Proof

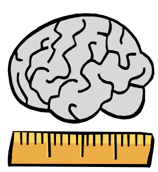
Part 4

Theorems

The Big Bang Theory

Theorems

- A *theorem* is a statement we intend to prove using existing known facts (called *axioms* or *lemmas*)
- Used extensively in all mathematical proofs – which should be obvious



Example

- Most theorems are of the form: If X, then Y
- The theorem below is very easy to interpret

If x and y are even integers
then x * y is an even integer

Example

- Theorems are arguments
- They can be structured as such.

```
x is even
y is even
_____________
x * y is even
```


Example

- Sometimes it is hard to see
- Below, the same theorem is written using different language

Suppose x and y are even integers. The product is even.

The product xy is even when x and y are both even.

Some Basic Definitions

Abstract? Not really.

Definition: x is even

x is even if and only if…

x = 2n for some integer n

Definition: x is odd

x is odd if and only if…

x = 2n + 1 for some integer n

Definition: x | y (x divides y)

x | y (x divides y) iff…

y = x * k for some integer k

Definition: $x \in Q$ (x is a rational)

x is a rational number iff…

x = y / z for some integers y and z, and $z \neq 0$

Proving $A \rightarrow B$

Modus Ponens

Proving A → B

- The boolean operator A → B is true <u>except</u> when A is true and B is false
- So, we prove A → B by showing that *whenever A is true, so **<u>must</u>** B*

Proving A → B

- This is essentially a *Modus Ponens* proof
- You are showing that if A is true, and A → B is true, then B must be true
- Also note that "A" and "B" can be compound statements

Modus Ponens

A → B Prove always true

A If this is true

B

The Steps

- There are basically just two steps to follow:
  1. Assume A is true
  2. Argue that B is true
- This shows that B is true whenever A is true

Example

- Let's prove the following theorem from before
- This is actually quite easy

If x and y are even integers
then x * y is an even integer

Example – the argument

```
x is even
y is even
_________
x * y is even
```

Example – internal structure

- Remember: all proofs are implications
- So, we will assume the both premises are true and show conclusion must be true.

```
x is even ∧ y is even → x * y is even
```


Example

```
Assume that x and y are even integers.

So, by the definition…

x = 2i and y = 2j (for some i, j)

Note: use different arbitrary variables
or you are assuming they are equal!
```


Example

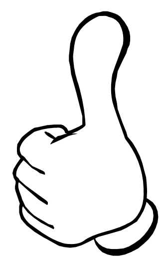
```
So, the product is:

x * y = 2i * 2j
      = 4 * i * j
      = 2 * (2 * i * j)

So, by definition, x * y is even
```

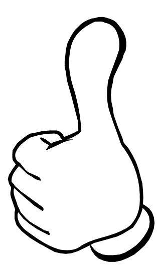

Proof Tips

- Begin your proof with what you assume to be true (the hypothesis)
- Don't argue the truth of a theorem *by example*
  - stay abstract
  - e.g. you know x and y are even integers – that's all you know



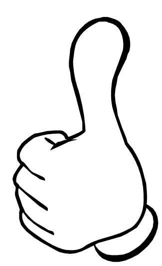
Proof Tips

- Your proof must work forward from your assumptions to your goal
- You may work backward on scratch paper to help you figure out how to work forward



Proof Tips

- Write your proof in prose
- Then read out loud, it should sound like well-written paragraph
- Quite often you'll use definitions to make progress



Example

- The following is a theorem about the product of an odd and even number
- The proof is straight-forward using the definitions

If x is even and y is odd, then x * y is even

Example

Assume:

x is an even integer and
y is an odd integer.

