Lecture Notes

1 Proof by Induction

The topic this week is proof by induction. Induction is by far the most powerful and commonly-used proof technique in computer science. Induction is useful when we want to prove a statement that involves some natural-valued variable. For example, "for all $n \in \mathcal{N}$, the sum $1 + 2 + 3 + \ldots + n$ is equal to $n(n + 1)/2$".

Proving such a statement by induction requires two steps. In the first step, we prove that the statement holds for $n = 0$. In the second step, we prove that if the statement is true for some value of n, then it must also be true for the next larger value of n. Why do these two steps prove that the statement is true for all natural values of n? Because there is an axiom that says so:

Axiom (Induction) Let $P(n)$ be a predicate. Suppose that $P(0)$ is true and $\forall n \in \mathcal{N}\ P(n) \Rightarrow P(n + 1)$. Then $P(n)$ is true for all $n \in \mathcal{N}$.

In other words, if $P(0)$ is true, $P(0) \Rightarrow P(1)$, $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$, and so on forever, then we can conclude that $P(n)$ is true for all $n \in \mathcal{N}$. The predicate $P(n)$ is called the *induction hypothesis.*

As an analogy, suppose that we have an infinite line of dominoes standing on end. If we tip the first domino and a falling domino always tips the next one in line, then the induction axiom says that no domino will remain standing. This seems reasonable!

2 A Complete Proof

Let's use induction to prove the statement used above as an example. This is a useful fact to remember anyway.

Theorem 2.1 $\forall n \in \mathcal{N}\ 1 + 2 + 3 + \ldots + n = n(n + 1)/2$

Notation such as $1 + 2 + 3 + \ldots + n$ is imprecise, but common because it is convenient. The idea is to show enough of a sequence so that anyone can figure out the pattern. We can be more precise with summation notation:

$$\sum_{i=1}^{n} i \quad or \quad \sum^{1 \leq i \leq n} i \quad or \quad \sum_{1 \leq i \leq n} i$$

In this notation, the pattern of terms in the summation is made explicit. In two important special cases, the definition of the summation requires some care:

- If $n = 1$, then $1+2+3+\ldots+n = 1$. There is only one term in the summation; the appearance of 2 and 3 and the presence of both 1 and n is misleading!
- If $n \leq 0$, then $1+2+3+\ldots+n = 0$. There are no terms at all in the summation, so the result is zero.

There are four parts to a proof by induction. We'll discuss each part below and then write a proof for the preceding theorem following this outline.

1. **State that the proof is by induction.** Always make clear that a proof uses induction. This immediately conveys the general structure of the argument.
2. **Specify the induction hypothesis,** $P(n)$**.** Sometimes, the choice of $P(n)$ will come directly from the theorem statement. In this case $P(n)$ will simply be the predicate $1+2+3+\ldots+n = n(n+1)/2$. Other times, the choice of $P(n)$ is not obvious at all; we will see an example of this at the end of the lecture.
3. **The basis step: prove** $P(0)$**.** The "basis step" or "base case" is a proof of the predicate $P(0)$. In this case, we must prove that $1+2+3+\ldots+n = n(n+1)/2$ when $n = 0$. This is trivial because both sides of the equality are zero.
4. **The inductive step: prove that** $\forall n \in \mathcal{N}\;\; P(n) \Rightarrow P(n+1)$**.** Begin the inductive step by writing, "For $n \geq 0$, assume" $P(n)$ "to prove" $P(n+1)$. (Substitute in the statements of the predicates $P(n)$ and $P(n+1)$.) Then verify that for all $n \geq 0$ $\;P(n)$ implies $P(n+1)$.

A complete proof of the theorem that follows this four-part formula is given below.

Proof. The proof is by induction. Let $P(n)$ be the predicate $1+2+3+\ldots+n = n(n+1)/2$. In the base case, $P(0)$ is true because both sides of the equality are zero. For $n \geq 0$, assume $1+2+3+\ldots+n = n(n+1)/2$ to prove $1+2+3+\ldots+n+(n+1) = (n+1)(n+2)/2$.

$$\begin{aligned}
1+2+3+\ldots+n &= \frac{n(n+1)}{2} \\
1+2+3+\ldots+n+(n+1) &= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n^2+n+2n+2}{2} \\
&= \frac{n^2+3n+2}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

This proves that for all $n \in \mathcal{N}\;\; P(n) \Rightarrow P(n+1)$ and completes the proof. ∎

In this case, we used induction purely as a proof technique; it gave little insight into why the theorem is true. Furthermore, while induction was essential in proving the summation equal to $n(n+1)/2$, it did not help us find this formula in the first place. We'll turn to the problem of finding sums of series in a couple weeks.

