(\forall k \leq n : P(k)\big) \rightarrow P(n+1)$
Let $n \geq n_0$, assume for all k in the range $n_0 \leq k \leq n$ that $P(k)$ 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:$\forall k \leq n : P(k)$, which can also be written $P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(n)$.

The strong induction form is often re-parameterized 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 $P(n)$ is true. In this case, the *induction hypothesis* is $\forall k < n : P(k)$, or $P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(n-1)$.

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, i.e. that

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

We must show that $P(n+1)$ holds, i.e. that

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

Then

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

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \qquad \text{by the induction hypothesis}$$

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

$$= \frac{(n+1) \cdot [(n+1)+1] \cdot [2(n+1)+1]}{6} \qquad \text{by some algebra}$$

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

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

There are several points of correctness and clarity to remember when writing an induction proof. Always state explicitly (1) the induction hypothesis, (2) the statement to be proved on the induction step, and (3) the point in the proof where the induction hypothesis is used.

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

$$\boxed{\sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}}$$

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**
$P(1)$ is true since

$$\sum_{i=0}^{0} x^i = x^0 = 1 = \frac{x - 1}{x - 1}$$

IIb. **Induction Step**
Let $n > 0$ and assume that $P(n-1)$ is true, i.e. assume for this *n* that

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}$$

We must show that $P(n)$ is true, i.e.

$$\sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}$$

Observe that

$$\sum_{i=0}^{n} x^i = \sum_{i=0}^{n-1} x^i + x^n$$

$$= \frac{x^n - 1}{x - 1} + x^n \quad \text{by the induction hypothesis}$$

$$= \frac{x^{n+1} - 1}{x - 1} \quad \text{by some algebra}$$

showing that $P(n)$ is true.

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

Exercise 1 Prove the following formulas using both induction forms **IIa** and **IIb**.

a. Show that for all $n \geq 1$:

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

b. Show that for all $n \geq 1$:

$$\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

Often the proposition to be proved is not an equation, but some other type of assertion, like an inequality, as in the following example.

Example 3 Define the function $T(n)$ 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 $n \geq 1$: $\boxed{T(n) \leq lg(n)}$, and therefore $T(n) = O(\lg(n))$

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

I. Base Step

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

IId. Induction Step

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 when $k = \lfloor n/2 \rfloor$, we have $T(\lfloor n/2 \rfloor) \leq \lg\lfloor n/2 \rfloor$. We must show that $T(n) \leq \lg(n)$. Thus

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

showing that $P(n)$ is true, and therefore $T(n) \leq \lg(n)$ for all $n \geq 1$, as claimed. ■

Exercise 2 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 $n \geq 1$: $S(n) \geq \lg(n)$, and hence $S(n) = \Omega(\lg(n))$.

There are many other variations on the (weak and strong) Induction Principles. Occasionally it is necessary that an induction proof include multiple base cases, with the following outline.

I **Base Step:** Prove $P(1), P(2), \ldots, P(n_0)$.

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

II **(Strong) Induction Step:** Prove $\forall n > n_0: (P(1) \wedge P(2) \wedge \cdots \wedge P(n-1)) \rightarrow P(n)$.

From I and II (either case), we conclude that $\forall n \geq 1 : P(n)$.

Example 4 Define a function $T(n)$ by the following recurrence.

$$T(n) = \begin{cases} 1 & \text{if } 1 \leq n \leq 2 \\ 4T(\lfloor n/3 \rfloor) + n & \text{if } n \geq 3 \end{cases}$$

Show that $\boxed{T(n) \leq n^2}$ for all $n \geq 1$, whence $T(n) = O(n^2)$.

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

I. Base Step
Observe $T(1) = 1 \leq 1^2$ and $T(2) = 1 \leq 2^2$, so both $P(1)$ and $P(2)$ are true.

II. Induction Step (strong version)
Let $n > 2$ and assume for all k in the range $1 \leq k < n$ that $P(k)$ is true, i.e. $T(k) \leq k^2$. In particular when $k = \lfloor n/3 \rfloor$, we have $T(\lfloor n/3 \rfloor) \leq \lfloor n/3 \rfloor^2$. We must show $T(n) \leq n^2$ is true. Observe that

$$\begin{aligned} T(n) &= 4T(\lfloor n/3 \rfloor) + n && \text{by the definition of } T(n) \\ &\leq 4\lfloor n/3 \rfloor^2 + n && \text{by the induction hypothesis} \\ &\leq 4(n/3)^2 + n && \text{since } \lfloor x \rfloor \leq x \text{ for any } x \\ &= \frac{4}{9}n^2 + n \\ &\leq n^2 \end{aligned}$$

where the last inequality follows from

$$n > 2 \quad \Rightarrow \quad \frac{9}{5} \le n \quad \Rightarrow \quad n \le \frac{5}{9}n^2 \quad \Rightarrow \quad \frac{4}{9}n^2 + n \le n^2.$$