Then x = 2i and y = 2j+1 for some integers i and j

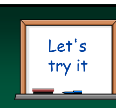
Example

```
Multiplying, we get:

x * y = (2i) * (2j + 1)
      = 4ij + 2i
      = 2 * (2ij + i)

...which is even
```

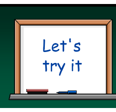

Example: Let's Try…



- The following is a theorem about the sum of two odd numbers
- *Let's try this one…*

If x is odd and y is odd, then x + y is even

Example: Let's Try…



- How about something more complicated?
- The following is a theorem about the product of two odd numbers
- *Let's try…*

If x is odd and y is odd, then x * y is odd

Proof by Contrapositive

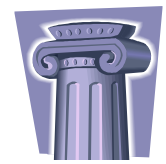
Proof with inverse logic

Proof by Contrapositive

- There are several techniques that can be employed to prove an theorem
- The direct approach, like before is quite common, but its not the only path you can take

Proof by Contrapositive

- *Proof by Contrapositive* has you prove the opposite of the original theorem
- Quite impressively, this will also prove the original theorem



Getting the Contrapositive

- First
  - negate both the assertion and conclusion of the implication
  - so, basically, put "not" in front of both operands
- Second…
  - reverse the implication
  - you basically swap the left-hand and right-hand operand of the implication

Getting the Contrapositive

- So, both operands swap positions and are negated
- Are they equal? Let's confirm in a Truth Table

```
p → q   composite is:  ¬ q → ¬ p
```


Contrapositive Truth Table

p	q	¬ q	¬ p	p → q	¬ q → ¬ p
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

Modus Ponens Contrapositive

Prove always true

```
¬ B → ¬ A
¬ B
```

If this is true

```
―――――――――
¬ A
```

How it Works

- So, if we prove the contrapositive, we also prove the original theorem
- For the original A → B
  - suppose that if B is false
  - show that A must be false
- It does make sense, if you think about it

Example

- The following is a theorem should look familiar
- This theorem states that the square of a odd number is also odd
- *Direct proof is near impossible!*

If x^2 is odd then x is odd

Example Contrapositive

- The contrapositive negates each operand in the implication A → B
- The following shows the reverse of each

A = x^2 is odd

¬ A = x^2 is not odd = x^2 is even

Example Contrapositive

- The contrapositive negates each operand in the implication A → B
- The following shows the reverse of each

B = x is odd

¬ B = x is not odd = x is even

Example Contrapositive

- Finally, we reconstruct our theory with B → A rather than A → B
- This expression is equivalent to the original

if x is not odd then x^2 is not odd

or… if x is even then x^2 is even

Example Contrapositive

We assume x is not odd

***x is not odd* means x is even**

x = 2k for some integer k

Example Contrapositive

```
We assume x is not odd (even)

x²   = (2k)²
     =  4k²
     =  2(2k²)

So, x² is even which is not odd
```


Example Result

We proved:
if x is even then x^2 is even

By contrapositive, we proved:
if x^2 is odd then x is odd

Proof by Contradiction

Welcome down the rabbit hole

Proof by Contradiction

- *Proof by Contradiction* takes a novel approach
- It uses the approach of *reductio ad absurdum*
- So what is it? Well, it proves the theorem by showing it <u>can't</u> be false

But, How?

- Assume it is false
- Show that (if it is false) something impossible results
- Therefore, it can't be false and, thus, true!

Contradicting Implications

- So, if you are proving $A \rightarrow B$
- Assume $A \wedge \neg B$ ...which is equivalent to $\neg(A \rightarrow B)$
- Show that something *impossible* results – therefore, $A \rightarrow B$

Contradiction

A	B	¬ B	A ∧ ¬B	¬ (A → B)
T	T	F	F	F
T	F	T	T	T
F	T	F	F	F
F	F	T	F	F

Example

- The following is a classic Proof By Contradiction
- The theorem covers if the square-root of 2, is an irrational number

The square root of 2 is irrational

Example

- To prove by contradiction, we need to show that the opposite cannot be true (i.e. false)
- The sentence bellow is the theorem negated
- So, how do we go about proving this?

The square root of 2 *is rational*

Example

- Well, what is a rational number?
- A rational number can be expressed as "a / b" where a and b are *integers with no common factors* (aka "lowest terms")

The square root of 2 *is rational*

Examples of Rational Numbers

- **1 / 3**
- **7 / 1**
- **22 / 7**
- **7734 / 10001**
- **1 / 123456789**
- **5 / 3**

The Proof: Prove Opposite

```
√2 is rational

√2   = a / b where a, b ∈ Z
       and b ≠ 0
       and a, b have no common factors
```

Analyzing a

$\sqrt{2}$ = a / b

Let's look at the properties of a

$\sqrt{2}$ * b = a

2 * b^2 = a^2

Analyzing a – It is even

2 * b^2 = a^2

So… a^2 is an even number

therefore we know a is also even
(previous proof – even × even)

Analyzing b

Since a is even and a / b is in lowest terms, then <u>b must be odd</u>

Why? If b is even, then a / b would have common factors – namely 2.

