Math 221 Winter 2023, Lecture 4: Induction

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wd`

1. Induction and recursion (cont'd)

1.8. More on the Fibonacci numbers (cont'd)

Recall the Fibonacci sequence, which we defined in Lecture 2:

Definition 1.8.1. The **Fibonacci sequence** is the sequence $(f_0, f_1, f_2, \ldots)$ of nonnegative integers defined recursively by setting

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and}$$
$$f_n = f_{n-1} + f_{n-2} \qquad \text{for each } n \geq 2.$$

The entries of the Fibonacci sequence are called the **Fibonacci numbers**. Here are the first few:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233

.

Is there an explicit formula for f_n, that is, a formula that does not rely on the previous entries of the Fibonacci sequence?

Yes, there is one; it is known as **Binet's formula**:

Theorem 1.8.6 (Binet's formula)**.** Let

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618\ldots \qquad \text{and} \qquad \psi = \frac{1-\sqrt{5}}{2} \approx -0.618\ldots.$$

Then,

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \qquad \text{for every integer } n \geq 0.$$

Some remarks:

- The number φ is called the **golden ratio**, and is famous for many properties, including the fact that $\varphi^2 = \varphi + 1$ (which you can easily check by

expanding both sides[1]). The number ψ is its so-called conjugate and also satisfies $\psi^2 = \psi + 1$.

- The numbers f_n are integers, but Binet's formula expresses them in terms of two irrational numbers φ and ψ. This should be rather unexpected.
- As n grows large, ψ^n approaches 0 (since $-1 < \psi < 1$), whereas φ^n grows exponentially (since $\varphi > 1$). So f_n also grows exponentially (according to Binet's formula), with growth rate $\varphi \approx 1.618\ldots$.

Questions:

1. How do we prove Binet's formula?
2. How could we find Binet's formula if we didn't already know it?

We will answer Question 1 today. Question 2 is significantly trickier and will not be answered in this course[2].

Let us try to prove Binet's formula by induction on n:

Attempted proof of Binet's formula. We induct on n:

Base case: For $n = 0$, we have $f_n = f_0 = 0$ and

$$\frac{\varphi^n - \psi^n}{\sqrt{5}} = \frac{\varphi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0.$$

Thus, Binet's formula holds for $n = 0$.

Induction step: Let $n \geq 0$ be an integer.

Assume (as induction hypothesis) that Binet's formula holds for n; we must prove that it holds for $n+1$.

[1] Namely: From $\varphi = \dfrac{1+\sqrt{5}}{2}$, we obtain

$$\varphi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1+\varphi.$$

[2] Answers at different levels of generality can be found in:

- Subsection 4.9.2 of my notes *Math 235: Mathematical Problem Solving* (which solves any linear recurrence of the form $x_n = ax_{n-1} + bx_{n-2}$ for constant numbers a and b in an explicit and elementary way);
- María Victoria Melián, *Linear recurrence relations with constant coefficients* and Nikolai V. Ivanov, *Linear Recurrences* (which solve the more general version $x_n = a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_k x_{n-k}$ in terms of the eigenvalues of a matrix).

Textbooks on combinatorics or advanced linear algebra also tend to discuss such sequences (called **linearly recurrent sequences**).

So we must prove that

$$f_{n+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}.$$

The recursive definition of the Fibonacci sequence yields

$$f_{n+1} = f_n + f_{n-1} = \frac{\varphi^n - \psi^n}{\sqrt{5}} + f_{n-1} \qquad \text{(by the induction hypothesis)}.$$

So far so good, but how can we simplify f_{n-1} ? Our induction hypothesis only tells us that $f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$, but it says nothing about f_{n-1}. □

So this induction proof does not work.[3]

Let us see how to fix this by introducing a more advanced version of induction.

1.9. Strong induction

1.9.1. Reminder on regular induction

Recall the (original) principle of mathematical induction:

Theorem 1.9.1 (Principle of Mathematical Induction)**.** Let b be an integer.
Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.
Assume the following:

1. "**Base case**": The statement $P(b)$ holds.
2. "**Induction step**": For each integer $n \geq b$, the implication $P(n) \Longrightarrow P(n+1)$ holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

We can restate this principle slightly by renaming the n in the induction step as $n-1$ (so that the implication $P(n) \Longrightarrow P(n+1)$ turns into $P(n-1) \Longrightarrow P(n)$). Thus, it takes the following form:

Theorem 1.9.2 (Principle of Mathematical Induction, restated)**.** Let b be an integer.
Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.
Assume the following:

1. "**Base case**": The statement $P(b)$ holds.

[3] There is also one more little (fixable) gap in the above attempted proof. Do you see it?

