Math 321: More Mathematical Induction

Kameryn J Williams

University of Hawaiʻi at Mānoa

Spring 2021

Proofs by induction

- Two ways to prove something $P(n)$ is true for every natural number n:

Direct proof

- Consider an arbitrary natural number n.
- Prove $P(n)$.

Proof by induction

- Prove $P(0)$.
- Consider an arbitrary natural number n.
- Prove $P(n)$ implies $P(n+1)$.

Proofs by induction

- Two ways to prove something $P(n)$ is true for every natural number n:

Direct proof

- Consider an arbitrary natural number n.
- Prove $P(n)$.

Proof by induction

- Prove $P(0)$.
- Consider an arbitrary natural number n.
- Prove $P(n)$ implies $P(n+1)$.
    - That is, assume $P(n)$.
    - Then prove $P(n+1)$.

Proofs by induction

- Two ways to prove something $P(n)$ is true for every natural number n:

Direct proof

- Consider an arbitrary natural number n.
- Prove $P(n)$.

Proof by induction

- Prove $P(0)$.
- Consider an arbitrary natural number n.
- Prove $P(n)$ implies $P(n+1)$.
    - That is, assume $P(n)$.
    - Then prove $P(n+1)$.

Both proofs have the goal of proving P holds for an arbitrarily chosen natural number, but induction lets you make an extra assumption in your proof. This extra assumption can make it easier to reach your goal.

An example: tiling most of a square

Theorem

If you remove a single square from a $2^n \times 2^n$ grid, then you can tile the remaining squares with L-shaped trominos.

An example: divisibility

Theorem

$6^n - 1$ *is always a multiple of* 5.

An example: divisibility

Theorem

$6^n - 1$ *is always a multiple of* 5*.*

Proof.

(Base case)

An example: divisibility

Theorem

$6^n - 1$ *is always a multiple of* 5.

Proof.

(Base case) $6^0 - 1 = 0$ is a multiple of 5.

An example: divisibility

Theorem

$6^n - 1$ *is always a multiple of* 5*.*

Proof.

(Base case) $6^0 - 1 = 0$ is a multiple of 5.
(Inductive step) Assume $6^n - 1$ is a multiple of 5, i.e. $6^n = 5k + 1$ for some integer k.

An example: divisibility

Theorem

$6^n - 1$ *is always a multiple of* 5*.*

Proof.

(Base case) $6^0 - 1 = 0$ is a multiple of 5.
(Inductive step) Assume $6^n - 1$ is a multiple of 5, i.e. $6^n = 5k + 1$ for some integer k. Then,

$$6^{n+1} = 6(5k+1) = 30k + 6 = 5(6k+1) + 1.$$

So $6^{n+1} - 1 = 5(6k+1)$ is a multiple of 5. □

An example: divisibility

Theorem

$6^n - 1$ *is always a multiple of* 5*.*

Proof.

(Base case) $6^0 - 1 = 0$ is a multiple of 5.
(Inductive step) Assume $6^n - 1$ is a multiple of 5, i.e. $6^n = 5k + 1$ for some integer k. Then,

$$6^{n+1} = 6(5k+1) = 30k + 6 = 5(6k+1) + 1.$$

So $6^{n+1} - 1 = 5(6k+1)$ is a multiple of 5. □

You can generalize this proof: $a^n - 1$ is a multiple of $a - 1$ for every positive integer a.

An example: Fibonacci numbers

The Fibonacci numbers f_k are defined recursively:

- $f_0 = 0$;
- $f_1 = 1$;
- $f_{k+2} = f_k + f_{k+1}$.

An example: Fibonacci numbers

The Fibonacci numbers f_k are defined recursively:

- $f_0 = 0$;
- $f_1 = 1$;
- $f_{k+2} = f_k + f_{k+1}$.

Here are the first few Fibonacci numbers:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ \ldots$$

An example: Fibonacci numbers

The Fibonacci numbers f_k are defined recursively:

- $f_0 = 0$;
- $f_1 = 1$;
- $f_{k+2} = f_k + f_{k+1}$.