Example: Oh ohhhhh

However… look again at 2 * b^2 = a^2

Since a is even, a^2 is a multiple of 2^2 (aka, a multiple of 4)

So, 2 * b^2 is also a multiple of 4

Thus, <u>b is even</u>

Result

Since b <u>has</u> to be <u>both</u> odd and even, we have a contradiction

The theorem "square root of 2 is rational" <u>cannot</u> be true

Therefore, "square root of 2 is irrational" is true

Predicate Logic

Just the facts…

Predicate Logic

- A predicate is a statement about one or more variables
- It is stated as a fact – being true for the data provided

Predicate Logic

- Predicates express *properties*
- These can apply to a single entity or *relations* which may hold on more than one individual

Predicate Notation

- It follows the same basic syntax as function calls in Java (and most programming languages)
- However, type case is important:
  - constants start with lower case letters
  - predicates start with upper case letters

Single variable predicate

- Predicates can have one variable (at a minimum)
- The following sentence states one that the cat named Pattycakes has the "sleepy" property

```
"Pattycakes The Cat is sleepy"
```


Single variable predicate

- Alternatively, we can write it in predicate form
- The "Sleepy" predicate for "Pattycakes" is true
- Note the uppercase and lowercase!

```
Sleepy(pattycakes)
```


Two Variable Predicate

- Predicates can have multiple variables (unlimited actually… well within reason)
- The following is a classic example of a two-variable relationship

```
x < y
```

Two Variable Predicate

- The LessThan predicate is true for x, y

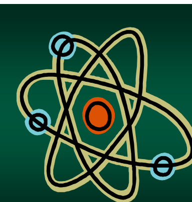
```
LessThan(x, y)
```


Predicates Summary

- 1-place predicates assign properties to individuals:
  - ___ is a cat
  - ___ is sleepy
- 2-place assign relations to a pair
  - ___ is sleeping on ___
  - ___ is the capitol of ___

Predicates Summary

- 3-place predicates assign relations to triples
  - ___ wants ___ to ____
  - Cat named ____ likes to ___ on ____
- Etc…

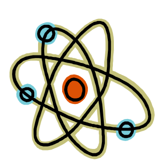


Quantified Statements

More Symbols

Quantified Statements

- Sometimes we want to say that *every element in the universe* has some property
- Let's say the universe is the people in this room and we want to say "*everyone in the room is awake*"



Limitations of Propositional Logic

- While propositional logic can express a great deal of complex logical expressions, it ultimately is insufficient for all arguments
- Why? The premises (and conclusions) in propositional logic have no internal structure.

Propositional Approach #1

- We can write out a descriptive sentence
- Shortcomings:
  - it is monolithic an inflexible
  - not "mathematical" enough

```
Everyone in this room is awake.
```

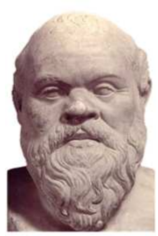

Propositional Approach #2

- We can also write out that sentence using a long list of predicates
- So, we list them all <u>or</u> make a pattern
- Shortcomings: Cumbersome & verbose

```
P(moe) and P(larry) and P(curly) and …
```


Limitations of Propositional Logic

- For example, it cannot show the validity of Socrates Argument
- This arguments states:
  "All humans are mortal.
  Socrates is a human.
  Therefore, he is mortal."



Socrates Argument

- The following is the propositional logic form of the Socrates Argument
- Can we prove the conclusion?

```
All humans are mortal
Socrates is a human
______________________________
Therefore, Socrates is mortal
```

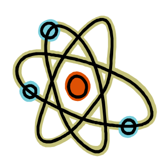

The Socrates Argument

- The following is the argument in normal form
- A problem arises since the validity of this argument comes from the internal structure which propositional logic cannot "see"

```
H
S
__
M
```


Solution

- It's time to break apart the logic and see the internal structure
- So, we are splitting the atom!



