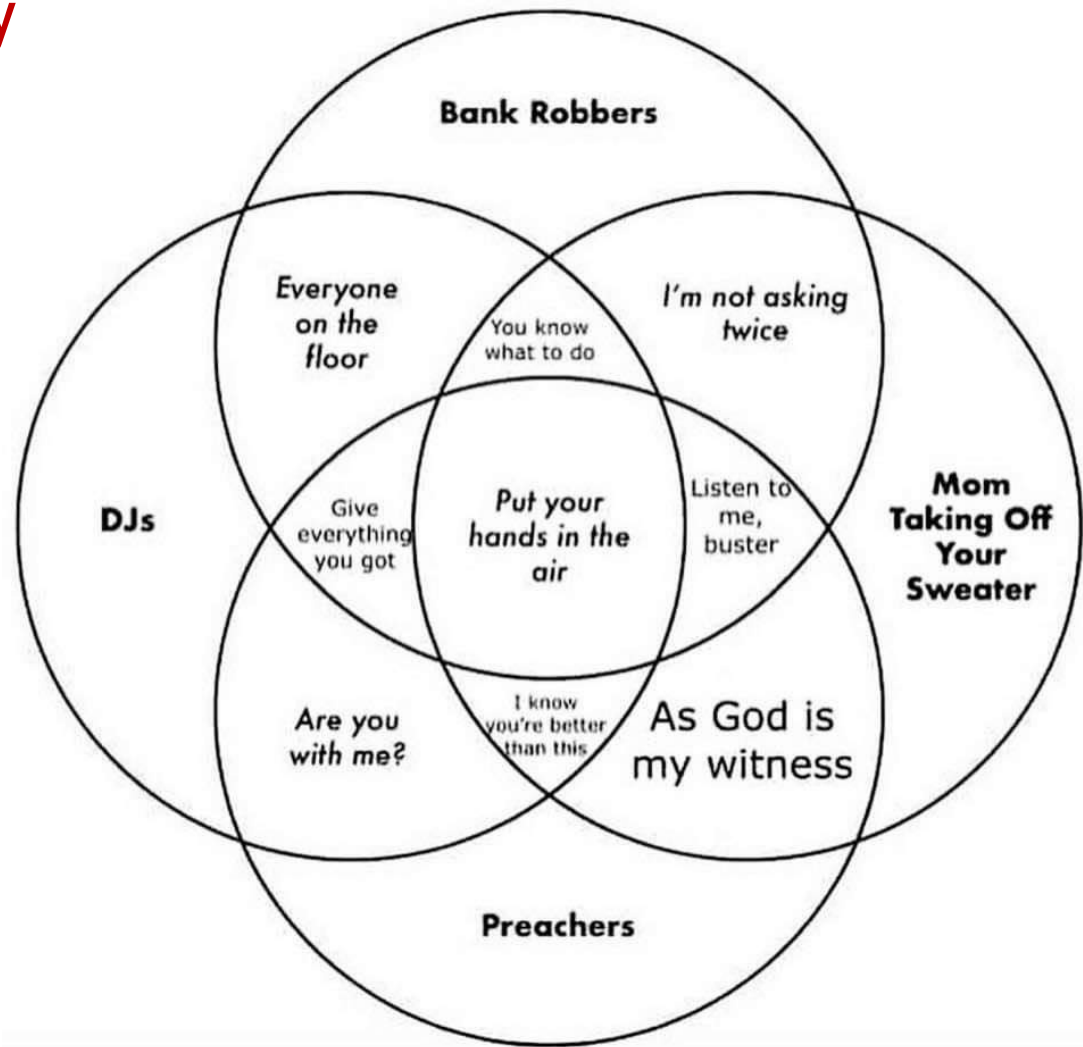


CSE 311: Foundations of Computing

Topic 4: Set Theory



Sets

Sets are collections of objects called **elements**.

Write $a \in B$ to say that a is an element of set B ,
and $a \notin B$ to say that it is not.

Some simple examples

$$A = \{1\}$$

$$B = \{1, 3, 2\}$$

$$C = \{\square, 1\}$$

$$D = \{\{17\}, 17\}$$

$$E = \{1, 2, 7, \text{cat}, \text{dog}, \emptyset, \alpha\}$$

Some Common Sets

\mathbb{N} is the set of **Natural Numbers**; $\mathbb{N} = \{0, 1, 2, \dots\}$

\mathbb{Z} is the set of **Integers**; $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

\mathbb{Q} is the set of **Rational Numbers**; e.g. $\frac{1}{2}$, -17 , $\frac{32}{48}$

\mathbb{R} is the set of **Real Numbers**; e.g. 1 , -17 , $\frac{32}{48}$, π , $\sqrt{2}$

$[n]$ is the set $\{1, 2, \dots, n\}$ when n is a natural number

$\emptyset = \{\}$ is the **empty set**; the *only* set with no elements

Sets can be elements of other sets

For example

$$A = \{\{1\}, \{2\}, \{1,2\}, \emptyset\}$$

$$B = \{1,2\}$$

Then $B \in A$.

Definition: Equality

A and B are *equal* if they have the same elements

$$A = B := \forall x (x \in A \leftrightarrow x \in B)$$

Examples:

- $\{1\} = \{1, 1, 1\}$
- \emptyset is **the** empty set

Definition: Equality

A and B are *equal* if they have the same elements

$$A = B := \forall x (x \in A \leftrightarrow x \in B)$$

$$A = \{1, 2, 3\}$$

$$B = \{3, 4, 5\}$$

$$C = \{3, 4\}$$

$$D = \{4, 3, 3\}$$

$$E = \{3, 4, 3\}$$

$$F = \{4, \{3\}\}$$

Which sets are equal?

Definition: Subset

A* is a *subset* of *B* if every element of *A* is also in *B

$$A \subseteq B := \forall x (x \in A \rightarrow x \in B)$$

$$A = \{1, 2\}$$
$$B = \{1, 2, 3\}$$

$A \subseteq B$ is true
 $B \subseteq A$ is false

Definition: Subset

A* is a *subset* of **B** if every element of *A* is also in **B*

$$A \subseteq B := \forall x (x \in A \rightarrow x \in B)$$

$$A = \{1, 2, 3\}$$

$$B = \{3, 4, 5\}$$

$$C = \{3, 4\}$$

QUESTIONS

$$A \subseteq B?$$

$$C \subseteq B?$$

$$\emptyset \subseteq A?$$

Definitions

- **A and B are *equal* if they have the same elements**

$$A = B := \forall x (x \in A \leftrightarrow x \in B)$$

- **A is a *subset* of B if every element of A is also in B**

$$A \subseteq B := \forall x (x \in A \rightarrow x \in B)$$

- **Notes:** $(A = B) \equiv (A \subseteq B) \wedge (B \subseteq A)$

$$A \supseteq B \text{ means } B \subseteq A$$

$$A \subset B \text{ means } A \subseteq B$$

Sets & Logic

Proofs About Sets

1. $A \subseteq B$

Given

2. $B \subseteq A$

Given

?. $A = B$

??