Therefore $P(n)$ is true, and hence $T(n) \le n^2$ for all $n \ge 1$, as claimed. ■

To see why two base cases were necessary in this last example, consider exactly which prior values are needed to compute each $T(n)$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	⋯
$\lfloor n/3 \rfloor$	·	·	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5	6	⋯

It's as if there are two independent sets of dominoes in this induction proof. One set tracing back to the case $n = 1$, and the other set tracing back to $n = 2$. For instance, the statements $P(3), P(4)$ and $P(5)$ all depend on $P(1)$, while $P(6)$, $P(7)$ and $P(8)$ depend on $P(2)$. If the base case $n = 2$ had been left out, then the truth of statements $P(6)$, $P(7)$ and $P(8)$ would not follow. Likewise any statement, such as $P(18)$, that depends on $P(6)$, traces back to the statement $P(2)$. In general, one checks that the truth of $P(n)$ depends on the base case $P\left(\left\lfloor n/3^{\lfloor \log_3 n \rfloor} \right\rfloor\right)$.

Another variation involving a modification of both base and induction steps is sometimes called *Double Induction*.

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

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

In terms of our domino analogy, we prove: (I) the first two dominos fall, and (II) if any two consecutive dominos fall, then the very next domino falls. From (I) and (II) we deduce that all dominos fall. This version lies somewhere between week and strong induction.

The next example concerns the Fibonacci sequence F_n defined by the recurrence

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \quad \text{for } n \ge 2 \end{cases}$$

i.e. each term in the sequence is the sum of the preceding two. Using this recurrence formula, the first few terms of the Fibonacci sequence are easily computed as $(0, 1, 1, 2, 3, 5, 8, 13, 21, \dots \dots)$.

Example 5
Let $a = (1 + \sqrt{5})/2$, and $b = (1 - \sqrt{5})/2$. Prove that for all $n \ge 0$:

$$\boxed{F_n = \frac{a^n - b^n}{\sqrt{5}}}$$

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

I. **Base Step** Observe that both $P(0)$ and $P(1)$ are true since

$$\frac{a^0 - b^0}{\sqrt{5}} = 0 = F_0 \quad \text{and} \quad \frac{a^1 - b^1}{\sqrt{5}} = 1 = F_1$$

II. **Induction Step** Let $n \geq 2$, and assume both $P(n-2)$ and $P(n-1)$ are true. Thus for this n we have

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

We must show that $P(n)$ is true:

$$F_n = \frac{a^n - b^n}{\sqrt{5}}.$$

The induction hypothesis yields

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &= \frac{a^{n-2} - b^{n-2}}{\sqrt{5}} + \frac{a^{n-1} - b^{n-1}}{\sqrt{5}} \\ &= \frac{a^{n-2}(a+1) - b^{n-2}(b+1)}{\sqrt{5}} \end{aligned}$$

It can be verified that a and b are roots of the quadratic equation $x^2 - x - 1 = 0$. Thus $a^2 = a + 1$, and $b^2 = b + 1$, from which it follows that

$$F_n = \frac{a^{n-2} \cdot a^2 - b^{n-2} \cdot b^2}{\sqrt{5}} = \frac{a^n - b^n}{\sqrt{5}},$$

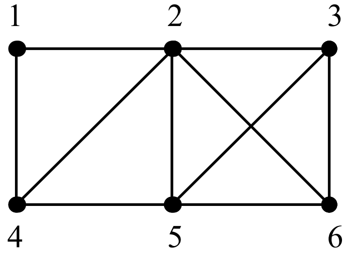
and hence $P(n)$ is true.

We conclude that $F_n = (a^n - b^n)/\sqrt{5}$ for all $n \geq 0$, as claimed. ■

Exercise 3 Let F_n be the Fibonacci sequence and define a as above. Show that $F_n \geq a^{n-2}$ for all $n \geq 2$, and hence $F_n = \Omega(a^n)$. (Prove this by double induction, not as a consequence of the last example.)