Why go nuclear?

1. Expose the internal structure of those "atomic" sentences
2. Create new terminology to describe the semantics
3. Introduce laws to use and manage them

New Notation: For All

- The "For-All" symbol states every element *x* in the universe makes P(*x*) true
- So, it is true if and only if the every P is the universe is true

$\forall_x$ **P(x)**

New Notation: Exists

- The "Exists" States at least one element *x* in the universe makes P(*x*) true
- True if just a single P is true

$\exists_x$ **P(x)**

Example: Pineapple Pizza

- Let's create the quantified statement for *"Someone doesn't like pineapple pizza!"*
- Let's create a predicate P(x) means *"x likes pineapple pizza"*
- What does someone mean? At least one person?

Pineapple Pizza: Try #1

- How about the following expression?
- It's not true if at least one person likes pineapple
- This means *"nobody likes pineapple pizza"*

$\neg$ ($\exists_x$ **P(x)**)

Pineapple Pizza: Try #2

- We can also negate the predicate
- Means, for at least one person, they dislike pineapple pizza
- Which is: *"someone doesn't like pineapple pizza!"*

$\exists_x$ $\neg$ **P(x)**

Quantifier Equivalence

Quantifier Conversion

Equivalence

- Just like propositional logic, quantitative expressions have equivalencies
- They follow the same basic logic we have seen before

Example: Opposite Expression

- Example: "Everyone in the room is awake"
- Let's create the opposite of this expression *(that still says the same thing)*

"Everyone in the room is awake."

Example: Opposite Expression

- So, let's just negate the predicate "is awake" into "is asleep"
- Does that work? No.

"Everyone in the room is asleep."

Example: Opposite Expression

- Now, let's negate the quantifier "everyone'" (for-all) into "someone" (exists)
- The expression below works: almost

"Someone in the room is asleep."

Example: Opposite Expression

- Well, what if we negate the quantifier "everyone'" (for-all) into "someone" (exists)
- The expression below works: yes

"There is no one in the room that is asleep."

Exists and For-All

- The previous two laws allows us to extrapolate two additional laws
- Note: we simply push the negative and remove the double-negation

$$\forall_x\ P(x)\ \equiv\ \neg\ \exists_x\ \neg\ P(x)$$

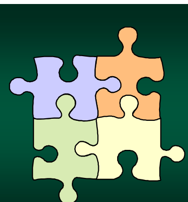
$$\exists_x\ P(x)\ \equiv\ \neg\ \forall_x\ \neg\ P(x)$$

Equivalence – Moving Negation

- You can push a negation through a quantifier by toggling the quantifier
- Read the expressions below carefully

$$\neg\ \exists_x\ P(x)\ \equiv\ \forall_x\ \neg\ P(x)$$

$$\neg\ \forall_x\ P(x)\ \equiv\ \exists_x\ \neg\ P(x)$$

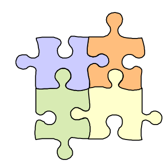


Conjunction & Disjunction

Breaking Apart and Combining

Conjunction & Disjunction

- Both the Exists and For-All quantifiers can be broken apart (and combined)
- This can occur if the expression contains an AND or an OR



Exists Disjunction

- If the Exists quantifier is used on a disjunction, it can be broken into two Exists
- This only works with $\vee$

$$\exists_x (P(x) \vee Q(x))\ \equiv\ \exists_x P(x)\ \vee\ \exists_x Q(x)$$

For-All Conjunction

- If the For-All quantifier is used on a conjunction, it can be broken into two For-All
- This only works with $\wedge$

$$\forall_x (P(x) \wedge Q(x))\ \equiv\ \forall_x P(x)\ \wedge\ \forall_x Q(x)$$

Bound & Free Variables

Some variables are not variable

Bound & Free Variables

- Not all variables used in a quantified expression is treated the same
- Each variable in an expression is either considered "bound" or "free"

Bound & Free Variables

- A variable is *free* if a value must be supplied to it before expression can be evaluated
- A variable is *bound* if it not free (usually a dummy variable) and contains values that are not needed to be evaluated

