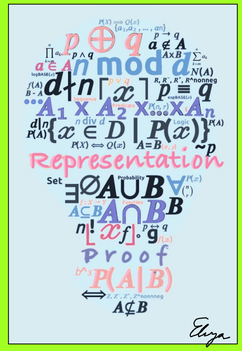
Discrete Structures



Lecture 11: More on induction

Susan L. Epstein

1

Last time

★ **Induction derives its power from *N***

- Induction is a proof method for infinite sets with cardinality $|N| = \aleph_0$
- Inductive proof has 2 parts: a basis followed by an inductive hypothesis

Fall 2023 CSCI 150 2/26

2

Today's outline

- Review of induction
- Trominoes
- Strong mathematical induction

Strong mathematical induction is a special case of mathematical induction

3

Review: proofs and infinite sets

Induction is a proof method for infinite sets that have exploitable regularity

Z an infinite set of logical statements

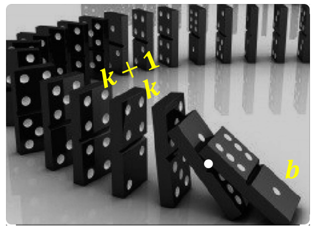
- Pushing the first domino is guaranteed
- Pieces are close enough to cause a chain reaction

4

Review: principle of mathematical induction

Let $P(n)$ be a property that is defined for integers n, and let b be a fixed integer. Suppose the following two statements are true:

- $P(b)$ is true b is called the basis
- For all integers $k \geq b$, if $P(k)$ is true then $P(k+1)$ is true



this inductive hypothesis assumes $P(k)$ and works to show that $P(k+1)$ is true

https://depositphotos.com/574666276/stock-video-black-dominoes-falling-row-slow.html

Then the statement "For all integers $n \geq b, P(n)$" Is true.

5

Reviews: infinitely many numbered statements

Let $P = \{P(b), P(b+1), \ldots, P(k), P(k+1), \ldots\}$ be an infinite set of sequentially numbered statements

$P(n) =$ nth statement **to be proved** P_n: $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

$P(b) =$ first statement **to be proved** if $b = 1$ P_1: $1 = \frac{1(1+1)}{2}$

$P(k) =$ kth statement where $n = k$ **assumed** P_k: $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$

$P(k+1) =$ $k+1$st statement where $n = k+1$ **to be proved**

$P(k+1)$: $1 + 2 + \cdots + k + k + 1 = \frac{(k+1)(k+2)}{2}$

To prove: $P(n)$: $\sum_{i=1}^{n} i^2$

Show $b = 1, P(b)$: $\sum_{i=1}^{1} i^2$

Assume $P(k)$: $\sum_{i=1}^{k} i^2$

Show $P(k+1)$: $\sum_{i=1}^{k+1} i^2$

To prove: $P(n)$: $\sum_{i=1}^{n} r^i = \frac{r^{n+1}-1}{r-1}$

Show $b = 1, P(b)$: $\sum_{i=1}^{1} r^i = \frac{r^{1+1}-1}{r-1}$

Assume $P(k)$: $\sum_{i=1}^{k} r^i = \frac{r^{k+1}-1}{r-1}$

Show $P(k+1)$: $\sum_{i=1}^{k+1} r^i = \frac{r^{k+2}-1}{r-1}$

6

Review: proof by mathematical induction

Theorem: Let $P(n)$ be (copy $P(n)$ here)
Proof by mathematical induction:
We must show that $P(n)$ is true for all $n \geq$ (state the basis value here)

Basis: Prove some initial case $P(b)$ is true (often but not always, $P(1)$)

Inductive step: Assume for some k that $P(k)$ is true.
By substitution (state $P(k+1)$ here).
We must show that $P(k+1)$ is true.
(prove that $P(k+1)$ is true)

SECRET: use $P(k)$ to prove $P(k+1)$

Since we have proved the basis step and the inductive step, the theorem is true.
QED

Fall 2023 CSCI 150 7/20

7

Review: setting up for induction

For each positive integer n, let $P(n)$ be the property $5^n - 1$ is divisible by 4.