A Short Introduction to Graphs

The propositional function $P(n)$ in an induction proof is not always a formula or an inequality, but instead an assertion concerning other types of mathematical structures, like graphs, trees, networks, etc. A *graph* G is a pair of sets $G = (V, E)$ where V is the set of *vertices*, and E is the set of *edges*. Each edge joins two distinct vertices, called its *ends*, and no two edges have the same ends. Abstractly, an edge is an unordered pair of vertices, i.e. a 2-element subset of V. Two vertices that are joined by an edge are said to be *adjacent*, and an edge is said to be *incident* with its two end vertices. Two edges are said to be *adjacent* if they are incident with a common end vertex. Thus in the example below: vertex 1 is adjacent to vertex 4, vertex 2 is incident with edge 26, and edge 45 is adjacent to edge 53.

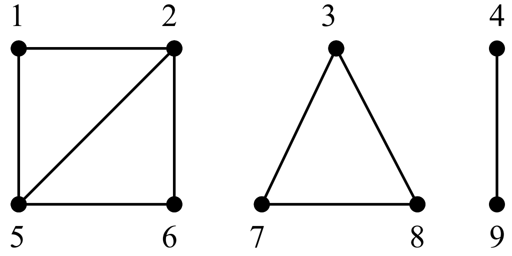


V={1, 2, 3, 4, 5, 6} E={12, 14, 23, 24, 25, 26, 35, 36, 45, 56}

Let $x, y \in V$. An *x-y path* in G is a sequence of vertices starting with x and ending with y, in which each consecutive pair of vertices are adjacent. We require that all vertices other than x and y be distinct, and that each edge in the sequence be traversed at most once. We call x the initial vertex and y the terminal vertex. If $x = y$, then the path is called a *cycle*. The *length* of a path is the number of edges traversed by the sequence. In the above example we have:

A 1-6 path of length 5: 1, 2, 4, 5, 3, 6
A 1-6 path of length 3: 1, 4, 5, 6
Another 1-6 path of length 3: 1, 2, 3, 6
A cycle of length 6: 1, 2, 6, 3, 5, 4, 1
A cycle of length 3: 6, 2, 5, 6

A graph is said to be *connected* if it contains an *x-y* path for every $x, y \in V$, otherwise it is called *disconnected*. The example above is clearly connected, while the following example is disconnected.

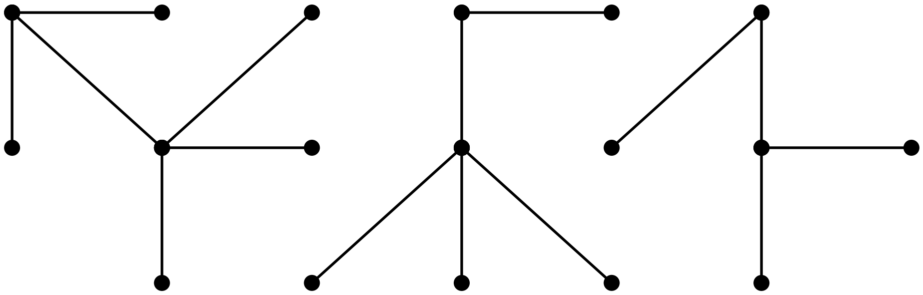


V={1, 2, 3, 4, 5, 6, 7, 8, 9} E={12, 15, 25, 26, 56, 37, 38, 78, 49}

A *subgraph* of a graph G is a graph H in which $V(H) \subseteq V(G)$, and $E(H) \subseteq E(G)$. In the above example $(\{1, 2, 5\}, \{12, 15, 25\})$ is a connected subgraph, while $(\{2, 3, 6, 7\}, \{26, 37\})$ is a disconnected subgraph.

A subgraph H is called a *connected component* of G if it is (i) connected, and (ii) maximal with respect to property (i), i.e. any other subgraph of G that contains H is disconnected. The previous example has three connected components: $(\{1, 2, 5, 6\}, \{12, 15, 25, 26, 56\})$, $(\{3, 7, 8\}, \{37, 38, 78\})$, and $(\{4, 9\}, \{49\})$. Obviously a graph is connected if and only if it has exactly one connected component.

A graph G is called *acyclic* if it contains no cycles. A *tree* is a graph that is both connected and acyclic. The connected components of an acyclic graph are therefore trees. For this reason an acyclic graph is sometimes called a *forest*. The following graph is a forest with three connected components.



Observe that the number of edges in each tree of this forest is one less than the number of vertices. This is true for all trees, as we now show.