Proofs About Sets

1. $A \subseteq B$

Given

2. $B \subseteq A$

Given

3. $\forall x (x \in A \rightarrow x \in B)$

Def of Subset: 1

4. $\forall x (x \in B \rightarrow x \in A)$

Def of Subset: 2

?. $A = B$

??

Proofs About Sets

1. $A \subseteq B$

Given

2. $B \subseteq A$

Given

3. $\forall x (x \in A \rightarrow x \in B)$

Def of Subset: 1

4. $\forall x (x \in B \rightarrow x \in A)$

Def of Subset: 2

?. $\forall x (x \in A \leftrightarrow x \in B)$

??

?. $A = B$

Def of Same Set

Proofs About Sets

1. $A \subseteq B$

Given

2. $B \subseteq A$

Given

3. $\forall x (x \in A \rightarrow x \in B)$

Def of Subset: 1

4. $\forall x (x \in B \rightarrow x \in A)$

Def of Subset: 2

Let y be arbitrary.

5.?. $y \in A \leftrightarrow y \in B$

??

5. $\forall x (x \in A \leftrightarrow x \in B)$

Intro \forall

6. $A = B$

Def of Same Set: 5

Proofs About Sets

1. $A \subseteq B$

Given

2. $B \subseteq A$

Given

3. $\forall x (x \in A \rightarrow x \in B)$

Def of Subset: 1

4. $\forall x (x \in B \rightarrow x \in A)$

Def of Subset: 2

Let y be arbitrary.

5.1. $y \in A \rightarrow y \in B$

Elim \forall : 3

5.2. $y \in B \rightarrow y \in A$

Elim \forall : 4

5.?. $y \in A \leftrightarrow y \in B$

??

5. $\forall x (x \in A \leftrightarrow x \in B)$

Intro \forall

6. $A = B$

Def of Same Set: 5

Proofs About Sets

- | | |
|--|---------------------------|
| 1. $A \subseteq B$ | Given |
| 2. $B \subseteq A$ | Given |
| 3. $\forall x (x \in A \rightarrow x \in B)$ | Def of Subset: 1 |
| 4. $\forall x (x \in B \rightarrow x \in A)$ | Def of Subset: 2 |
| Let y be arbitrary. | |
| 5.1. $y \in A \rightarrow y \in B$ | Elim \forall : 3 |
| 5.2. $y \in B \rightarrow y \in A$ | Elim \forall : 4 |
| 5.3. $(y \in A \rightarrow y \in B) \wedge$
$(y \in B \rightarrow y \in A)$ | Intro \wedge : 5.1, 5.2 |
| 5.4. $y \in A \leftrightarrow y \in B$ | Biconditional: 5.3 |
| 5. $\forall x (x \in A \leftrightarrow x \in B)$ | Intro \forall |
| 6. $A = B$ | Def of Same Set: 5 |

Building Sets from Predicates

Every set S defines a predicate $P(x) := "x \in S"$

We can also define a set from a predicate P :

$$S := \{x : P(x)\}$$

S = the set of all x for which $P(x)$ is true

$$S := \{x \in U : P(x)\} = \{x : (x \in U) \wedge P(x)\}$$

Inference Rules on Sets

$$S := \{x : P(x)\}$$

When a set is defined this way,
we can reason about it using its definition:

1. $x \in S$ Given
2. $P(x)$ Def of S
- ...
8. $P(y)$
9. $y \in S$ Def of S

This will be our **only**
inference rule for sets!

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

Suppose we want to prove $A \subseteq B$.

We have a definition of subset:

$$A \subseteq B := \forall x (x \in A \rightarrow x \in B)$$

We need to show that is definition holds

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

9. $A \subseteq B$

??

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

8. $\forall x (x \in A \rightarrow x \in B)$

9. $A \subseteq B$

??

Def of Subset: 8

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

Let x be arbitrary

1.1. $x \in A \rightarrow x \in B$

1. $\forall x (x \in A \rightarrow x \in B)$

2. $A \subseteq B$

??

Intro \forall : **1**

Def of Subset: **2**

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

Let x be arbitrary

1.1.1. $x \in A$

Assumption

1.1.?. $x \in B$

??

1.1. $x \in A \rightarrow x \in B$

Direct Proof

1. $\forall x (x \in A \rightarrow x \in B)$

Intro \forall : 1

2. $A \subseteq B$

Def of Subset: 2

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

Let x be arbitrary

1.1.1. $x \in A$

1.1.2. $P(x)$

1.1.?. $Q(x)$

1.1.?. $x \in B$

1.1. $x \in A \rightarrow x \in B$

1. $\forall x (x \in A \rightarrow x \in B)$

2. $A \subseteq B$

Assumption

Def of A

??

Def of B

Direct Proof

Intro \forall : 1

Def of Subset: 2

Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

Prove that $A \subseteq B$.

Proof: Let x be an arbitrary object.

Suppose that $x \in A$. By definition of A , this means $P(x)$.

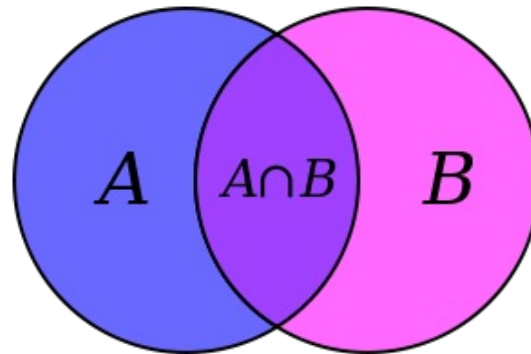
...

Thus, we have $Q(x)$. By definition of B , this means $x \in B$.

Since x was arbitrary, we have shown, by definition of subset, that $A \subseteq B$.

English *template* for a Subset Proof

Operations on Sets



Set Operations

$$A \cup B := \{ x : (x \in A) \vee (x \in B) \}$$

Union

$$A \cap B := \{ x : (x \in A) \wedge (x \in B) \}$$

Intersection

$$A \setminus B := \{ x : (x \in A) \wedge (x \notin B) \}$$

Set Difference

$$A = \{1, 2, 3\}$$

$$B = \{3, 5, 6\}$$

$$C = \{3, 4\}$$

QUESTIONS

Using A, B, C and set operations, make...

$$\{6\} =$$

$$\{3\} =$$

$$\{1,2\} =$$

More Set Operations

$$A \oplus B := \{x : (x \in A) \oplus (x \in B)\}$$

**Symmetric
Difference**

$$\bar{A} = A^C := \{x : x \in U \wedge x \notin A\}$$

(with respect to universe U)

Complement

$$A = \{1, 2, 3\}$$

$$B = \{1, 2, 4, 6\}$$

Universe:

$$U = \{1, 2, 3, 4, 5, 6\}$$

$$A \oplus B = \{3, 4, 6\}$$

$$\bar{A} = \{4, 5, 6\}$$

Note that $A \cup \bar{A} = U$

De Morgan's Laws

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

De Morgan's Laws

Prove that $(A \cup B)^c = A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \leftrightarrow x \in A^c \cap B^c)$

Equivalently, prove $(A \cup B)^c \subseteq A^c \cap B^c$ and
 $A^c \cap B^c \subseteq (A \cup B)^c$

Recall: Proofs About Sets

$$A := \{x : P(x)\}$$

$$B := \{x : Q(x)\}$$

Prove that $A \subseteq B$.