- What is $P(0)$?
  $4|5^0 - 1$
- What is $P(k)$?
  $4|5^k - 1$
- What is $P(k+1)$?
  $4|5^{k+1} - 1$
- In any proof by mathematical induction what must be shown in the inductive step?
  That if $P(k)$ is true, then $P(k+1)$
  if $4|5^k - 1$ then $4|5^{k+1} - 1$

Fall 2023 CSCI 150 8/26

8

Review: example 1 (an arithmetic sum)

Theorem: Let $P(n)$ be $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof by mathematical induction:
We must show that $P(n)$ is true for all $n \geq 1$.

This is NOT algebra. You may only **work on 1 side at a time**.

Basis: $P(1)$ is $\sum_{i=1}^{1} i \stackrel{?}{=} \frac{1(1+1)}{2}$

Since the left side is 1 and the right side is $\frac{1(2)}{2} = \frac{2}{2} = 1$, $P(1)$ is true.

Inductive step: Assume for some k that $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ is true.

By substitution $P(k+1)$: $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2}$

We must show $P(k+1)$ is true. By definition of Σ, the left side of P_{k+1} is
$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} = \frac{k^2+k+2k+2}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}$ which is the right side of $P(k+1)$.

Since we have proved the basis step and the inductive step, the theorem is true. **QED**

How can you use $P(k)$ to prove $P(k+1)$?

Fall 2023 CSCI 150 9/20

9

Example 2 (*simple* geometric sum)

Theorem: Let $P(n)$ be P_n: $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$ for any $r \neq 1$ and integer $n \geq 0$.
Proof by mathematical induction:
We must show that $P(n)$ is true for all $n \geq 0$.
Basis: $P(0)$ is $\sum_{i=0}^{0} r^i \stackrel{?}{=} \frac{r^{0+1}-1}{r-1}$

Since the left side is $r^0 = 1$ and the right side is $\frac{r^1-1}{r-1} = 1$, $P(0)$ is true.

Inductive step: Assume for some k that $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$ is true.

By substitution $P(k+1) = \sum_{i=0}^{k+1} r^i \stackrel{?}{=} \frac{r^{k+2}-1}{r-1}$

We must show $P(k+1)$ is true. By definition of Σ, the left side of
$P(k+1)$ is $\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + \left(r^{k+1}\right) = \frac{r^{k+1}-1}{r-1} + r^{k+1} = \frac{r^{k+1}-1}{r-1} + r^{k+1}$
$\frac{r^{k+1}-1+(r-1)r^{k+1}}{r-1} = \frac{r^{k+1}-1+r^{k+2}-r^{k+1}}{r-1} = \frac{r^{k+2}-1}{r-1}$ = the right side of $P(k+1)$.

Since we have proved the basis step and the inductive step, the theorem is true.
QED

Fall 2023 CSCI 150 10/21

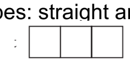
10

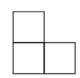
Today's outline

✓ Review of induction
- Trominoes
- Strong mathematical induction

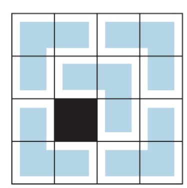
Trominoes

- Tromino = 3 attached same-size squares
- Come in 2 shapes: straight and L-shaped





- Checkerboard = $n \times n$ square formed from $n \cdot n$ attached same-size squares
- Some checkerboards with 1 square missing can be covered completely by L-shaped trominoes



- But a 3×3 square cannot be covered completely by L-shaped trominoes

why not?

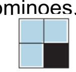
Proof for trominoes (1)

Theorem: Let $P(n)$ be for any integer $n \geq 1$, if one square is removed from a $2^n \times 2^n$ checkerboard, it can be completely covered by L-shaped trominoes.

Proof by mathematical induction:

We must show that $P(n)$ is true for all $n \geq 1$.