Example 6 For all $n \geq 1$, $\boxed{\text{if } T \text{ is a tree on } n \text{ vertices, then } T \text{ contains } n-1 \text{ edges.}}$

Proof:
Let $P(n)$ be the boxed statement above. We begin at $n_0 = 1$, and use the strong induction form IId.

I. **Base step**
If T has just one vertex, then T can have no edges, since in the definition of a graph, each edge has distinct end vertices. Therefore $P(1)$ holds.

IId. **Induction Step**
Let $n > 1$ and assume for all k in the range $1 \leq k < n$, that $P(k)$ is true, i.e. for any such k, all trees on k vertices contain $k-1$ edges. We must show that $P(n)$ is true, i.e. any tree with n vertices has $n-1$ edges.

Let T be a tree having n vertices, and remove any edge e from T. The removal of e splits T into two subtrees, each having fewer than n vertices. (This follows from some elementary facts about graphs which we omit. See the handout on Graph Theory for details.) Call the two subtrees T_1 and T_2 respectively, and suppose T_i has k_i vertices $(i = 1, 2)$. Since no vertices were removed, we must have $k_1 + k_2 = n$. By our induction hypothesis, each T_i has $k_i - 1$ edges $(i = 1, 2)$. Upon re-inserting edge e, we see that the number of edges originally in T was

$$|E(T_1)| + |E(T_2)| + 1 = (k_1 - 1) + (k_2 - 1) + 1$$

$$= k_1 + k_2 - 1$$

$$= n - 1$$

as required.

By the second principle of mathematical induction, all trees on *n* vertices have $n - 1$ edges. ■

Induction Fallacies

The next three examples illustrate some pitfalls to be avoided when constructing induction proofs. The result in Example A below was proved correctly in Example 6. Here we give an invalid proof of the same fact illustrating an argument that 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: (Valid) If $n = 1$, then *T* has no edges, since each edge must have distinct end vertices.
Induction Step: (Invalid) 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. To be precise, the new edge has the new vertex at one end, and the other end can be any existing vertex in *T*. The resulting graph has $n + 1$ vertices and *n* edges. This new graph must be 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. □

First note that the base step is identical to that in Example 6, and is correct. For the induction step, the argument attempts to follow IIa, but fails to do so. In this example $P(n)$ is of the form $A(n) \rightarrow B(n)$ 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 $n \geq 1$, that $P(n) \rightarrow P(n + 1)$, i.e.

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

To prove this, we should assume $A(n) \rightarrow B(n)$, 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

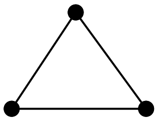
The argument did not follow this format however. Instead it does the following.

- 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 argument was not a proof by induction. Some students would nevertheless hold that the argument is still valid, even though it is not a true induction proof. The next example shows convincingly that it cannot be valid.

Example B For all $n \geq 1$, if G is a connected 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: (Valid) If $n = 1$ then G has no edges, since each edge must have distinct end vertices.
Induction Step: (Invalid) Let $n \geq 1$ and let G be a connected 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. This new graph is also connected since the new vertex is joined to the rest by the new edge. By the principle of mathematical induction, all connected graphs on n vertices have $n-1$ edges. □

Notice that Example B follows the format of Example A exactly. 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.

Example C All horses have the same color.

Proof: (Invalid)
We prove that for all $n \geq 1$

$$\boxed{\text{If } S \text{ is a set of } n \text{ horses, then all horses in } S \text{ have the same color}}$$

It follows that any finite set of horses have the same color, and in particular, the set of all horses have the same color. 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 have the same color. Let S be a set of $n+1$ horses, say $S = \{\, h_1, h_2, h_3, \dots, h_{n+1}\}$. Then the sets

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

and

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

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 have 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.

Justification of the Induction Principles

Here we prove the validity of the first and second principles of mathematical induction (1st PMI and 2nd PMI). Both principles follow from a basic property of the integers, called the *well ordering property* (WOP), which says: *Any non-empty set of positive integers contains a least element.* We assume this property, for the moment, without proof.

Theorem 1 (1st PMI form IIb)

For any propositional function $P(n)$ defined on the positive integers, the following sentence is true:

$$\left[P(1) \land \left(\forall n > 1: P(n-1) \rightarrow P(n)\right)\right] \rightarrow \forall n \geq 1: P(n)$$

Proof:

Assume that $P(1)$ and $\forall n > 1: P(n-1) \rightarrow P(n)$ are both true. Let

$$S = \{\, n \in Z^+ \mid \ P(n) \ \text{ is false}\,\}$$

It is sufficient to show that $S = \emptyset$, since then $P(n)$ is true for all $n \geq 1$. Assume, to get a contradiction, that $S \neq \emptyset$. Then, by the well ordering property of Z^+, S contains a least element, call it *m*. Since $P(1)$ is true, we have $1 \notin S$. Therefore $m > 1$, and $m - 1$ is a positive integer. Since *m* is the smallest element in *S*, we must have $m - 1 \notin S$, whence $P(m-1)$ is true.