3 Examples of Proof by Induction

This section contains several examples of induction. There are two simple examples and then a tricky false proof. Next we address an application vital to the future of computer science at MIT and finally wind up with another false proof.

3.1 Simple Examples

Theorem 3.1 $\forall n \in \mathcal{N}\ n^3 \equiv n \pmod 3$

This notation may be unfamiliar. The $\equiv$ and mod always go together:

Definition $x \equiv y \pmod q$ iff $q \mid (x - y)$.

In words, this definition says x is "congruent" to y "mod" q if and only if q evenly divides $x - y$. For example, $10 \equiv 2 \pmod 4$ since 4 evenly divides $10 - 2 = 8$. As a second example, the theorem statement is exactly equivalent to, "$\forall n \in \mathcal{N}\ 3 \mid n^3 - n$". In fact, we will prefer this notation in the proof.

While the plan for writing an induction proof is clear, there is no rigid plan for finding such a proof. There are, however, a few good tricks to know. There are usually two difficulties in completing a proof by induction: choosing the right induction hypothesis $P(n)$ and completing the inductive step. (Sometimes proving the base case is also hard.) The most obvious candidate for an induction hypothesis is the theorem statement itself.

Method 1 When searching for a proof by induction, first try to lift an induction hypothesis directly from the theorem statement.

Sometimes the theorem statement will not immediately suggest a suitable induction hypothesis. In such cases, considerable trial and error may be necessary.

To complete the inductive step, we must prove that for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$. Typically $P(n)$ and $P(n+1)$ are very similar statements, but with some small difference or gap. The challenge is to clearly identify this gap and then to bridge it with some extra facts. Working "backward" is often helpful.

Method 2 To prove $P(n) \Rightarrow P(n+1)$, write down $P(n+1)$ and then use $P(n)$ to reduce this statement to a simpler assertion; this assertion is the extra fact needed to bridge the gap from $P(n)$ to $P(n+1)$ and complete the proof.

We can apply these principles to obtain a proof by induction of the preceding theorem. First, we can lift the induction hypothesis directly from the theorem statement. Let $P(n)$ be the predicate $3 \mid n^3 - n$. Second, we have to prove that for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$. The predicate $P(n+1)$

is $3 \mid (n+1)^3 - (n+1)$. Expanding terms in $P(n+1)$ gives $3 \mid n^3 + 3n^2 + 2n$. We can now use $P(n)$ to simplify $P(n+1)$ by subtracting off the quantity that $P(n)$ asserts is divisible by 3. This gives $3 \mid 3n^2 + 3n$. This obvious statement is the extra fact needed to bridge the gap from $P(n)$ to $P(n+1)$. In short, we can show that $P(n)$, together with the extra fact $3 \mid 3n^2 + 3n$, implies $P(n+1)$. Here is the complete proof:

Proof. The proof is by induction. Let $P(n)$ be the proposition $3 \mid n^3 - n$. In the base case, the proposition is true because $3 \mid 0 - 0$. For $n \geq 0$ assume $3 \mid n^3 - n$ to prove $3 \mid (n+1)^3 - (n+1)$.

$$\begin{aligned} & 3 \mid (n^3 - n) \\ \Rightarrow\ & 3 \mid (n^3 - n) + 3(n^2 + n) \\ \Rightarrow\ & 3 \mid n^3 + 3n^2 + 3n + 1 - n - 1 \\ \Rightarrow\ & 3 \mid (n+1)^3 - (n+1) \end{aligned}$$

The first implication follows because $3(n^2 + n)$ is divisible by 3. The remaining implications involve only rewriting the expression on the right. This proves that for all $n \in \mathcal{N}$, $P(n) \Rightarrow P(n+1)$ and completes the proof. ∎

The final proof would look very mysterious to anyone not privy to the scratchwork we did beforehand. For example, one might ask how we had the foresight to introduce the magic term $3(n^2 + n)$. Of course, this was not foresight at all; we worked backward.

The next example involves Fibonacci numbers, which are denoted by F_i for $i = 0, 1, 2, \ldots$. We define $F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$; that is, each Fibonacci number is the sum of the two before. The first few Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, 21. Fibonacci numbers have many strange properties. The following theorem has a nice inductive proof, but is a good thing to forget if you run low on brain space.

Theorem 3.2 $\forall n \geq 1\ F_1^2 + F_2^2 + \ldots + F_n^2 = F_n F_{n+1}$

For example, for $n = 4$ we have $1^2 + 1^2 + 2^2 + 3^2 = 15 = 3 \cdot 5$.