Example 1

- Which variables need we supply a value before the expression can be evaluated?
- Both x and c
- Without knowing both we cannot evaluate the expression (both are free)

```
(x ^ 2 < 4 * c)
```


Example 2

- Which variables need to be supplied before the expression can be evaluated?
- x: no, it is a dummy variable
- c: yes, once we give a value for c, we can evaluate the expression

$\forall_x$ `(x ^ 2 < 4 * c)`

Multiple Quantifiers

Many E's and A's doing headstands

Multiple Quantifiers

- A quantified statement may have more than one quantifier
- In fact, most of the time, statements will contain several

Example

- x > y is an expression with two variables
- The expression is true if an x is supplied which is greater than y

$\forall x \; \exists y \; P(x, y)$

Example

- ∃y (x > y) is an expression with one free variable
- Evaluates to true if x is supplied and there is a y greater than the supplied x

$\forall x \; \exists y \; P(x, y)$

Example

- ∀x ∃y (x > y) contains no free variables
- Evaluates to true if ∃y (x > y) is true for every x in the universe.

$\forall x \; \exists y \; P(x, y)$

Example 2

- The following in an implication with two quantifiers as operands
- It states that whenever "∀x P(x)" is a true statement, then so is "∀x Q(x)".

$\forall x \; P(x) \rightarrow \forall x \; Q(x)$

Difficult Example

- Let's create a quantified statement for the following logical statement
- *We will go slowly, since this is not easy*

Everyone who has a friend who has measles will have to be quarantined

Difficult Example

- "Everyone" is a For-All relationship
- So, we can factor it out into the expression below
- *Now*, let's look at the sub expression…

```
∀x (if x has a friend with measles,
    then x must be quarantined)
```


Difficult Example

- The sentence *" if x has a friend with measles, x must be quarantined"* is an implication!
- Let's look at the antecedent (hypothesis)

```
if x has a friend with measles,
   then x must be quarantined
```


Difficult Example

- How do we say "*x has a friend with measles*"?
- They just need a single friend
- So, this is an Exists quantifier

```
∃y (x is friends with y, and y has measles)
```


Difficult Example

- Now that we have a basic form of the final version, let's make some predicates
- We will use single letter names for brevity

```
F(x, y) means "x and y are friends"
M(x)    means "x has measles"
Q(x)    means "x must be quarantined"
```


Difficult Example

- This says: "There exists a *person y* where *y* is friends with *person x*, and *y* has measles"
- Note: *x* is not bound in this expression

$$\exists y \; (F(x, y) \land M(y))$$

Difficult Example

- So, what happens if a friend has measles?
- Then, they must be quarantined
- Note: implication is outside the exists

$$\exists y \; (F(x, y) \land M(y)) \rightarrow Q(x)$$

Difficult Example

- Now we can put it all together…
- The following is the quantified expression for our original statement

$$\forall x \; (\; \exists y \; (F(x, y) \wedge M(y)) \rightarrow Q(x) \;)$$

Bounded Quantifiers

Hidden Implication
(for those who hate to type)

Bound Quantifiers

- Some quantifiers can be more than meets the eye
- For brevity, many predicate and propositional expresses are merged with the $\forall$ and $\exists$

Shorthand Notation

- The following type of expression is quite common
- So much so that a shortcut notation is often employed

$$\forall_x \; (R(x) \rightarrow P(x))$$

Shorthand Notation

- The membership sub-expression is moved to the quantifier's subscript
- This is equivalent to the last

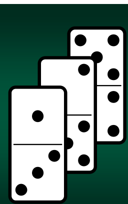
$$\forall_{R(x)} P(x)$$

Likewise…

- The sub-expression before the implication can be anything
- In this example, x > 5 is moved to the subscript

$$\forall_x \; (x > 5 \rightarrow P(x))$$

$$= \forall_{x > 5} \; P(x)$$

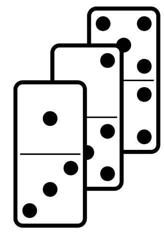


Induction

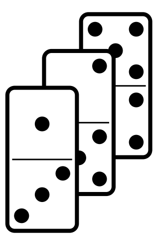
Proof by Pattern

Induction

- Many proofs, in fact a great number of them, are based on "all positive integers"
- *Induction* is a technique of proving a theorem that is based on this criteria