We have assumed for all $n > 1$ that $P(n-1) \rightarrow P(n)$ is true. In particular for $n = m$, we have

$$P(m-1) \rightarrow P(m)$$

Since both $P(m-1)$ and $P(m-1) \rightarrow P(m)$ are true, we must conclude that $P(m)$ is also true. Therefore $m \notin S$, contradicting the very definition of *m* as the smallest element *in S*. This contradiction shows our assumption was false, and $S = \emptyset$ as required. ■

Theorem 2 (2nd PMI form IId)

For any propositional function $P(n)$ defined on the positive integers, the following sentence is true:

$$\Big[P(1) \land \Big(\forall n > 1: \big(\forall k < n: P(k)\big) \rightarrow P(n)\Big)\Big] \rightarrow \forall n \geq 1: P(n)$$

Proof:

Assume $P(1)$ and $\forall n > 1: \big(\forall k < n: P(k)\big) \rightarrow P(n)$ are both true. Again let

$$S = \{\, n \in Z^+ \mid \ P(n) \ \text{ is false}\,\}$$

As before we show $S = \emptyset$, hence $P(n)$ is true for all $n \geq 1$. Assume, to get a contradiction, that $S \neq \emptyset$. By the well ordering property of $\mathbb{Z}^+$, S contains a least element, which we call m. Since $P(1)$ is true, we have $1 \notin S$. Therefore $m > 1$, and $m - 1 \geq 1$. Since m is the smallest element in S, we have for any k in the range $1 \leq k \leq m - 1$ that $k \notin S$, whence $P(k)$ is true. In other words, $\forall k < m: P(k)$ is true.

We have assumed for all $n > 1$, that $\big(\forall k < n: P(k)\big) \rightarrow P(n)$ is true. In particular, when $n = m$, we have

$$\big(\forall k < m: P(k)\big) \rightarrow P(m)$$

Since both $\forall k < m: P(k)$ and $\big(\forall k < m: P(k)\big) \rightarrow P(m)$ are true, we may conclude $P(m)$ is also true. Therefore $m \notin S$, again contradicting the definition of m as the smallest element *in S*. Our assumption was therefore false, and $S = \emptyset$ as required. ■

Although we proved both theorems independently, it is possible to show that each implies the other, i.e. theorems 1 and 2 are logically equivalent. In fact both theorems are equivalent to the well ordering property itself. We prove below that the well ordering property (WOP) follows from the 2nd PMI, and leave the remaining equivalences as an exercise. The terms "strong" and "weak" are therefore misnomers in some sense, since neither theorem is stronger than the other. The term "strong induction" refers instead to the stronger assumption being made in the induction step.

Theorem 3 (The well ordering property)
Any non-empty set of positive integers contains a least element.

Proof:
Assume S is a set containing only positive integers and that $S \neq \emptyset$. We must show that S contains a least element. We will prove the following fact using strong induction form IId.

$$\forall n \geq 1\colon\ (\, n \in S \ \Rightarrow\ S \ \text{contains a least element}\,)$$

Since $S \neq \emptyset$, it must contain at least one positive integer n, so the above statement implies that S contains a least element, as required.

I. If $1 \in S$ then certainly 1 is the least element of S, since 1 is less than or equal to all positive integers.

II. Let $n > 1$ and assume

$$\forall k < n\colon\ (\, k \in S \ \Rightarrow\ S \ \text{contains a least element}\,)$$

We must show that

$$n \in S \ \Rightarrow\ S \text{ contains a least element}$$

Suppose $n \in S$. If it is the case that $n \leq k$ for all $k \in S$, then n is the least element in S, and we are done. If not, then there exists a positive integer $k < n$ with $k \in S$. By the induction hypothesis, we have that S contains a smallest element. In any case, S contains a least element.

It follows from the 2nd PMI that any non-empty set of positive integers contains a least element. ■

Exercise 4 Prove that 1st PMI ⇒ 2nd PMI.

When this exercise is done, we have the implications WOP ⇒ 1st PMI ⇒ 2nd PMI ⇒ WOP, which proves the logical equivalence of all three statements.