Induction is a method for proving theorems of the form "For all n, $P(n)$", where n ranges over the positive integers. It is particularly useful in computer science when reasoning about the correctness of algorithms. Let's start with an example.

Theorem 1. *For every n, the sum of the integers from 1 to n is $n(n+1)/2$.*

The kinds of proofs we learned last time don't seem to help. Before we do the proof let's gain some confidence that the theorem is plausible by working out a few small examples:

- When $n = 1$, $(1+1)/2 = 1$.
- When $n = 2$, $1+2 = 3$, and $2 \cdot (2+1)/2 = 3$.
- When $n = 3$, $1+2+3 = 6$ and $3 \cdot (3+1)/2 = 6$.
- When $n = 4$, $1+2+3+4 = 10$ and $4 \cdot (4+1)/2 = 10$.

The cases check out, but we cannot go on like this forever. How can we prove the theorem for *all* n? Let's give the predicate "The sum of integers from 1 to n is $n(n+1)/2$ a name; call it $P(n)$.

Induction models the following reasoning process. First, we prove $P(1)$. Then we prove $P(2)$; in our proof for $P(2)$, we can assume that $P(1)$ is known to be true (use it as an axiom). When we prove $P(3)$, we can assume $P(2)$ to be true, and so on:

$$\frac{P(1) \qquad P(1) \longrightarrow P(2) \qquad P(2) \longrightarrow P(3) \qquad P(3) \longrightarrow P(4)}{P(1) \text{ AND } P(2) \text{ AND } P(3) \text{ AND } P(4)}$$

We can extend this reasoning to a *general* value of n. If we prove $P(1)$ is true, and we prove that for every $n \geq 1$, $P(n+1)$ is true *assuming* $P(n)$, then $P(n)$ must be true for all n:

Induction proof method:

$$\frac{P(1) \qquad P(n) \longrightarrow P(n+1) \text{ for all positive integers } n}{P(n) \text{ for all positive integers } n}$$

Proposition $P(1)$ is called the *base case*; proposition "$P(n) \longrightarrow P(n+1)$ for all n" is called the *inductive step*. To prove the inductive step, you can try any of the methods from last lecture.

Proof of Theorem 1. We prove the theorem by induction on n. Let $S(n)$ denote the sum of the first n integers. Then the proposition says that

$$S(n) = \frac{n(n+1)}{2} \qquad \text{for all positive integers } n$$

Base case $n = 1$: $S(1) = 1$ and $1(1+2)/2 = 1$, so $S(1) = 1(1+1)/2$.

Inductive step: We need to show that for every positive integer n

$$S(n) = \frac{n(n+1)}{2} \quad \longrightarrow \quad S(n+1) = \frac{(n+1)(n+2)}{2}.$$

Let n be any positive integer. We assume $S(n) = n(n+1)/2$. Then

$$S(n+1) = S(n) + (n+1)$$

so, by our assumption that $S(n) = n(n+1)/2$, we get

$$S(n+1) = S(n) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

It follows by induction that $S(n) = n(n+1)/2$ for all positive integers n. □

1 More proofs by induction

Let's do another example, this one involving an inequality. The *factorial* of n, denoted by $n!$, is the number obtained by multiplying all integers from 1 to n:

$$n! = 1 \cdot 2 \cdots n.$$

Theorem 2. *For every integer $n \geq 4, n! > 2^n$.*

We will prove this theorem by induction. The base case here will be $n = 4$.

Proof. We prove the theorem by induction on n.

Base case $n = 4$: $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 > 16 = 2^4$, so the base case holds.

Inductive step: We need to show that for every positive integer $n \geq 4$

$$n! > 2^n \quad \longrightarrow \quad (n+1)! > 2^{n+1}.$$

Let n be any positive integer greater or equal to 4. We assume $n! > 2^n$. Then

$$(n+1)! = n! \cdot (n+1) > 2^n \cdot (n+1) > 2^n \cdot 2 = 2^{n+1}.$$

It follows by induction that $n! > 2^n$ for all integers $n \geq 4$. □

How did one come up with the inequality $2^n \cdot (n+1) > 2^n \cdot 2$? It looks like a lucky guess, but we can reason about it backwards. In the inductive step, we *need* to prove that $2^n \cdot (n+1) > 2^{n+1}$. If we factor out 2^n from both sides, we are left with showing that $n + 1 > 2$. This is the same as saying $n > 1$, which is certainly true under the assumption $n \geq 4$.