Proof: Let x be an arbitrary object.

Suppose that $x \in A$. By definition of A , this means $P(x)$.

...

Thus, we have $Q(x)$. By definition of B , this means $x \in B$.

Since x was arbitrary, we have shown, by definition of subset, that $A \subseteq B$.

De Morgan's Laws

Prove that $(A \cup B)^c \subseteq A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c)$

Proof: Let x be an arbitrary object.

Suppose that $x \in (A \cup B)^c$. By the definition of ...

By the definition of ..., this means $x \in A^c \cap B^c$.

Since x was arbitrary, we have shown, by the definition of subset, that $(A \cup B)^c \subseteq A^c \cap B^c$.

De Morgan's Laws

Prove that $(A \cup B)^c \subseteq A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c)$

Proof: Let x be an arbitrary object.

Suppose that $x \in (A \cup B)^c$. By the definition of complement, we have $\neg(x \in A \cup B)$.

By the definition of ..., this means $x \in A^c \cap B^c$.

Since x was arbitrary, we have shown, by the definition of subset, that $(A \cup B)^c \subseteq A^c \cap B^c$.

De Morgan's Laws

Prove that $(A \cup B)^c \subseteq A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c)$

Proof: Let x be an arbitrary object.

Suppose that $x \in (A \cup B)^c$. By the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$.

...

By the definition of ..., this means $x \in A^c \cap B^c$.

Since x was arbitrary, we have shown, by the definition of subset, that $(A \cup B)^c \subseteq A^c \cap B^c$.

De Morgan's Laws

Prove that $(A \cup B)^c \subseteq A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c)$

Proof: Let x be an arbitrary object.

Suppose that $x \in (A \cup B)^c$. By the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$.

...

Thus, $x \in A^c$ and $x \in B^c$. By the definition of intersection, this means $x \in A^c \cap B^c$.

Since x was arbitrary, we have shown, by the definition of subset, that $(A \cup B)^c \subseteq A^c \cap B^c$.

De Morgan's Laws

Prove that $(A \cup B)^c \subseteq A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c)$

Proof: Let x be an arbitrary object.

Suppose that $x \in (A \cup B)^c$. By the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$.

...

So $\neg(x \in A)$ and $\neg(x \in B)$. Thus, $x \in A^c$ and $x \in B^c$ by the definition of complement. By the definition of intersection, this means $x \in A^c \cap B^c$.

Since x was arbitrary, we have shown, by the definition of subset, that $(A \cup B)^c \subseteq A^c \cap B^c$.

De Morgan's Laws

Prove that $(A \cup B)^c \subseteq A^c \cap B^c$

Formally, prove $\forall x (x \in (A \cup B)^c \rightarrow x \in A^c \cap B^c)$

Proof: Let x be an arbitrary object.

Suppose that $x \in (A \cup B)^c$. By the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$, or equivalently, $\neg(x \in A) \wedge \neg(x \in B)$ by De Morgan's law. Thus, $x \in A^c$ and $x \in B^c$ by the definition of complement. By the definition of intersection, this means $x \in A^c \cap B^c$.

Since x was arbitrary, we have shown, by the definition of subset, that $(A \cup B)^c \subseteq A^c \cap B^c$.

De Morgan's Laws

Prove that $A^C \cap B^C \subseteq (A \cup B)^C$

Formally, prove $\forall x (x \in A^C \cap B^C \rightarrow x \in (A \cup B)^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in A^C \cap B^C$. Then, by the definition of intersection, we have $x \in A^C$ and $x \in B^C$. That is, we have $\neg(x \in A) \wedge \neg(x \in B)$, which is equivalent to $\neg(x \in A \vee x \in B)$ by De Morgan's law. The last is equivalent to $\neg(x \in A \cup B)$, by the definition of union, so we have shown $x \in (A \cup B)^C$, by the definition of complement.

Since x was arbitrary, we have shown, by the definition of subset, that $A^C \cap B^C \subseteq (A \cup B)^C$.

Proofs About Set Equality

A lot of *repetitive* work to show \rightarrow and \leftarrow .

Suppose $x \in (A \cup B)^c$.

Then, by the definition of complement, we have $\neg(x \in A \cup B)$.

The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$,

or equivalently, $\neg(x \in A) \wedge \neg(x \in B)$ by De Morgan's law.

Thus, we have $x \in A^c$ and $x \in B^c$ by the definition of complement, and we can see that $x \in A^c \cap B^c$ by the definition of intersection.

Suppose $x \in A^c \cap B^c$.

Then, by the definition of intersection, we have $x \in A^c$ and $x \in B^c$.

We then have $\neg(x \in A) \wedge \neg(x \in B)$ by the definition of complement.

which is equivalent to $\neg(x \in A \vee x \in B)$ by De Morgan's law.

The last is equivalent to $\neg(x \in A \cup B)$, by the definition of union,

so we have shown $x \in (A \cup B)^c$, by the definition of complement.

Proofs About Set Equality

A lot of *repetitive* work to show \rightarrow and \leftarrow .

Suppose $x \in (A \cup B)^c$.

Then, by the definition of **complement**, we have $\neg(x \in A \cup B)$.

The latter says, by the definition of **union**, that $\neg(x \in A \vee x \in B)$,

or equivalently, $\neg(x \in A) \wedge \neg(x \in B)$ by **De Morgan's law**.

Thus, we have $x \in A^c$ and $x \in B^c$ by the definition of **complement**,

and we can see that $x \in A^c \cap B^c$ by the definition of **intersection**.

Suppose $x \in A^c \cap B^c$.

Then, by the definition of **intersection**, we have $x \in A^c$ and $x \in B^c$.

We then have $\neg(x \in A) \wedge \neg(x \in B)$ by the definition of **complement**.

which is equivalent to $\neg(x \in A \vee x \in B)$ by **De Morgan's law**.

The last is equivalent to $\neg(x \in A \cup B)$, by the definition of **union**,

so we have shown $x \in (A \cup B)^c$, by the definition of **complement**.

Proofs About Set Equality

A lot of *repetitive* work to show \rightarrow and \leftarrow .

Do we have a way to prove \leftrightarrow directly?