Let's look for a proof by induction. First, the theorem statement suggests that the induction hypothesis $P(n)$ be $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$. Second, we want to identify the gap between $P(n)$ and $P(n+1)$. The predicate $P(n+1)$ states that $\sum_{i=1}^{n+1} F_i^2 = F_{n+1} F_{n+2}$. Now the plan is to use $P(n)$ to reduce this statement to a simpler assertion. An easy way is to subtract the equation in predicate $P(n)$. Taking $P(n+1)$ "minus" $P(n)$ gives:

$$F_{n+1}^2 = F_{n+1} F_{n+2} - F_n F_{n+1}$$

This is the Fibonacci recurrence in disguise; dividing by F_{n+1} and moving a term gives $F_n + F_{n+1} = F_{n+2}$. This is the extra fact need to bridge the gap between $P(n)$ and $P(n+1)$ in the inductive step. The full proof is written below.

Proof. The proof is by induction. Let $P(n)$ be the proposition $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$. In the base case, $P(0)$ is true because $0 = F_0 F_1 = 0 \cdot 1 = 0$. For $n \geq 0$ assume $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$ to prove $\sum_{i=1}^{n+1} F_i^2 = F_{n+1} F_{n+2}$. For all $n \geq 0$, the we have $F_n + F_{n+1} = F_{n+2}$. Multiplying both sides by F_{n+1} and rearranging terms gives $F_{n+1}^2 = F_{n+1}F_{n+2} - F_n F_{n+1}$. Adding this identity to $P(n)$ gives:

$$\begin{aligned} F_{n+1}^2 + \sum_{i=1}^{n} F_i^2 &= (F_{n+1}F_{n+2} - F_n F_{n+1}) + F_n F_{n+1} \\ \sum_{i=1}^{n+1} F_i^2 &= F_{n+1}F_{n+2} \end{aligned}$$

This proves that for all $n \in \mathcal{N}$, $P(n) \Rightarrow P(n+1)$ and completes the proof. ■

3.2 A False Proof

Note that an induction argument need not start with 0. For example, we could prove a statement for all $n \geq 1$. In this case, $P(1)$ must be proven in the basis step, and $\forall n \geq 1$ $P(n) \Rightarrow P(n+1)$ must be proven in the inductive step. This is a valid variant of induction and is *not* the problem with the proof below.

False Theorem 3.3 All horses are the same color.

Proof. The proof is by induction. Let $P(n)$ be the proposition that in any set of n horses, all the horses are the same color. This is true in the base case $n = 1$, since there is only one horse in the set. For $n \geq 1$, assume that in every set of n horses, all are the same color in order to prove that in every set of $n+1$ horses, all are the same color. Consider a set of $n+1$ horses $h_1, h_2, \ldots, h_{n+1}$. By induction, $h_1, h_2, \ldots, h_n$ all are the same color. And by induction, $h_2, \ldots, h_{n+1}$ all are the same color. Therefore, $\mathit{color}(h_1) = \mathit{color}(h_2, \ldots, h_n) = \mathit{color}(h_{n+1})$, and so all the horses $h_1, h_2, \ldots, h_{n+1}$ must be the same color. This proves that for all $n \geq 1$, $P(n) \Rightarrow P(n+1)$ and completes the proof. ■

Where is the bug?

The error is in the statement, "$\mathit{color}(h_1) = \mathit{color}(h_2, \ldots, h_n) = \mathit{color}(h_{n+1})$". The notation helps create the confusion. If $n = 1$, then $h_2, \ldots, h_n$ refers to no horses at all! Therefore, $\mathit{color}(h_2, \ldots, h_n)$ has no meaning and the conclusion $\mathit{color}(h_1) = \ldots = \mathit{color}(h_n)$ is incorrect.

Because of this bug, we have really only proven $P(1)$, $P(2) \Rightarrow P(3)$, $P(3) \Rightarrow P(4)$, and so on. But since we have not proven $P(2)$, we have not proven $P(3), P(4)$, etc. In fact, $P(2), P(3), P(4), \ldots$ are all false– there are horses of a different color.

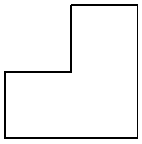

Figure 1: One of the L-shaped tiles that will be used in the courtyard of the new computer science building.

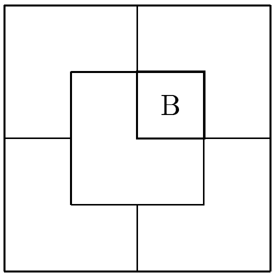

Figure 2: A legal tiling of a 4x4 courtyard. The B marks Bill.