2. "**Induction step**": For each integer $n > b$, the implication $P(n-1) \Longrightarrow P(n)$ holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

The idea behind the principle (in either form) is that the base case gives us $P(b)$ whereas the induction step gives us the implications

$$\begin{aligned} P(b) &\Longrightarrow P(b+1), \\ P(b+1) &\Longrightarrow P(b+2), \\ P(b+2) &\Longrightarrow P(b+3), \\ &\cdots. \end{aligned}$$

In the domino metaphor, the base case tips over the first domino, and the induction step ensures that each domino falls from the impact of the previous domino's falling.

1.9.2. Strong induction

Now, assume that the $b+2$-domino (i.e., $P(b+2)$) falls not from the impact of the previous domino $P(b+1)$, but rather from the combined force of the dominos $P(b)$ and $P(b+1)$. This would still suffice, because the latter two dominos have already fallen. In other words, instead of the implication $P(b+1) \Longrightarrow P(b+2)$, we could just as well prove the implication

$$(P(b) \text{ AND } P(b+1)) \Longrightarrow P(b+2),$$

which is somewhat weaker (since it assumes more to get to the same conclusion) but nevertheless gives the same result. Likewise, we could just as well replace the implication $P(b+2) \Longrightarrow P(b+3)$ by the weaker implication

$$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2)) \Longrightarrow P(b+3).$$

More generally, for each $n > b$, instead of proving the implication $P(n-1) \Longrightarrow P(n)$, it will suffice to prove the weaker implication

$$\underbrace{(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1))}_{\text{i.e., the statement } P(k) \text{ holds for each } k \in \{b, b+1, \ldots, n-1\}} \Longrightarrow P(n)$$

(so that the domino $P(n)$ is tipped over by the combined force of all the preceding dominos, not just the one domino directly to its left).

This induction principle is called **strong induction**. Explicitly, it says the following:

Theorem 1.9.3 (Principle of Strong Induction)**.** Let b be an integer.
Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.
Assume the following:

1. "**Base case**": The statement $P(b)$ holds.
2. "**Induction step**": For each integer $n > b$, the implication

   $$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

   holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

Proofs using this principle are called **proofs by strong induction** (or **strong induction proofs**). They differ from proofs by (regular) induction as follows: In the induction step of a strong induction proof, you can use not just the preceding statement $P(n-1)$, but also all the statements before it ($P(n-2)$ and $P(n-3)$ and so on, all the way down to $P(b)$). In other words, the induction hypothesis is now stronger (thus the name "strong induction"). Roughly speaking, strong induction is "induction with a long memory" (as opposed to regular induction, whose memory only is 1 step long).

(We will later see a slightly nicer form of strong induction, in which the base case is incorporated in the induction step.)

Before we see an example of a strong induction proof, let me explain why it works. Let's say you have proved a statement $P(n)$ for all $n \geq 0$ by strong induction. Thus,

- you have proved $P(0)$ (this is the base case);
- you have proved the implication $P(0) \Longrightarrow P(1)$ (this is the induction step for $n = 1$), so you conclude that $P(1)$ holds (since $P(0)$ holds);
- you have proved the implication $(P(0) \text{ AND } P(1)) \Longrightarrow P(2)$ (this is the induction step for $n = 2$), so you conclude that $P(2)$ holds (since $P(0)$ and $P(1)$ hold);
- you have proved the implication $(P(0) \text{ AND } P(1) \text{ AND } P(2)) \Longrightarrow P(3)$ (this is the induction step for $n = 3$), so you can conclude that $P(3)$ holds (since $P(0)$ and $P(1)$ and $P(2)$ hold);
- and so on.

1.9.3. Example: Proof of Binet's formula

Let us now prove Binet's formula by strong induction:

Proof of Theorem 1.8.6 (i.e., of Binet's formula). We strongly induct on n (i.e., we use strong induction on n):

Base case: As above, we check that the formula holds for $n = 0$.

Induction step: Let $n > 0$ be an integer.

We assume that Binet's formula holds for 0, for 1, for 2, and so on, all the way up to $n-1$. (In other words, we assume that $f_k = \dfrac{\varphi^k - \psi^k}{\sqrt{5}}$ for each $k \in \{0, 1, \ldots, n-1\}$.)

We have to prove that Binet's formula also holds for n. In other words, we have to prove that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$.

We assumed that Binet's formula holds for $n-1$. That is, we have $f_{n-1} = \dfrac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}}$.

We assumed that Binet's formula holds for $n-2$. That is, we have $f_{n-2} = \dfrac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}}$.

As we have seen above, we have $\varphi^2 = \varphi + 1$ and $\psi^2 = \psi + 1$.