Recall that $A \equiv B$ and $(A \leftrightarrow B) \equiv T$ are the same

We can use an equivalence chain to prove that a biconditional holds.

De Morgan's Law

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

The stated biconditional holds since:

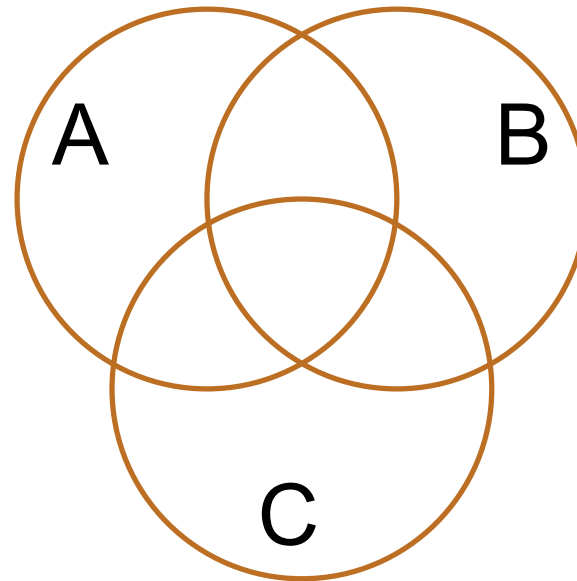
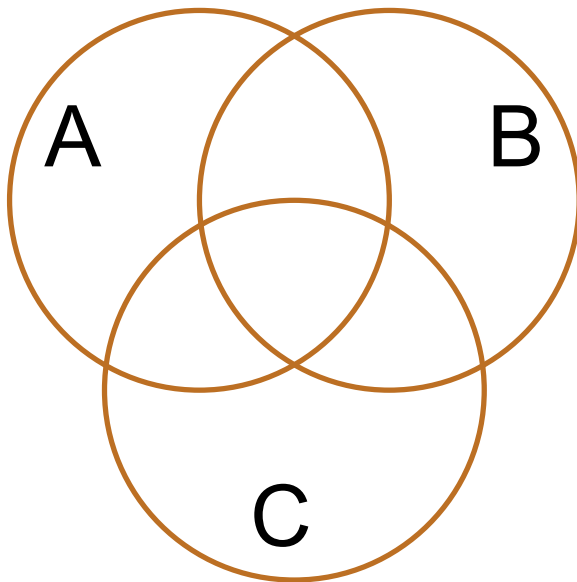
$x \in (A \cup B)^C$	$\equiv \neg(x \in A \cup B)$	Def of Comp
	$\equiv \neg(x \in A \vee x \in B)$	Def of Union
	$\equiv \neg(x \in A) \wedge \neg(x \in B)$	De Morgan
	$\equiv x \in A^C \wedge x \in B^C$	Def of Comp
	$\equiv x \in A^C \cap B^C$	Def of Intersection

Calculation blocks
are often easier to
read like this rather
than as English text

Since x was arbitrary, we have shown, by definition, that the sets are equal. ■

Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



Distributive Law

Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof: Let x be an arbitrary object.

The stated biconditional holds since:

$$\begin{aligned}x \in A \cap (B \cup C) & \\ \equiv (x \in A) \wedge (x \in B \cup C) & \quad \text{Def of Intersection} \\ \equiv (x \in A) \wedge ((x \in B) \vee (x \in C)) & \quad \text{Def of Union} \\ \equiv ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C)) & \quad \text{Distributive} \\ \equiv (x \in A \cap B) \vee (x \in A \cap C) & \quad \text{Def of Intersection} \\ \equiv x \in (A \cap B) \cup (A \cap C) & \quad \text{Def of Union}\end{aligned}$$

Since x was arbitrary, we have shown, by definition, that the sets are equal. ■

The Meta Theorem

Meta-Theorem: Translate any Propositional Logic equivalence into “=” relationship between sets by replacing \cup with \cap , \cap with \cup , and \cdot^c with \neg .

Example: $\neg(A \vee B) \equiv \neg A \wedge \neg B$ becomes

$$(A \cup B)^c = A^c \cap B^c$$

Example: $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ becomes

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

The Meta Theorem Proof Template

Meta-Theorem: Translate any Propositional Logic equivalence into “=” relationship between sets by replacing \cup with \vee , \cap with \wedge , and \cdot^c with \neg .

“Proof”: Let x be an arbitrary object.

The stated bi-condition holds since:

$x \in \text{left side}$ \equiv replace set ops with propositional logic
 \equiv apply Propositional Logic equivalence
 \equiv replace propositional logic with set ops
 $\equiv x \in \text{right side}$

Since x was arbitrary, we have shown, by definition, that the sets are equal. ■

Power Set

- Power Set of a set A = set of all subsets of A

$$\mathcal{P}(A) := \{B : B \subseteq A\}$$

- e.g., let $\text{Days} = \{M, W, F\}$ and consider all the possible sets of days in a week you could ask a question in class

$$\mathcal{P}(\text{Days}) = ?$$

Power Set

- Power Set of a set A = set of all subsets of A

$$\mathcal{P}(A) := \{B : B \subseteq A\}$$

- e.g., let $\text{Days} = \{M, W, F\}$ and consider all the possible sets of days in a week you could ask a question in class

$$\mathcal{P}(\text{Days}) = \{\{M, W, F\}, \{M, W\}, \{M, F\}, \{W, F\}, \{M\}, \{W\}, \{F\}, \emptyset\}$$

$$\mathcal{P}(\emptyset) = ?$$

Power Set

- Power Set of a set A = set of all subsets of A

$$\mathcal{P}(A) := \{B : B \subseteq A\}$$

- e.g., let $\text{Days} = \{M, W, F\}$ and consider all the possible sets of days in a week you could ask a question in class

$$\mathcal{P}(\text{Days}) = \{\{M, W, F\}, \{M, W\}, \{M, F\}, \{W, F\}, \{M\}, \{W\}, \{F\}, \emptyset\}$$

$$\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$$

Cartesian Product

$$A \times B := \{x : \exists a \exists b ((a \in A) \wedge (b \in B) \wedge (x = (a, b))) \}$$

- $\mathbb{R} \times \mathbb{R}$ is the real plane.
 - you've seen ordered pairs before... these are just for arbitrary sets.
- $\mathbb{Z} \times \mathbb{Z}$ is “the set of all pairs of integers”

If $A = \{1, 2\}$, $B = \{a, b, c\}$, then $A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$.

Cartesian Product

$$A \times B := \{x : \exists a \exists b ((a \in A) \wedge (b \in B) \wedge (x = (a, b)))\}$$

- $\mathbb{R} \times \mathbb{R}$ is the real plane.
 - you've seen ordered pairs before... these are just for arbitrary sets.
- $\mathbb{Z} \times \mathbb{Z}$ is “the set of all pairs of integers”

If $A = \{1, 2\}$, $B = \{a, b, c\}$, then $A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$.