This kind of "backwards reasoning" is often helpful in proofs by induction. You are encouraged to use it as part of your scratch work, but not in the written proof.

Theorem 3. *For every positive integer n, $n^3 - n$ is a multiple of 6.*

You can prove this theorem in several ways. Try a proof by cases at home. Here we'll do it using induction.

Proof. We prove the theorem by induction on n.

Base case $n = 1$: $1^3 - 1 = 0$, which is a multiple of 6, so the base case holds.

Inductive step: We need to show that for every positive integer n,

$$n^3 - n \text{ is a multiple of } 6 \quad \longrightarrow \quad (n+1)^3 - (n+1) \text{ is a multiple of } 6.$$

Let n be any positive integer. We assume that $n^3 - n$ is a multiple of 6. Then

$$(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = n^3 + 3n^2 + 2n = (n^3 - n) + 3(n^2 + n)$$

By inductive hypothesis, $n^3 - n$ is a multiple of 6. In the last lecture we showed that $n^2 + n$ is even for all n, so $3(n^2 + n)$ is also a multiple of 6. Therefore $(n^3 - n) + 3(n^2 + n)$ is also a multiple of 6.

It follows by induction that $n^3 - n$ is a multiple of 6 for all positive integers n. □

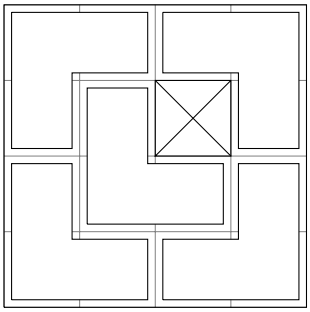
Where did the equality

$$n^3 + 3n^2 + 2n = (n^3 - n) + 3(n^2 + n)$$

come from? Our inductive hypothesis says that $n^3 - n$ is a multiple of 6, but the expression $n^3 + 3n^2 + 2n$ doesn't "contain" $n^3 - n$. To take advantage of the inductive hypothesis, it makes sense to subtract one n from n^3 and compensate by adding another one to $3n^2 + 2n$.

Strengthening the hypothesis

You are given a 2^n by 2^n square grid with a central square removed. (A central square is one that touches the center of the grid.) You want to tile the remaining squares with L-shaped tiles, each tile occupying 3 squares. Can it always be done? Here is an example with $n = 2$:



Let us prove that that a tiling always exists.

Theorem 4. *For every positive integer n, there exists a tiling of a 2^n by 2^n square grid with a central square removed using L-shaped tiles.*

Let us try to prove this theorem by induction. In the base case $n = 1$, the tile has dimensions 2 by 2 and the proposition is clearly true.

Now let's try the inductive step. Let us fix n and assume the proposition is true for n, namely there exists a tiling of a 2^n by 2^n grid with a central square removed. We want to show that there also exists a tiling of a 2^{n+1} by 2^{n+1} grid with a central square removed. To apply the inductive hypothesis, it makes sense to split this grid into four 2^n by 2^n subgrids. Unfortunately, the subgrids don't satisfy the requirement of having their central square removed; one of them will be missing a corner and the other three will be whole. It looks like we are stuck.

The trick here is to prove a *more general* theorem – one of which Theorem 4 is a special case.

Theorem 5. *For every positive integer n, there exists a tiling of a 2^n by 2^n square grid with* any one *square removed using L-shaped tiles.*

Proof. We prove the theorem by induction on n.

Base case $n = 1$: Given a 2 by 2 grid with any square removed, the other 3 form a 2 by 1 L-shape, so they can be covered by one tile. Therefore a covering of the grid by tiles exists.