Basis: $P(1)$ a $2^1 \times 2^1$checkerboard missing 1 square can be covered completely by trominoes. P_1 is true since all possible such checkerboards are symmetric to



Inductive step: Assume for some k, $P(k)$ is true, that is, a $2^k \times 2^k$ checkerboard missing 1 square can be covered completely by trominoes.

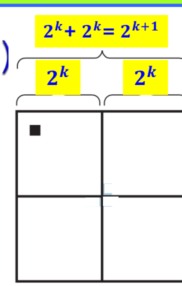
We must show $P(k+1)$ that a $2^{k+1} \times 2^{k+1}$ checkerboard missing 1 square can be covered completely by trominoes is true.

Any ideas? How can you use P_k to show P_{k+1}?

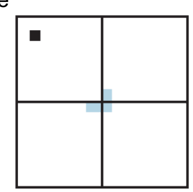
Fall 2023 CSCI 150 13/26

13

Proof for trominoes (2)



- Subdivide the $2^{k+1} \times 2^{k+1}$ checkerboard into 4 equal quadrants and remove any 1 square from 1 of the quadrants.
- Since that is a $2^k \times 2^k$ checkerboard missing 1 square, by P_k we know that we can cover it completely by trominoes
- What about the other 3 quadrants?
- If we put an L-shaped tromino at the center of the $2^{k+1} \times 2^{k+1}$ checkerboard so that it covers 1 square in each of the three remaining quadrants, they are also $2^k \times 2^k$ checkerboards missing 1 square can also be covered completely by trominoes.



Since we have proved the basis step and the inductive step, the theorem is true.
QED

Fall 2023 CSCI 150 14/26

14

Today's outline

- ✓ Review of induction
- ✓ Trominoes
- Strong mathematical induction

15

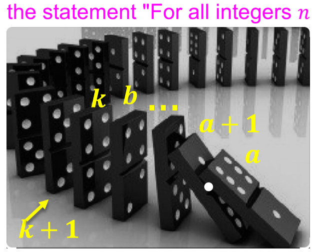
Principle of strong mathematical induction

(aka the second principle of induction, the second principle of finite induction, the principle of complete induction):

Let $P(n)$ be a property that is defined for integer n and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

- $P(a), P(a+1), \ldots P(b)$ are true
- For any integers $k \geq b$, if $P(a), P(a+1), \ldots, P(\boldsymbol{k})$ are all true then $P(k+1)$ is true

Then the statement "For all integers $n \geq b, P(n)$" Is true.



Strong induction begins with **multiple consecutive** bases

Strong induction relies on 1 or more $P(i)$ **up to $\boldsymbol{P(k)}$**

16

Encore: proof by mathematical induction skeleton

Theorem: Let $P(n)$ be (copy $P(n)$ here)
Proof by mathematical induction:
We must show that $P(n)$ is true for all $n \geq$ (state the basis value here)

Basis: Prove some initial case $P(b)$ is true (often but not always, $P(1)$)

Inductive step: Assume for some k that $P(k)$is true.
By substitution (state $P(k+1)$ here).
We must show that $P(k+1)$ is true.
(prove that $P(k+1)$ is true)

SECRET: use $P(k)$ to prove $P(k+1)$

Since we have proved the basis step and the inductive step, the theorem is true.

QED

17

Proof by strong mathematical induction skeleton

Theorem: Let $P(n)$ be (copy $P(n)$ here)
Proof by strong mathematical induction:
We must show that $P(n)$ is true for all $n \geq$ (state basis value(s) here)

Basis: Prove some initial case(s) $P(a), P(a+1), \ldots, P(b)$ are true

Inductive step: Assume for some k that $P(a), P(a+1), \ldots, P(k)$ are **all** true
By substitution (state $P(k+1)$ here)
We must show that $P(k+1)$ is true.
(prove that $P(k+1)$ is true)

Since we have proved the basis step and the inductive step, the theorem is true.
QED

Fall 2023 CSCI 150 18/27

18

Example: divisibility by a prime (1)

Theorem: Let $P(n)$ be any integer n is divisible by a prime for $n \geq 2$.