What is $A \times \emptyset$?

Cartesian Product

$$A \times B := \{x : \exists a \exists b ((a \in A) \wedge (b \in B) \wedge (x = (a, b)))\}$$

- $\mathbb{R} \times \mathbb{R}$ is the real plane.
 - you've seen ordered pairs before... these are just for arbitrary sets.
- $\mathbb{Z} \times \mathbb{Z}$ is “the set of all pairs of integers”

If $A = \{1, 2\}$, $B = \{a, b, c\}$, then $A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$.

$$\begin{aligned} A \times \emptyset &= \{x : \exists a \exists b (a \in A \wedge b \in \emptyset \wedge x = (a, b))\} \\ &= \{x : \exists a \exists b (a \in A \wedge \mathbf{F} \wedge x = (a, b))\} \\ &= \{x : \mathbf{F}\} = \emptyset \end{aligned}$$

More Set Builder Notation

$$A \times B := \{x : \exists a \exists b ((a \in A) \wedge (b \in B) \wedge (x = (a, b))) \}$$

- This can be written more concisely as follows...

$$A \times B := \{(a, b) : a \in A, b \in B \}$$

- within set builder variables are implicitly \exists -quantified

this is the one exception to the rule that
unbound variables are implicitly \forall -quantified

Another Expression on the Left Side

- The set of all squares can be defined as

$$S := \{ n^2 : n \in \mathbb{Z} \}$$

- Formally, this is the set of all x such that $x = n^2$ for some $n \in \mathbb{Z}$.
- Informally, go through all $n \in \mathbb{Z}$, and for each of them, add n^2 to the set.
 - can think of this as a "map" operation

More Set Builder Notation

$$S := \{ x \in U : P(x) \}$$

"filter"

- Then $x \in S$ tells us that $P(x)$ holds

$$T := \{ f(x) : x \in U \}$$

"map"

- Then $y \in T$ tells us that $y = f(x)$ for **some** $x \in U$

More Set Builder Notation

- Both notations can be used together, e.g.

$$V := \{ f(x) : x \in U \wedge P(x) \}$$

- Then $y \in V$ tells us that $y = f(x)$ for **some** x such that $P(x)$ holds

these two notations can be thought of as "filter" and "map"
they are widely used operations in programming as well

Russell's Paradox

$$S := \{x : x \notin x\}$$

Suppose that $S \in S$...

Russell's Paradox

$$S := \{x : x \notin x\}$$

Suppose that $S \in S$. Then, by the definition of S , $S \notin S$, but that's a contradiction.

Suppose that $S \notin S$. Then, by the definition of S , $S \in S$, but that's a contradiction too.

Since one of these must hold, we have proven F in general.

Uh... that's not good.

Recall: Formal Proofs

- In principle, formal proofs are the standard for what it means to be “proven” in mathematics
 - almost all math (and theory CS) done in Predicate Logic
- But they can be tedious and impractical
 - e.g., applications of commutativity and associativity
 - Russell & Whitehead’s formal proof that $1+1 = 2$ is *several hundred pages long*
 - we allow ourselves to cite “Arithmetic”, “Algebra”, etc.

Domain-Restriction to Sets

Often want to prove facts about all elements of a set

$$\forall x (x \in A \rightarrow P(x))$$

Note the domain restriction.

We will use a shorthand restriction to a set

$$\forall x \in A (P(x)) \quad \text{means} \quad \forall x (x \in A \rightarrow P(x))$$

Restricting set-restricted variables improves *clarity*

Sets of Numbers

- Define some familiar sets of numbers

$$\mathbb{E} = \{n \in \mathbb{Z} \mid \exists k (n = 2k)\}$$

$$\mathbb{O} = \{n \in \mathbb{Z} \mid \exists k (n = 2k + 1)\}$$

- previously, we defined these as predicates

Recall: Even and Odd

Prove “The square of every even integer is even.”

Formally, prove $\forall x (\text{Even}(x) \rightarrow \text{Even}(x^2))$

Proof: Let **a** be an arbitrary integer.

Suppose **a** is even. Then, by definition, $\mathbf{a = 2b}$ for some integer **b**. Squaring both sides, we get $\mathbf{a^2 = 4b^2 = 2(2b^2)}$. So $\mathbf{a^2}$ is, by definition, is even.

Since **a** was arbitrary, we have shown that the square of every even number is even. ■

Even and Odd As Sets

Prove “The square of every even integer is even.”

Formally, prove $\forall x \in \mathbb{E} (x^2 \in \mathbb{E})$

Proof: Let **a** be an arbitrary **even** integer.

~~Suppose **a** is even.~~ Then, by definition, **a** = **2b** for some integer **b**. Squaring both sides, we get **a**² = **4b**² = **2(2b**²). So **a**² is, by definition, is even.

Since **a** was arbitrary, we have shown that the square of every even number is even. ■

The structure of the proof *follows* the structure of the claim.

Recall: Even and Odd

Prove “The sum of any two odd numbers is even.”

Formally, prove $\forall x \forall y ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Proof: Let x and y be arbitrary integers.

Suppose that both are odd. Then, we have $x = 2a+1$ for some integer a and $y = 2b+1$ for some integer b . Their sum is $x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1)$, so $x+y$ is, by definition, even.

Since x and y were arbitrary, the sum of any two odd integers is even. ■

Recall: Even and Odd

Prove “The sum of any two odd numbers is even.”

Formally, prove $\forall x \in \mathbb{O}, \forall y \in \mathbb{O} (x + y \in \mathbb{E})$

Proof: Let x and y be arbitrary **odd** integers.

~~Suppose that both are odd.~~ Then, we have $x = 2a+1$ for some integer a and $y = 2b+1$ for some integer b . Their sum is $x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1)$, so $x+y$ is, by definition, even.

Since x and y were arbitrary, the sum of any two odd integers is even. ■

Another Odd One

“The square of the sum of any even and odd is congruent to 1 mod 4”

Formally, prove $\forall x \in \mathbb{E}, \forall y \in \mathbb{O} ((x + y)^2 \equiv_4 1)$

Proof:

Let x be an arbitrary **even** and y an arbitrary **odd**.

Since x is even and y is odd, we have $x = 2j$ for some integer j , and $y = 2k + 1$ for some integer k . We can now see that

$$\begin{aligned}(x+y)^2 &= (2j + 2k+1)^2 \\ &= (2(j+k) + 1)^2 \\ &= 4(j+k)^2 + 4(j+k) + 1\end{aligned}$$

This shows that $4 \mid (x+y)^2 - 1$ by definition of divides, which means that $(x+y)^2 \equiv_4 1$ by definition of congruent.