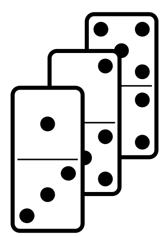


Induction



- The proof by induction is based on the *Well-Ordering Property*
- It states that: given a set of non-negative numbers there is a *least* element

Induction



- Induction basically helps prove $\forall x\ P(x)$ where the universe is positive numbers
- *Or any range starting at one point and going off to infinity (positive or negative)*

How it Works

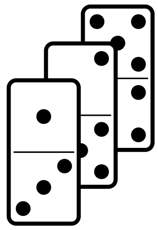
- It works in 2 steps
  1. proving P(1) and then
  2. proving that $P(n) \rightarrow P(n + 1)$
- As a result...
  - since $P(n) \rightarrow P(n + 1)$
  - then $P(n + 1) \rightarrow P(n + 2)$ and so on…

Metaphor: Line

- There is a line of people
- First person tells a secret to the second person
- The second person then tells it to the third
- … and so on until everyone knows the secret

Metaphor: Dominos

- You have a long row of Dominos
- The first domino falls over and hits the second domino
- The second hits the third
- … and so on until they are all knocked over



Foundation of Induction

- The following summarizes the proof technique
- It is important to understand the approach since it is so commonly used

$$P(1) \land \forall n\ (P(n) \rightarrow P(n+1)) \rightarrow \forall n\ P(n)$$

Steps to Proof

- Step 1: *Basis*
  - show the proposition P(1) is true
  - very easy to do – just plug in the values
- Step 2: *Induction*
  - assume P(n) is true (which is your theorem)
  - show that P(n + 1) must be true

Example: Sum of Odds

Using induction…

Show that the sum of n odd numbers equals n^2

Example: Sum of Odds

- So, the sum of odd numbers is a square?
- Is that true?
  - 1 + 3 = 4
  - 1 + 3 + 5 = 9
  - 1 + 3 + 5 + 7 = 16
- Okay, that's just odd! *(pun intended)*

Basis: Sum of Odds

- The sum of odds, for just 1 number is simply 1
- Of course, this is also 1 squared

$$P(1) = 1 = 1^2$$

Induction: Sum of Odds

P(n) is written as:
$1 + 3 + 5 + ... + (2n - 1) = n^2$

We assume P(n) is true.

Now we prove $P(n) \rightarrow P(n + 1)$

Induction: Sum of Odds

P(n + 1) is written as:

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

Let's look at the left hand side of the equation

Induction: Sum of Odds

$1 + 3 + … + (2n - 1) + (2n + 1)$

$= 1 + 3 + … + (2n - 1) + (2n + 1)$

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

$= (n + 1)^2$

P(n) assumed true, so the equality is true. You can replace!

Induction: Sum of Odds

So, we have shown that when P(n) is true, then P(n + 1) is true.

$P(n) \rightarrow P(n + 1)$

Since P(1) is true, we have proved
$\forall n\ P(n)$

Example: Divisible by 3

Using induction…

Show that $n^3 - n$ is divisible by 3 whenever n is a positive integer

Basis: Divisible by 3

- For our basis, we plug 1 into our expression and get the result
- The result, 0, is divisible by 3.

$P(1) = 1^3 - 1 = 1 - 1 = 0$

Induction: Divisible by 3

P(n) is written as:

$n^3 - n$

P(n + 1) is written as:

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

Induction: Divisible by 3

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

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

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

$= n^3 - n + 3n^2 + 3n$ Rearranged

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

Induction: Divisible by 3

So, for $(n^3 - n) + 3(n^2 + n)$

Since we assumed P(n) is true, then $(n^3 - n)$ is divisible by 3.