Here are the first few Fibonacci numbers:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ \ldots$$

When a sequence is defined recursively, it means that later values in the sequence depend on previous values. So induction is a natural way to prove facts about the Fibonacci numbers.

An example: Fibonacci numbers

Theorem

The Fibonacci numbers satisfy:

$$f_0{}^2 + f_1{}^2 + \cdots + f_n{}^2 = f_n \cdot f_{n+1}.$$

An example: Fibonacci numbers

Theorem

The Fibonacci numbers satisfy:

$$f_0^2 + f_1^2 + \cdots + f_n^2 = f_n \cdot f_{n+1}.$$

Proof.

(Base case) If $n = 0$ this is the statement $0^2 = 0 \cdot 1$.

An example: Fibonacci numbers

Theorem

The Fibonacci numbers satisfy:

$$f_0{}^2 + f_1{}^2 + \cdots + f_n{}^2 = f_n \cdot f_{n+1}.$$

Proof.

(Base case) If $n = 0$ this is the statement $0^2 = 0 \cdot 1$.
(Inductive step) Assume the equation holds for n, and consider this equation. Add $f_{n+1}{}^2$ to both sides:

$$f_0{}^2 + f_1{}^2 + \cdots + f_n{}^2 + f_{n+1}{}^2 = f_n \cdot f_{n+1} + f_{n+1}{}^2.$$

The right-hand side is then $f_{n+1}(f_n + f_{n+1})$. By the definition of the Fibonacci numbers, this is $f_{n+1} \cdot f_{n+2}$, which is exactly what we wanted to show. □

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Proof.

(Base case)

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Proof.

(Base case) $f_0 = 0 < 2^0 = 1$

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Proof.

(Base cases) $f_0 = 0 < 2^0 = 1$ and $f_1 = 1 < 2^1 = 2$.

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Proof.

(Base cases) $f_0 = 0 < 2^0 = 1$ and $f_1 = 1 < 2^1 = 2$.
(Inductive step) Assume $f_n < 2^n$ and $f_{n+1} < 2^{n+1}$.

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Proof.

(Base cases) $f_0 = 0 < 2^0 = 1$ and $f_1 = 1 < 2^1 = 2$.
(Inductive step) Assume $f_n < 2^n$ and $f_{n+1} < 2^{n+1}$. Then,

$$f_{n+2} = f_n + f_{n+1} < 2^n + 2^{n+1} < 2 \cdot 2^{n+1} = 2^{n+2}.$$

□

Another Fibonacci example

Theorem

The n-th Fibonacci number is always less than 2^n.

Proof.

(Base cases) $f_0 = 0 < 2^0 = 1$ and $f_1 = 1 < 2^1 = 2$.
(Inductive step) Assume $f_n < 2^n$ and $f_{n+1} < 2^{n+1}$. Then,

$$f_{n+2} = f_n + f_{n+1} < 2^n + 2^{n+1} < 2 \cdot 2^{n+1} = 2^{n+2}. \qquad \square$$

With common induction, we assume the result is true for the immediate prior natural number, and use that to prove the result for a new number. But we could instead assume the result is true for the two prior natural numbers (at the cost of needing an extra base case). The extreme version of this—which the book calls strong induction—is assuming the result is true for *all* smaller natural numbers to prove it's true for a new number.

An example: base-2 representations

Theorem

Every natural number has a unique base-2 representation.

An example: base-2 representations

Theorem

Every natural number has a unique base-2 representation.

Most commonly, we write numbers in base-10.

- For example,

$$7302 = 7 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0.$$

An example: base-2 representations

Theorem

Every natural number has a unique base-2 representation.

Most commonly, we write numbers in base-10.

- For example,

$$7302 = 7 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0.$$

But we can also write numbers in different bases. In base-2, the only bits (= binary digits) are 0 and 1.

$$110101 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

An example: base-2 representations

Theorem

Every natural number has a unique base-2 representation.

Most commonly, we write numbers in base-10.

- For example,

$$7302 = 7 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0.$$

But we can also write numbers in different bases. In base-2, the only bits (= binary digits) are 0 and 1.

$$110101 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

We don't write leading zeros, unless we're writing the number zero itself, which we do as 0.