Since x and y were arbitrary, we have proven the claim. ■

Recall: Recursive definitions of functions

- $0! = 1$; $(n + 1)! = (n + 1) \cdot n!$ for all $n \geq 0$.
- $F(0) = 0$; $F(n + 1) = F(n) - 1$ for all $n \geq 0$.
- $G(0) = 1$; $G(n + 1) = 2 \cdot G(n)$ for all $n \geq 0$.
- $H(0) = 1$; $H(n + 1) = 2^{H(n)}$ for all $n \geq 0$.

Recursive Definitions of Sets

Recursive Definitions of Sets (Data)

Natural numbers

Basis: $0 \in S$

Recursive: If $x \in S$, then $x+1 \in S$

Even numbers

Basis: $0 \in S$

Recursive: If $x \in S$, then $x+2 \in S$

In comparison to earlier definitions:

- $\mathbb{N} := \{x \in \mathbb{Z} \mid x \geq 0\}$
- $\mathbb{E} := \{x \in \mathbb{N} \mid \exists k (x = 2k)\}$

these definitions are constructive.

Recursive Definitions of Sets

Recursive definition of set S

- **Basis Step:** $0 \in S$
- **Recursive Step:** If $x \in S$, then $x + 2 \in S$

The only elements in S are those that follow from the basis step and a finite number of recursive steps

Recursive Definitions of Sets

Natural numbers

Basis: $0 \in S$

Recursive: If $x \in S$, then $x+1 \in S$

Even numbers

Basis: $0 \in S$

Recursive: If $x \in S$, then $x+2 \in S$

Powers of 3:

Basis: $1 \in S$

Recursive: If $x \in S$, then $3x \in S$.

Basis: $(0, 0) \in S, (1, 1) \in S$

Recursive: If $(n-1, x) \in S$ and $(n, y) \in S$,
then $(n+1, x + y) \in S$. ?

Recursive Definitions of Sets

Natural numbers

Basis: $0 \in S$

Recursive: If $x \in S$, then $x+1 \in S$

Even numbers

Basis: $0 \in S$

Recursive: If $x \in S$, then $x+2 \in S$

Powers of 3:

Basis: $1 \in S$

Recursive: If $x \in S$, then $3x \in S$.

Basis: $(0, 0) \in S, (1, 1) \in S$

Recursive: If $(n-1, x) \in S$ and $(n, y) \in S$, then $(n+1, x + y) \in S$.

Fibonacci numbers

Recall: Recursive definitions of functions

- **Before, we considered only simple data**
 - inputs and outputs were just integers
- **Proved facts about those functions with induction**
 - $n! \leq n^n$
 - $f_n < 2^n$ and $f_n \geq 2^{n/2-1}$
- **How do we prove facts about functions that work with more complex (recursively defined) data?**
 - we need a more sophisticated form of induction

Structural Induction

How to prove $\forall x \in S, P(x)$ is true:

Base Case: Show that $P(u)$ is true for all **specific elements** u of S mentioned in the *Basis step*

Inductive Hypothesis: Assume that P is true for some arbitrary values of each of the **existing named elements** mentioned in the *Recursive step*

Inductive Step: Prove that $P(w)$ holds for each of the **new elements** w constructed in the *Recursive step* using the named elements mentioned in the Inductive Hypothesis

Conclude that $\forall x \in S, P(x)$

Structural Induction

Basis: $0 \in S$
Recursive: If $x \in S$, then $x+2 \in S$

How to prove $\forall x \in S, P(x)$ is true:

Base Case: Show that $P(u)$ is true for all **specific elements u** of S mentioned in the *Basis step*

Inductive Hypothesis: Assume that P is true for some arbitrary values of each of the **existing named elements** mentioned in the *Recursive step*

Inductive Step: Prove that $P(w)$ holds for each of the **new elements w** constructed in the *Recursive step* using the named elements mentioned in the Inductive Hypothesis

Conclude that $\forall x \in S, P(x)$

Structural Induction vs. Ordinary Induction

Ordinary induction is a special case of structural induction:

Recursive definition of \mathbb{N}

Basis: $0 \in \mathbb{N}$

Recursive step: If $k \in \mathbb{N}$ then $k + 1 \in \mathbb{N}$

Structural induction follows from ordinary induction:

Define $Q(n)$ to be “for all $x \in S$ that can be constructed in at most n recursive steps, $P(x)$ is true.”

Using Structural Induction

- Let S be given by...
 - **Basis:** $6 \in S$; $15 \in S$
 - **Recursive:** if $x, y \in S$ then $x + y \in S$.

Claim: Every element of S is divisible by 3.

Formally, $\forall x \in S (3 \mid x)$

Claim: Every element of S is divisible by 3.

1. Let $P(x)$ be “ $3 \mid x$ ”. We prove that $P(x)$ is true for all $x \in S$ by structural induction.

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$, then $x + y \in S$

Claim: Every element of S is divisible by 3.

1. Let $P(x)$ be " $3 \mid x$ ". We prove that $P(x)$ is true for all $x \in S$ by structural induction.
2. Base Case: $3 \mid 6$ and $3 \mid 15$ so $P(6)$ and $P(15)$ are true

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$, then $x + y \in S$

Claim: Every element of S is divisible by 3.

1. Let $P(x)$ be " $3 \mid x$ ". We prove that $P(x)$ is true for all $x \in S$ by structural induction.
2. Base Case: $3 \mid 6$ and $3 \mid 15$ so $P(6)$ and $P(15)$ are true
3. Inductive Hypothesis: Suppose that $P(x)$ and $P(y)$ are true for some arbitrary $x, y \in S$
4. Inductive Step:

Goal: $P(x+y)$, i.e., $3 \mid x+y$

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$, then $x + y \in S$

Claim: Every element of S is divisible by 3.

1. Let $P(x)$ be " $3 \mid x$ ". We prove that $P(x)$ is true for all $x \in S$ by structural induction.
2. Base Case: $3 \mid 6$ and $3 \mid 15$ so $P(6)$ and $P(15)$ are true
3. Inductive Hypothesis: Suppose that $P(x)$ and $P(y)$ are true for some arbitrary $x, y \in S$

4. Inductive Step:

Since $P(x)$ is true, $3 \mid x$ and so $x=3m$ for some integer m and since $P(y)$ is true, $3 \mid y$ and so $y=3n$ for some integer n .

Therefore $x+y=3m+3n=3(m+n)$ and thus $3 \mid (x+y)$.

Hence $P(x+y)$ is true.

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$, then $x + y \in S$

Claim: Every element of S is divisible by 3.

1. Let $P(x)$ be " $3 \mid x$ ". We prove that $P(x)$ is true for all $x \in S$ by structural induction.

2. Base Case: $3 \mid 6$ and $3 \mid 15$ so $P(6)$ and $P(15)$ are true

3. Inductive Hypothesis: Suppose that $P(x)$ and $P(y)$ are true for some arbitrary $x, y \in S$

4. Inductive Step:

Since $P(x)$ is true, $3 \mid x$ and so $x=3m$ for some integer m and since $P(y)$ is true, $3 \mid y$ and so $y=3n$ for some integer n .