Inductive step: Let us assume that a 2^n by 2^n grid with any one square removed can be tiled using L-shaped tiles. We will show that the same is true for a 2^{n+1} by 2^{n+1} grid. Let G be a 2^{n+1} by 2^{n+1} grid with some square removed. Divide G into four 2^n by 2^n quadrants G_1, G_2, G_3, G_4. One of these quadrants will contain the missing tile. Temporarily remove the center tiles of G that do not below to that quadrant. Then each of G_1, G_2, G_3, and G_4 becomes a 2^n by 2^n grid with one square removed. By inductive hypothesis, each one of them can be tiled using 2 by 1 L-shapes. Tile all the subgrids and cover the temporarily removed three center tiles of G by one more L-shape. The resulting tiling covers all of G except for the removed square.

It follows by induction that for every n there exists a tiling of the 2^n by 2^n square grid with any square removed using L-shaped tiles. □

Theorem 5 (which allows for any square in the grid to be removed) is more general than Theorem 4, so we would expect it to be more difficult to prove. However, we proved Theorem 5, while the same proof method failed when we tried it on Theorem 4! The reason is that in proofs by induction, the predicate $P(n)$ plays the role both of assumption and conclusion. Sometimes making a stronger assumption allows us to prove a stronger conclusion.

An interesting feature of this proof is that it not only tells us the desired tiling exists, but also how to find it. You can write a computer program that does it or play with the python code available from the course web page.

A false proof

"Theorem:" In every nonempty set of horses, all horses are of the same colour.

Proof. We prove this theorem by induction on the size n of the set.

Base case $n = 1$: The set has one horse, so the statement is true.

Inductive step: Assume that in every collection of n horses, all of them have the same colour. We will prove that in every set of $n + 1$ horses, all of them have the same colour. Take any set of $n + 1$ horses:

$$h_1, h_2, \ldots, h_{n+1}.$$

By our assumption, the first n horses $h_1, \ldots, h_n$ are of the same colour. By the same assumption, the last n horses $h_2, \ldots, h_{n+1}$ have the same colour. So $h_1, \ldots, h_{n+1}$ all have the same colour.

It follows by induction that all horses in the set are of the same colour. □

Where was the mistake? To "debug" a proof by induction, it is a good idea to try out some values of n and see where the chain of reasoning went wrong. Let $P(n)$ be the predicate "All sets of n horses have the same colour." As we saw, $P(1)$ is true. However, $P(2)$ is already false. So the inductive step fails when $n = 1$, that is when we try to prove $P(2)$ assuming $P(1)$. The proof says

that in this case, the first 1 horse(s) have the same colour and the last 1 horse(s) have the same colour. We cannot conclude that both have the same colour! In other words, the deduction

$$\frac{h_1, \ldots, h_n \text{ have the same colour} \qquad h_2, \ldots, h_{n+1} \text{ have the same colour}}{h_1, \ldots, h_{n+1} \text{ have the same colour}}$$

is not valid when $n = 1$.

2 State Machines and Invariants

In computer science you often encounter systems that evolve over discrete time according to some rules. State machines provide a useful abstraction for describing such systems. A *state machine* is specified by a set of *states*, a *transition predicate* $q \to r$ that says if the system is allowed to transition from state q to state r, and a *start state*.

An *invariant* is a predicate of states that remains true over the lifetime of the state machine. Induction allows us to prove invariants: To show the invariant holds, we prove it is satisfied in the initial state, and that assuming it holds at time n, it also holds at time $n + 1$ for every n; namely, it is preserved by the transitions.

Here is an example. You have a robot that can walk across diagonals on an infinite 2-dimensional grid. Its coordinates at any given time are described by a pair of integer coordinates (x, y). In each time step, the robot moves by exactly one unit left or right *and* by exactly one unit up or down. At time 0 robot starts at position $(0, 0)$. (Thus, at time 1, the robot will be in one of the four positions $(-1, -1)$, $(-1, 1)$, $(1, -1)$, $(1, 1)$.) Can the robot ever reach position $(1, 0)$?