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2*.*

Proof.

(base case) 0 is the empty sum—the sum of zero numbers—so it trivially is a sum of powers of 2.

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

Proof.

(base case) 0 is the empty sum—the sum of zero numbers—so it trivially is a sum of powers of 2.

(Inductive step) Suppose $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$ is uniquely expressed as a sum of powers of 2, where $m_1 < m_2 < \cdots < m_k$. Then,

$$1 + n = 2^0 + 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}.$$

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

Proof.

(base case) 0 is the empty sum—the sum of zero numbers—so it trivially is a sum of powers of 2.
(Inductive step) Suppose $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$ is uniquely expressed as a sum of powers of 2, where $m_1 < m_2 < \cdots < m_k$. Then,

$$1 + n = 2^0 + 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}.$$

If n didn't include 2^0 in its expression in powers of 2—that is, if n is even—then we are done. Otherwise, we have to carry the 1: combine the two 2^0 terms to get $2^1 = 2^0 + 2^0$.

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

Proof.

(base case) 0 is the empty sum—the sum of zero numbers—so it trivially is a sum of powers of 2.
(Inductive step) Suppose $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$ is uniquely expressed as a sum of powers of 2, where $m_1 < m_2 < \cdots < m_k$. Then,

$$1 + n = 2^0 + 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}.$$

If n didn't include 2^0 in its expression in powers of 2—that is, if n is even—then we are done. Otherwise, we have to carry the 1: combine the two 2^0 terms to get $2^1 = 2^0 + 2^0$. And now we repeat this process. If n had no 2^1 term, we are done. Otherwise, carry the 1, and combine the two 2^1 terms to get 2^2. Keep doing this process until we stop. □

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

Alternate proof using stong induction.

It's easy to check the $n = 0$ case, so let's consider the $n > 0$ case. Suppose that each $m < n$ can be expressed as a sum of powers of 2.

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

Alternate proof using stong induction.

It's easy to check the $n = 0$ case, so let's consider the $n > 0$ case. Suppose that each $m < n$ can be expressed as a sum of powers of 2. Let k be the largest integer so that $2^k \leq n$. (This is where we use $n > 0$.) Then, $n = 2^k + m$ for some integer $m < 2^k \leq n$. So adding 2^k to the binary expansion for m gives a binary expansion for n. We don't need to worry that 2^k appears in the binary expansion for m because $m < 2^k$. □

An example: base-2 representations

Theorem

Every natural number can be expressed as a sum of powers of 2.

Alternate proof using stong induction.

It's easy to check the $n = 0$ case, so let's consider the $n > 0$ case. Suppose that each $m < n$ can be expressed as a sum of powers of 2. Let k be the largest integer so that $2^k \leq n$. (This is where we use $n > 0$.) Then, $n = 2^k + m$ for some integer $m < 2^k \leq n$. So adding 2^k to the binary expansion for m gives a binary expansion for n. We don't need to worry that 2^k appears in the binary expansion for m because $m < 2^k$. □

We still have to prove that binary expansions are *unique*.

An example: base-2 representations

Theorem

Every natural number can be uniquely expressed as a sum of powers of 2.

An example: base-2 representations

Theorem

Every natural number can be uniquely expressed as a sum of powers of 2.

We will prove this by strong induction.

Proof.

Consider a natural number n, and suppose that all natural numbers $m < n$ have unique expressions as sums of powers of 2.

An example: base-2 representations

Theorem

Every natural number can be uniquely expressed as a sum of powers of 2.

We will prove this by strong induction.

Proof.

Consider a natural number n, and suppose that all natural numbers $m < n$ have unique expressions as sums of powers of 2.

Let k be the largest number so that $2^k \leq n$, so that $n = 2^k + m$ for some $m < 2^k \leq n$. Observe that 2^k must appear in the binary expression of n, as $2^{k+1} > n$ and summing up all the powers of 2 below k give $2^k - 1 < n$. So adding 2^k to the unique binary expression for m gives a unique binary expression for n. □