Therefore $x+y=3m+3n=3(m+n)$ and thus $3 \mid (x+y)$.

Hence $P(x+y)$ is true.

5. Therefore, by induction, $3 \mid x$ for all $x \in S$.

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$, then $x + y \in S$

Using Structural Induction

- Let T be given by...
 - **Basis:** $6 \in T$; $15 \in T$
 - **Recursive:** if $x \in T$, then $x + 6 \in T$ and $x + 15 \in T$
- Now, two base cases and two *recursive* cases

Claim: Every element of T is also in S .

Formally, $\forall x \in T (x \in S)$

Claim: Every element of T is an element of S

1. Let $P(x)$ be " $x \in S$ ". We prove that $P(x)$ is true for all $x \in T$ by structural induction.

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$,
then $x + y \in S$

Basis: $6 \in T$; $15 \in T$

Recursive: if $x \in T$, then $x + 6 \in T$
and $x + 15 \in T$

Claim: Every element of T is an element of S

1. Let $P(x)$ be " $x \in S$ ". We prove that $P(x)$ is true for all $x \in T$ by structural induction.
2. Base Case: $6 \in S$ and $15 \in S$ so $P(6)$ and $P(15)$ are true

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$,
then $x + y \in S$

Basis: $6 \in T$; $15 \in T$

Recursive: if $x \in T$, then $x + 6 \in T$
and $x + 15 \in T$

Claim: Every element of T is an element of S

1. Let $P(x)$ be " $x \in S$ ". We prove that $P(x)$ is true for all $x \in T$ by structural induction.
2. Base Case: $6 \in S$ and $15 \in S$ so $P(6)$ and $P(15)$ are true
3. Inductive Hypothesis: Suppose that $P(x)$ is true for some arbitrary $x \in T$

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$,
then $x + y \in S$

Basis: $6 \in T$; $15 \in T$

Recursive: if $x \in T$, then $x + 6 \in T$
and $x + 15 \in T$

Claim: Every element of T is an element of S

1. Let $P(x)$ be " $x \in S$ ". We prove that $P(x)$ is true for all $x \in T$ by structural induction.
2. Base Case: $6 \in S$ and $15 \in S$ so $P(6)$ and $P(15)$ are true
3. Inductive Hypothesis: Suppose that $P(x)$ is true for some arbitrary $x \in T$
4. Inductive Step: **Goal: Show $P(x+6)$ and $P(x+15)$**

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$,
then $x + y \in S$

Basis: $6 \in T$; $15 \in T$

Recursive: if $x \in T$, then $x + 6 \in T$
and $x + 15 \in T$

Claim: Every element of T is an element of S

1. Let $P(x)$ be “ $x \in S$ ”. We prove that $P(x)$ is true for all $x \in T$ by structural induction.

2. Base Case: $6 \in S$ and $15 \in S$ so $P(6)$ and $P(15)$ are true

3. Inductive Hypothesis: Suppose that $P(x)$ is true for some arbitrary $x \in T$

4. Inductive Step:

Since $P(x)$ holds, we have $x \in S$. From the recursive step of S , since $6 \in S$, we can see that $x + 6 \in S$, so $P(x+6)$ is true, and since $15 \in S$, we can see that $x + 15 \in S$, so $P(x+15)$ is true.

Basis: $6 \in S$; $15 \in S$

Recursive: if $x, y \in S$,
then $x + y \in S$

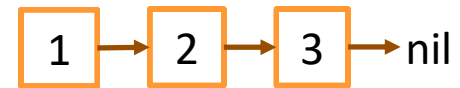
Basis: $6 \in T$; $15 \in T$

Recursive: if $x \in T$, then $x + 6 \in T$
and $x + 15 \in T$

Claim: Every element of T is an element of S

1. Let $P(x)$ be “ $x \in S$ ”. We prove that $P(x)$ is true for all $x \in T$ by structural induction.
2. Base Case: $6 \in S$ and $15 \in S$ so $P(6)$ and $P(15)$ are true
3. Inductive Hypothesis: Suppose that $P(x)$ is true for some arbitrary $x \in T$
4. Inductive Step:
Since $P(x)$ holds, we have $x \in S$. From the recursive step of S , since $6 \in S$, we can see that $x + 6 \in S$, so $P(x+6)$ is true, and since $15 \in S$, we can see that $x + 15 \in S$, so $P(x+15)$ is true.
5. Therefore $P(x)$ for all $x \in T$ by induction.

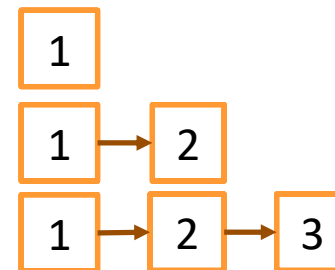
Lists of Integers



- **Basis:** $\text{nil} \in \text{List}$
- **Recursive step:**
if $L \in \text{List}$ and $a \in \mathbb{Z}$,
then $a :: L \in \text{List}$

Examples:

- nil
- $1 :: \text{nil}$
- $1 :: 2 :: \text{nil}$
- $1 :: 2 :: 3 :: \text{nil}$



Functions on Lists

Length:

$$\text{len}(\text{nil}) := 0$$

$$\text{len}(a :: L) := \text{len}(L) + 1 \quad \text{for any } L \in \mathbf{List} \text{ and } a \in \mathbb{Z}$$

Concatenation:

$$\text{concat}(\text{nil}, R) := R \quad \text{for any } R \in \mathbf{List}$$

$$\text{concat}(a :: L, R) := a :: \text{concat}(L, R) \quad \text{for any } L, R \in \mathbf{List} \text{ and any } a \in \mathbb{Z}$$

Structural Induction

How to prove $\forall x \in S, P(x)$ is true:

Basis: $\text{nil} \in \text{List}$

Recursive step:

if $L \in \text{List}$ and $a \in \mathbb{Z}$,
then $a :: L \in \text{List}$

Base Case: Show that $P(u)$ is true for all **specific elements u** of S mentioned in the *Basis step*

Inductive Hypothesis: Assume that P is true for some arbitrary values of each of the **existing named elements** mentioned in the *Recursive step*

Inductive Step: Prove that $P(w)$ holds for each of the **new elements w** constructed in the *Recursive step* using the named elements mentioned in the Inductive Hypothesis

Conclude that $\forall x \in S, P(x)$

Claim: $\text{concat}(S, \text{nil}) = S$ for all $S \in \text{List}$

Claim: $\text{concat}(S, \text{nil}) = S$ for all $L \in \text{List}$

Let $P(S)$ be “ $\text{concat}(S, \text{nil}) = S$ ” .

We will prove $P(S)$ for all $S \in \text{List}$ by structural induction.