3.3 The Fate of Computer Science at MIT

In the preceding examples, induction has served purely as a proof technique. However, it can be useful more generally in problem solving.

MIT is constructing a new computer science building at a cost of $100 million. The TAs will pass a collection plate around at the end of lecture. If this is insufficient, MIT will adopt a desperate measure to attract cash: there will be a statue of Bill Gates in the courtyard.

The planned courtyard consists of $2^n \times 2^n$ squares. Most of these will be covered by L-shaped tiles, each covering three squares. However, one square will be covered by the statue of our hero; in fact, this should be one of the central squares. Your problem is to find a suitable tiling. An example solution for the case of $n = 2$ is shown.

(The phrase "central squares" is a little ambiguous. If $n = 0$ and the courtyard is a single square, Bill takes it. If $n > 0$, then there are four central squares, and Bill will take any of them.)

Let's try to prove by induction that such a tiling exists. As usual, we first try to lift the inductive hypothesis directly from the theorem statement.

Theorem 3.4 For all $n \geq 0$ there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in a central square.

Proof. *(doomed attempt)* The proof is by induction. Let $P(n)$ be the proposition that there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in the center. In the base case, $P(0)$ is true because Bill fills the whole courtyard. For $n \geq 0$, assume that there is a tiling of a $2^n \times 2^n$ courtyard with Bill in the center to prove that there is is a legal tiling of a $2^{n+1} \times 2^{n+1}$ courtyard with Bill in the center... ■

Now we're in trouble! The ability to tile a smaller courtyard with Bill in the center does not help tile a larger courtyard with Bill in the center. The usual recipe for finding an inductive proof will not work!

Sometimes, making the induction hypothesis *stronger* makes a proof *easier*. For example, we could make $P(n)$ the proposition that for every position of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. This hypothesis is "stronger" in the sense that the earlier claim was just a special case. However, when we have to prove $P(n) \Rightarrow P(n+1)$, we will be in better shape because we can *assume* $P(n)$, which is now a more general, more useful statement.

Method 3 If you can not show that $P(n) \Rightarrow P(n+1)$ in a proof by induction, change the induction hypothesis; in particular, strengthening the hypothesis may make the proof easier.

Even with this new hypothesis, finding the right way to prove that $P(n) \Rightarrow P(n+1)$ requires some work.

Proof. *(successful attempt)* The proof is by induction. Let $P(n)$ be the proposition that if any one square of a $2^n \times 2^n$ courtyard must be left blank, then there exists a tiling of the remainder. In the base case, $P(0)$ is true because if the one and only square is left blank, then there exists a tiling of the remainder (which is nothing). For $n \geq 0$, assume that if any one square of a $2^n \times 2^n$ courtyard must be left blank, then there exists a tiling of the remainder. We will use this to prove that if any one square of a $2^{n+1} \times 2^{n+1}$ courtyard must be left blank, then there exists a tiling of the remainder.

Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One will contain the square that must be left blank and can be tiled by induction. Now place a tile in the center of the courtyard so that it covers one sqaure in each remaining quadrant. All that remains is to tile each of these three quadrants, excluding the one square in each that is already covered. But this can also be done by induction. This proves that $\forall n \geq 1, P(n) \Rightarrow P(n+1)$. The theorem follows as a special case in which a central square is left blank during tiling and is later covered by a statue of Bill. ■

This proof has two nice properties. First, not only does the proof guarantee that a tiling exists, but also it gives an algorithm for finding such a tiling. Second, we have a stronger result; if Bill wants his statue on the edge of the courtyard, away from the pigeons, we can accommodate him.

3.4 Another False Proof

False Theorem 3.5 I can lift all the sand on the beach.

Proof. The proof is by induction. Let $P(n)$ be the predicate, "I can lift n grains of sand." The base case $P(1)$ is true because I can certainly lift one grain of sand. In the inductive step, assume that I can lift n grains of sand to prove that I can lift $n+1$ grains of sand. If I can lift n grains of sand, then surely I can lift $n+1$; one grain of sand will not make any difference. Therefore $P(n) \Rightarrow P(n+1)$, completing the proof. ■

The flaw here is in the bogus assertion that I can lift $n+1$ grains of sand because I can lift n grains. It is hard to say for exactly which n this is false, but certainly there is some value!

There is a field called "fuzzy logic" in which truth is not a 0/1 thing, but is rather represented by a real value between 0 and 1. There is an analogue of induction in which the truth value decreases a bit with each implication. We will not be using fuzzy logic in this class, however; at least, not intentionally.