… and $3(n^2 + n)$ is divisible by 3 since 3 is a factor

Hence, P(n) → P(n + 1)

Example: Sum of 2^n

Using induction…

Show that $2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$ whenever n is a positive integer

Basis: Sum of 2^n

- For our basis, we plug 1 into our expression and get the result
- The result is 1 – which is true

$P(0) = 2^0 = 1 = 2^1 - 1$

Induction: Sum of 2^n

P(n) is written as:

$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$

P(n + 1) is written as:

$2^0 + 2^1 + \ldots + 2^n + 2^{n+1} = 2^{n+2} - 1$

Induction: Sum of 2^n

$2^0 + 2^1 + \ldots + 2^n + 2^{n+1}$

$= (2^0 + 2^1 + \ldots + 2^n) + 2^{n+1}$
$= (2^{n+1} - 1) + 2^{n+1}$
$= 2^{n+1} + 2^{n+1} - 1$
$= 2^n(2^1 + 2^1) - 1$
$= 2^n(2^2) - 1$
$= 2^{n+2} - 1$

P(n) assumed true, so the equality is true

Induction: Sum of 2^n

Since we assumed P(n) is true…

$2^0 + 2^1 + \ldots + 2^n + 2^{n+1}$ is equal to $2^{n+2} - 1$

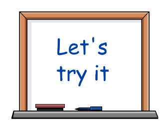
Hence, P(n) → P(n + 1)

Example: Polygons

The sum of the interior angles of a convex polygon with n >= 3 corners is (n-2) * 180 degrees.

Example: Polygons

- Induction is not just useful for mathematical series
- It can also be used to prove concepts like geometry
- For this one, let's draw on the board rather than using slides…



Example Polygons

- Since we can cut each polygon into triangles, we can show the number of points is related to the number of triangles
- In particular, the number of triangles is the number of points - 2

Example: Sum of Integers

Using induction…

Show that the sum of n integers equals n (n+1) / 2

Induction: Sum of Integers

P(n) is written as:

$$1 + 2 + \ldots n = n(n+1) / 2$$

P(n + 1) is written as:

$$1 + 2 + \ldots n + (n+1) = (n+1)(n+2) / 2$$

Induction: Sum of Integers

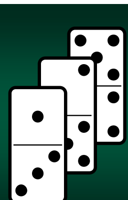
$$1 + 2 + 3 + \ldots n \quad + (n+1)$$

$$= n(n + 1) / 2 \quad + (n+1)$$

$$= (n^2 + n) / 2 \quad + 2(n+1) / 2$$

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

$$= (n + 1)(n + 2) / 2$$

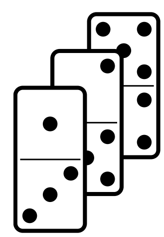


Strong Induction

Another approach

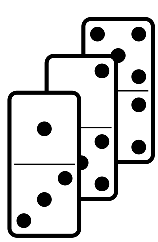
Strong Induction

- *Weak* induction assumes that P(*n*) is true, and then uses that to show P(*n* +1) is true
- *Strong* induction assumes P(1), P(2), …, P(*n*) are all true and then uses that to show that P(*n* +1) is true



Using the Domino Metaphor…

If all the dominos (1 to n) fell over, will it also have knocked over n+1?



Strong Induction

- So, strong induction uses more "dominoes" than weak induction – *which just uses one*
- Both proof techniques are equally valid

$$(P(1) \land P(2) \land \ldots \land P(k)) \rightarrow P(k + 1)$$

Steps to Proof

- Step 1: *Basis*
  - show the proposition P(1) is true
  - very easy to do – just plug in the values
- Step 2: *Induction*
  - assume that P(1), P(2), …, P(*n*) are all true
  - show that P(*n* + 1) is true

Example: Product of Primes

Using strong induction…

Show that any number n >= 2 can be written as the product of primes

Basis: Product of Primes

- For 2, we can show that 2 is a product of two primes
- Namely, 1 and itself

```
P(2) = 1 * 2 = 2
```


Induction: Product of Primes

- There are two cases for n + 1:
- P(n + 1) is prime
- P(n + 1) is composite
  - it can be written as the product of two composites, a and b
  - where 2 ≤ a ≤ b < n + 1

Induction: Product of Primes

```
n + 1 prime:

   it is a product itself and 1

n + 1 is composite:

   both P(a) and P(b) are assumed to be
   true

   so, there exists primes where
   a * b = n + 1
```


Result

- We showed that any number can be either prime or composite of two numbers
- … and that number holds the same
- As a result, we can keep moving backwards to show that everything must be whittled down to primes