Proof by strong mathematical induction:

We must show that $P(n)$ is true for all $n \geq 2$.

Basis: $P(2) = 2$ is divisible by a prime.

Because $2|2$ and 2 is prime, $P(2)$ is true.

Inductive step: Assume for some $k \geq 2$ that $P(2), \ldots, P(k)$ are all true.

By substitution $P(k+1) = k+1$ is divisible by a prime.

We must show that $P(k+1)$ is true.

There are 2 cases: $k+1$ is prime or it is not.

Case 1: $k+1$ is prime

Then $(k+1)|(k+1)$ and $P(k+1)$ is true.

(continued)

Example: divisibility by a prime (2)

Case 2: $k+1$ is not prime

By definition of composite there are positive integers a and b such that $k+1 = ab$ where $1 < a < k+1$ and $1 < b < k+1$.

Since $a < k+1,\ P(a)$ is true so there exists a prime p that divides a, that is, $a = pq$ for some integer q.

But we don't know *which* prime. That's why we need strong induction.

But $k+1 = ab$ so $k+1 = pqb$ and by definition of divisibility $p|(k+1)$ and $P(k+1)$ is true.

Since we have proved the basis step and the inductive step is true regardless of which is the case, the theorem is true.

QED

Example: property of a sequence

Theorem: Define a sequence $s_0, s_1, s_2, \ldots$, by $s_0 = 0$, $s_1 = 4$, $s_k = 6s_{k-1} - 5s_{k-2}$. Let $P(n)$ be $s_n = 5^n - 1$ for $k \geq 2$.

Proof by strong mathematical induction:

We must show that $P(n)$ is true for all $n \geq 2$ with basis $P(0)$ and $P(1)$.

Basis: $P(0)$: $5^0 - 1 = 1 - 1 = 0 = s_0$ and $P(1) = 5^1 - 1 = 4 = s_1$.

Inductive step: Assume for some $k \geq 2$ that $P(0), \ldots, P(k)$ are all true, that is, for all integers a such that $0 \leq a \leq k$, $P(k) = 5^k - 1$.

By substitution $P(k+1)$ is $s_{k+1} = 5^{k+1} - 1$. We must show that $P(k+1)$ is true. By definition and the inductive hypothesis,

$s_{k+1} = 6s_{k+1-1} - 5s_{k+1-2} = 6s_k - 5s_{k-1} = 6(5^k - 1) - 5(5^{k-1} - 1) =$
$6 \cdot 5^k - 6 - 5 \cdot 5^{k-1} + 5 = 6 \cdot 5^k - 6 - 5^k + 5 = (6-1)\, 5^k - 6 + 5 =$
$5 \cdot 5^k - 1 = 5^{k+1} - 1$ so $P(k+1)$ is true.

Since we have proved the basis step and the inductive step, the theorem is true.

QED

Fall 2023 CSCI 150 21/26

21

Review: numeric representation

- Base 10 represents integers in base 10 with the symbols $\{0,1,2,3,4,5,6,7,8,9\}$ to multiply powers of 10 and sum those products
  $$2935 = 2 \cdot 10^3 + 9 \cdot 10^2 + 3 \cdot 10^1 + 5 \cdot 10^0$$
- Base 2 (binary representation) represents integers with the symbols $\{0,1\}$ to multiply powers of 2 and sum the products
  $$1001 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$
- Base b represents integers with the symbols $\{0,1,2,\ldots,b-1\}$ to multiply nonnegative powers of b and sum the products
  $$c_r \cdot b^r + c_{r-1} \cdot b^{r-1} + \ldots + c_1 \cdot b^1 + c_0 \cdot b^0$$
- Binary representation is used in computers to signify
  - Presence or absence of electrical charge
  - Presence or absence of magnetic field
  - Open or closed electrical switch
- For any base $b \geq 2$ and for any symbols $c_i \in \{0,1,2,\ldots,b-1\}$
  $$b^{r+1} > c_r \cdot b^r + c_{r-1} \cdot b^{r-1} + \ldots + c_1 \cdot b^1 + c_0 \cdot b^0$$

base 10: $10^3 = 1000 > 999, 998, 997, \ldots$ base 2: $1000 > 111, 110, 101, \ldots$