But the recursive definition of the Fibonacci sequence yields

$$
\begin{aligned}
f_n &= f_{n-1} + f_{n-2} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}} \\
&\qquad \left(\text{since } f_{n-1} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} \text{ and } f_{n-2} = \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}} \right) \\
&= \frac{1}{\sqrt{5}} \left(\varphi^{n-1} - \psi^{n-1} + \varphi^{n-2} - \psi^{n-2} \right) \\
&= \frac{1}{\sqrt{5}} \left(\underbrace{\varphi^{n-1} + \varphi^{n-2}}_{=\varphi^{n-2}(\varphi+1)} - \underbrace{\left(\psi^{n-1} + \psi^{n-2} \right)}_{=\psi^{n-2}(\psi+1)} \right) \\
&= \frac{1}{\sqrt{5}} \left(\varphi^{n-2} \underbrace{(\varphi + 1)}_{=\varphi^2} - \psi^{n-2} \underbrace{(\psi + 1)}_{=\psi^2} \right) \\
&= \frac{1}{\sqrt{5}} \left(\underbrace{\varphi^{n-2}\varphi^2}_{=\varphi^n} - \underbrace{\psi^{n-2}\psi^2}_{=\psi^n} \right) = \frac{1}{\sqrt{5}} \left(\varphi^n - \psi^n \right) = \frac{\varphi^n - \psi^n}{\sqrt{5}}.
\end{aligned}
$$

So we have proved Binet's formula for n. Right?

. . . . . .

Wait a moment! We have assumed (as the induction hypothesis) that Binet's formula holds for each of the numbers $0, 1, \ldots, n-1$. But then we have used

it for $n-2$ and for $n-1$. This tacitly relied on the fact that $n-2$ and $n-1$ are among the numbers $0, 1, \ldots, n-1$. However, this fact is only true if $n \geq 2$. If $n = 1$, then $n-2$ is not among the numbers $0, 1, \ldots, n-1$ (because it is negative).

So our induction step worked for $n = 2, 3, 4, \ldots$ but not for $n = 1$. What can we do?

We can fix this by just proving the claim for $n = 1$ by hand. So we must prove that $f_1 = \dfrac{\varphi^1 - \psi^1}{\sqrt{5}}$. This can be checked by a direct computation:

$$\frac{\varphi^1 - \psi^1}{\sqrt{5}} = \frac{\varphi - \psi}{\sqrt{5}} = \frac{\dfrac{1+\sqrt{5}}{2} - \dfrac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = f_1.$$

Now our induction step is really complete, and Binet's formula is proved. □

Let us summarize: We have used strong induction in our above proof of Theorem 1.8.6, because the "extra memory" in a strong induction step allowed us to express not just f_{n-1} but also f_{n-2} via the induction hypothesis.

Note that we have had to handle the two cases $n = 0$ and $n = 1$ by hand in our above proof, because we had to reach "2 steps back" in memory in the induction step (i.e., we had to apply the induction hypothesis both to $n-1$ and to $n-2$). [4] The case $n = 0$ was our base case, whereas the case $n = 1$ was part of the induction step, but nevertheless had to be singled out for special treatment (since $n-2$ is negative for $n = 1$). Nevertheless, it makes sense to think of the $n = 1$ case as a "second base case", even if it is de-jure part of the induction step.

1.9.4. Baseless strong induction

You can actually reformulate the principle of strong induction in a form that does not have a de-jure base case at all:

Theorem 1.9.4 (Principle of Strong Induction, restated)**.** Let b be an integer. Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$. Assume the following:

- "**Induction step":** For each integer $n \geq b$, the implication

  $$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

  holds.

Then, the statement $P(n)$ holds for every integer $n \geq b$.

[4] Had we reached further back, we would have needed extra cases (e.g., if we had applied the induction hypothesis to $n-5$, then we would have to handle all the cases $n = 0, 1, 2, 3, 4$ by hand).

How does this restated principle work without a base case? Easy: We have just repackaged the base case into the induction step. Indeed, note that the induction step now says "$n \geq b$", not "$n > b$". In particular, this means that the implication

$$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

has to hold for $n = b$. However, for $n = b$, the antecedent (= if-part) of this implication is a tautology (i.e., is an empty statement that is automatically true by dint of its emptiness[5]), and thus proving this implication is tantamount to just unconditionally proving $P(b)$, which was what we previously viewed as our base case. So we have not magically removed the need for a base case; we just have merged it into the induction step. Nevertheless, this makes for a slightly cleaner version of strong induction.

1.9.5. Example: Prime factorizations exist

Another example of a strong induction proof comes from elementary number theory. We recall a basic definition (more on this later, when we cover number theory):

Definition 1.9.5. A **prime** (or **prime number**) means an integer $p > 1$ whose only positive divisors are 1 and p.

So the primes (in increasing order) are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots.$$

There are infinitely many primes, as we will show later.

Theorem 1.9.6. Every positive integer is a product of finitely many primes.

Here and in the following, I understand an empty product (i.e., a product of no numbers whatsoever) to be 1. Thus, Theorem 1.9.6 does hold for 1, since 1 is a product of no primes.