In this example, the motion of the robot can be described by a state machine whose states are pairs of integers (x, y), whose transitions are described by the predicate

$$\begin{aligned}(x, y) \to (x', y') \quad \text{if} \quad & (x' = x - 1 \text{ AND } y' = y - 1) \text{ OR } (x' = x - 1 \text{ AND } y' = y + 1) \text{ OR} \\ & (x' = x + 1 \text{ AND } y' = y - 1) \text{ OR } (x' = x + 1 \text{ AND } y' = y + 1),\end{aligned}$$

and whose start state is the state $(0, 0)$. The next theorem states that the predicate "$x + y$ is even" is an invariant of this system:

Theorem 6. *For every n, if the robot is at position (x, y) at time n, then $x + y$ is even.*

Therefore the robot can never reach position $(1, 0)$ because $1 + 0$ is odd.

Proof. We prove the theorem by induction on n.

Base case $n = 0$**:** The start state is $(0, 0)$ and $0 + 0$ is even.

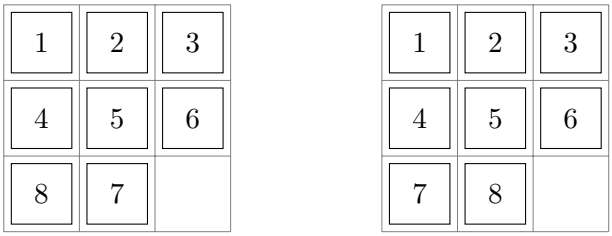
Inductive step: Assume that at time n, the robot is at position (x, y) and $x + y$ is even. Let (x', y') be the position of the robot at time $n+1$. We will prove that $x' + y'$ is even by case analysis:

- The robot moves left and down: Then $x' = x - 1$, $y' = y - 1$, so $x' + y' = (x + y) - 2$ – an even number minus two, therefore even.
- The robot moves left and up: Then $x' = x - 1$, $y' = y + 1$, so $x' + y' = x + y$, which is even.
- The robot moves right and up: Then $x' = x + 1$, $y' = y + 1$, so $x' + y' = (x + y) + 2$ – an even number plus two, therefore even.

- The robot moves right and down: Then $x' = x + 1$, $y' = y - 1$, so $x' + y' = x + y$, which is even.

It follows by induction that the sum of the robot's coordinates is always even. □

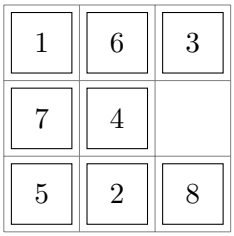
Here is another, more challenging example. It is about the following puzzle. The starting configuration is the one on the left. You are supposed to reach the configuration on the right. At each point, you are allowed to move an adjacent tile into the unoccupied square.



We will show that this is not possible using an invariant. This invariant is trickier than the one in the last problem. To explain it, we need two concepts.

We say tile a appears *before* tile b if tile a is in a higher row than tile b or if they are in the same row, tile a is to the left of tile b. We say the pair of tiles $\{a, b\}$ form an *inversion* if $a > b$ and tile a appears before tile b.

For example, in the final configuration there are no inversions. In the initial configuration, there is exactly one inversion consisting of the pair $\{8, 7\}$. In the following configuration, the inversions are $\{3, 2\}$, $\{4, 2\}$, $\{5, 2\}$, $\{6, 2\}$, $\{7, 2\}$, $\{6, 3\}$, $\{6, 4\}$, $\{7, 4\}$, $\{6, 5\}$, and $\{7, 5\}$.



We will show the following invariant:

Theorem 7. *The number of inversions is always odd.*

Proof. We prove the theorem by induction on n.

Initial configuration: In the initial configuration, there is exactly one inversion – the pair $\{8, 7\}$. So initially the number of inversions is odd.

Transitions: Assume that before a transition the number of inversions is odd. We will show that the same is true after the transition. The transition can be a row move (a tile moves to the left or to the right) or a column move (a tile moves up or down). The proof is by case analysis.