Fall 2023 CSCI 150 22/26

22

Example: unique binary representation (1)

Theorem: $P(n)$ = any positive integer n has a unique representation in the form $n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0$ where r is a nonnegative integer, $c_r = 1$, and $c_j \in \{0,1\} \, \forall j = 0,1,2,\dots,r-1$.
Proof that such a representation exists by strong mathematical induction:
We must show that $P(n)$ is true for all $n \in N, n > 0$.

Basis: $P(1)$: For $r = 0$, and $c_0 = 1, n = 1$, so $P(1)$ is true.

Inductive step: Assume for some $k \geq 1$ that $P(1), \dots, P(k)$ are all true.

By substitution, $P(k+1)$ is for all integers a such that $1 \leq a \leq k$, $P(a)$ has form $n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0$ where r is a nonnegative integer, $c_r = 1$, and $c_j \in \{0,1\} \, \forall j = 0,1,2,\dots,r-1$.
We must show that $P(k+1)$ is true.
There are 2 cases: either $k+1$ is even or it is odd.

(continued on the next slide)

Example: unique binary representation (2)

Case 1: $k+1$ is even. Then $\frac{k+1}{2}$ is an integer and $1 \leq \frac{k+1}{2} \leq k$.
By definition of even, and by the inductive hypothesis where r is a nonnegative integer, $c_r = 1$, and for a set of c's that are 0 or 1, with $c_0 = 0$ since even numbers represented in binary end in 0.

$$\frac{k+1}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0$$

Multiplication by 2 yields
$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2 + 0$ and $P(k+1)$ is true.

Case 2: $k+1$ is odd. Then k is an even integer, $\frac{k}{2}$ is an integer, $1 \leq \frac{k}{2} \leq k$,
By definition of even, $c_0 = 0$ and by the inductive hypothesis where r is a nonnegative integer, $c_r = 1$, and for a set of c's that are 0 or 1, with $c_0 = 0$,

$$\frac{k}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0$$

Thus $k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2 + 1$ and $P(k+1)$ is true. Since we have proved the basis step and the inductive step is true regardless of which is the case, such a representation exists.

But we aren't done! Why not?)

Example: unique binary representation (3)

To prove by contradiction that the representation is unique, assume some integer has 2 different representations as the sum of nonnegative integer powers of 2 where all c_i's and d_i's are 0 or 1. We will show that this assumption logically leads to a contradiction.

Since they represent the same number, we set the representations equal to one another and remove all identical terms.

$c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 = d_r \cdot 2^s + d_{r-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0$

Assume without loss of generality that $r < s$. Changing all the c_i's to 1's, $c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 \leq 2^r + 2^{r-1} + \cdots + 2 + 1$ and by the formula for the sum of a geometric series, the right side equals $2^{r+1} - 1$.

Because $r < s$, the c_i representation has a 0 for 2^s and so $2^{r+1} - 1 < 2^s$.

This contradicts the assumption that the representations produce equal values. Because the assumption led to a contradiction, the representation must be unique.

QED

Any questions?

25

Proof methods (so far)

Truth table

Sequence of statements with reasons

Valid argument forms (modus ponens, modus tollens,…)

Method of exhaustion

Predicate logic (quantification, existence, uniqueness)

Proof by cases

Generalization from the generic particular

Proof by contradiction

Proof by contraposition

Mathematical induction

Strong mathematical induction

26

What you should know

- ★ **Strong mathematical induction is a special case of mathematical induction**
- Strong mathematical induction relies on a sequence of consecutive integers for its basis
- Strong mathematical induction can reference any of its bases during proof
- Multiple ways to construct a proof

Any questions?

Test 1 during next lecture time

Next up: *Introduction to set theory*

Time to finish up that Opening sheet!

Problem set 11,12 is due on Thursday, October 19 at 11PM