Here are more interesting examples:

- $2023 = 7 \cdot 17 \cdot 17$ is a product of three primes.
- $2024 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23$ is a product of five primes.

[5] Don't believe it? Observe that this antecedent

$$(P(b) \text{ AND } P(b+1) \text{ AND } P(b+2) \text{ AND } \cdots \text{ AND } P(n-1))$$

is a conjunction of $n - b$ statements (since there are $n - b$ numbers between b and $n - 1$ inclusive). If $n = b$, this means that it is a conjunction of $b - b = 0$ statements, i.e., of no statements whatsoever. So it is an empty statement, automatically true.

- $2 = 2$ is a product of one prime (namely, 2 itself).

How do we prove Theorem 1.9.6 in general?

Proof of Theorem 1.9.6. We must prove the statement

$$P(n) = (\text{“}n \text{ is a product of finitely many primes”})$$

for each integer $n \geq 1$.

We shall prove this by strong induction on n. (We use the original variant of strong induction, with a base case.)

Base case: $P(1)$ is true, since 1 is a product of finitely many primes (specifically, of 0 primes, as we saw).

Induction step: Let $n > 1$. We must prove the implication

$$(P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n).$$

So we assume that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. We must prove that $P(n)$ holds.

In other words, we must prove that n is a product of finitely many primes.

We are in one of the following two cases:

Case 1: The only positive divisors of n are 1 and n.

Case 2: There is a positive divisor d of n that is neither 1 nor n.

(Other cases are not possible, since 1 and n always are positive divisors of n.)

Consider Case 1 first. In this case, n itself is a prime (by the definition of a prime), and thus is a product of finitely many primes (namely, of just 1 prime: itself). Thus, $P(n)$ holds in Case 1.

Now, consider Case 2. In this case, there is a positive divisor d of n that is neither 1 nor n. Consider such a d (you might have to choose one, but any choice is fine). Since d is a positive divisor of n, we have $1 \leq d \leq n$ (strictly speaking, this needs to be proved, but we take this for granted here). Therefore, $1 < d < n$ (since d is neither 1 nor n). Hence, d is one of the numbers $1, 2, \ldots, n-1$ (actually $2, 3, \ldots, n-1$, but we don't care).

Furthermore, $\dfrac{n}{d}$ is an integer (since d is a divisor of n) and positive (since n and d are positive). Multiplying the inequality $1 < d$ by $\dfrac{n}{d}$, we obtain $1 \cdot \dfrac{n}{d} < d \cdot \dfrac{n}{d}$ (since we can always divide an inequality by a positive number[6]). In other words, $\dfrac{n}{d} < n$. Since $\dfrac{n}{d}$ is a positive integer, we thus conclude that $\dfrac{n}{d}$ is one of the numbers $1, 2, \ldots, n-1$.

Now, our induction hypothesis says that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. In particular, $P(d)$ holds (since d is one of the numbers $1, 2, \ldots, n-1$). In other words, d is a product of primes. That is, we can write d as

$$d = p_1 p_2 \cdots p_k \qquad \text{for some primes } p_1, p_2, \ldots, p_k.$$

[6] This is a basic fact that we are taking for granted.

Consider these primes $p_1, p_2, \ldots, p_k$.

Again, our induction hypothesis says that $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. In particular, $P\left(\frac{n}{d}\right)$ holds (since $\frac{n}{d}$ is one of the numbers $1, 2, \ldots, n-1$). In other words, $\frac{n}{d}$ is a product of primes. That is, we can write $\frac{n}{d}$ as

$$\frac{n}{d} = q_1 q_2 \cdots q_\ell \qquad \text{for some primes } q_1, q_2, \ldots, q_\ell.$$

Consider these primes $q_1, q_2, \ldots, q_\ell$.

Now,

$$n = d \cdot \frac{n}{d} = p_1 p_2 \cdots p_k \cdot q_1 q_2 \cdots q_\ell$$

(since $d = p_1 p_2 \cdots p_k$ and $\frac{n}{d} = q_1 q_2 \cdots q_\ell$). This shows that n is a product of primes (since $p_1, p_2, \ldots, p_k$ as well as $q_1, q_2, \ldots, q_\ell$ are primes). In other words, $P(n)$ holds. Thus, we have proved $P(n)$ in Case 2.

Now, we have proved $P(n)$ both in Case 1 and Case 2. Therefore, $P(n)$ always holds. Thus, the induction step is complete, and Theorem 1.9.6 is proven. □

The above proof is just reflecting the elementary recursive algorithm for factoring an integer n into a product of primes: We search for a positive divisor d of n that is neither 1 nor n. If such a d does not exist, then n itself is a prime. If it does, then we are reduced to the simpler problems of factoring d and $\frac{n}{d}$, and just have to multiply the resulting factorizations at the end.