Concatenation:

$\text{concat}(\text{nil}, R) := R$

$\text{concat}(a :: L, R) := a :: \text{concat}(L, R)$

Claim: $\text{concat}(S, \text{nil}) = S$ for all $L \in \text{List}$

Let $P(S)$ be “ $\text{concat}(S, \text{nil}) = S$ ” .

We will prove $P(S)$ for all $S \in \text{List}$ by structural induction.

Base Case (nil): By the definition of concat , we can see that $\text{concat}(\text{nil}, \text{nil}) = \text{nil}$, which is $P(\text{nil})$.

Claim: $\text{concat}(S, \text{nil}) = S$ for all $L \in \text{List}$

Let $P(S)$ be “ $\text{concat}(S, \text{nil}) = S$ ” .

We will prove $P(S)$ for all $S \in \text{List}$ by structural induction.

Base Case (nil): By the definition of concat , we can see that $\text{concat}(\text{nil}, \text{nil}) = \text{nil}$, which is $P(\text{nil})$.

Inductive Hypothesis: Assume that $P(L)$ is true for some arbitrary $L \in \text{List}$, i.e., $\text{concat}(L, \text{nil}) = L$.

Inductive Step:

Concatenation:

$\text{concat}(\text{nil}, R) := R$

$\text{concat}(a :: L, R) := a :: \text{concat}(L, R)$

Goal: For any $a \in \mathbb{Z}$, show $P(a :: L)$, i.e., $\text{concat}(a :: L, \text{nil}) = a :: L$

Claim: $\text{concat}(S, \text{nil}) = S$ for all $L \in \text{List}$

Let $P(S)$ be “ $\text{concat}(S, \text{nil}) = S$ ” .

We will prove $P(S)$ for all $S \in \text{List}$ by structural induction.

Base Case (nil): By the definition of concat , we can see that $\text{concat}(\text{nil}, \text{nil}) = \text{nil}$, which is $P(\text{nil})$.

Inductive Hypothesis: Assume that $P(L)$ is true for some arbitrary $L \in \text{List}$, i.e., $\text{concat}(L, \text{nil}) = L$.

Inductive Step:

Let $a \in \mathbb{Z}$ be arbitrary. We can calculate as follows

$$\begin{aligned} \text{concat}(a :: L, \text{nil}) &= a :: \text{concat}(L, \text{nil}) && \text{def of concat} \\ &= a :: L && \text{IH} \end{aligned}$$

which is $P(a :: L)$.

By induction, we have shown the claim holds for all $L \in \text{List}$.

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \text{List}$

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Base Case (nil): Let $R \in \mathbf{List}$ be arbitrary. Then,

Length:

$\text{len}(\text{nil}) := 0$

$\text{len}(a :: L) := \text{len}(L) + 1$

Concatenation:

$\text{concat}(\text{nil}, R) := R$

$\text{concat}(a :: L, R) := a :: \text{concat}(L, R)$

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Base Case (nil): Let $R \in \mathbf{List}$ be arbitrary. Then,

$$\begin{aligned} \text{len}(\text{concat}(\text{nil}, R)) &= \text{len}(R) && \text{def of concat} \\ &= 0 + \text{len}(R) \\ &= \text{len}(\text{nil}) + \text{len}(R) && \text{def of len} \end{aligned}$$

Since R was arbitrary, $P(\text{nil})$ holds.

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Base Case (nil): Let $R \in \mathbf{List}$ be arbitrary. Then, $\text{len}(\text{concat}(\text{nil}, R)) = \text{len}(R) = 0 + \text{len}(R) = \text{len}(\text{nil}) + \text{len}(R)$, showing $P(\text{nil})$.

Inductive Hypothesis: Assume that $P(L)$ is true for some arbitrary $L \in \mathbf{List}$, i.e., $\text{len}(\text{concat}(L, R)) = \text{len}(L) + \text{len}(R)$ for all $R \in \mathbf{List}$.

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Base Case (nil): Let $R \in \mathbf{List}$ be arbitrary. Then, $\text{len}(\text{concat}(\text{nil}, R)) = \text{len}(R) = 0 + \text{len}(R) = \text{len}(\text{nil}) + \text{len}(R)$, showing $P(\text{nil})$.

Inductive Hypothesis: Assume that $P(L)$ is true for some arbitrary $L \in \mathbf{List}$, i.e., $\text{len}(\text{concat}(L, R)) = \text{len}(L) + \text{len}(R)$ for all $R \in \mathbf{List}$.

Inductive Step:

Goal: For any $a \in \mathbb{Z}$, and $R \in \mathbf{List}$, show $P(a :: L)$, i.e.,
 $\text{len}(\text{concat}(a :: L, R)) = \text{len}(a :: L) + \text{len}(R)$

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Base Case (nil): Let $R \in \mathbf{List}$ be arbitrary. Then, $\text{len}(\text{concat}(\text{nil}, R)) = \text{len}(R) = 0 + \text{len}(R) = \text{len}(\text{nil}) + \text{len}(R)$, showing $P(\text{nil})$.

Inductive Hypothesis: Assume that $P(L)$ is true for some arbitrary $L \in \mathbf{List}$, i.e., $\text{len}(\text{concat}(L, R)) = \text{len}(L) + \text{len}(R)$ for all $R \in \mathbf{List}$.

Inductive Step: Let $a \in \mathbb{Z}$ and $R \in \mathbf{List}$ be arbitrary. Then,

Length:

$\text{len}(\text{nil}) := 0$

$\text{len}(a :: L) := \text{len}(L) + 1$

Concatenation:

$\text{concat}(\text{nil}, R) := R$

$\text{concat}(a :: L, R) := a :: \text{concat}(L, R)$

Claim: $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $S, R \in \mathbf{List}$

Let $P(S)$ be “ $\text{len}(\text{concat}(S, R)) = \text{len}(S) + \text{len}(R)$ for all $R \in \mathbf{List}$ ”.

We prove $P(S)$ for all $S \in \mathbf{List}$ by structural induction.

Base Case (nil): Let $R \in \mathbf{List}$ be arbitrary. Then, $\text{len}(\text{concat}(\text{nil}, R)) = \text{len}(R) = 0 + \text{len}(R) = \text{len}(\text{nil}) + \text{len}(R)$, showing $P(\text{nil})$.

Inductive Hypothesis: Assume that $P(L)$ is true for some arbitrary $L \in \mathbf{List}$, i.e., $\text{len}(\text{concat}(L, R)) = \text{len}(L) + \text{len}(R)$ for all $R \in \mathbf{List}$.

Inductive Step: Let $a \in \mathbb{Z}$ and $R \in \mathbf{List}$ be arbitrary. Then, we have

$$\begin{aligned} \text{len}(\text{concat}(a :: L, R)) &= \text{len}(a :: \text{concat}(L, R)) && \text{def of concat} \\ &= 1 + \text{len}(\text{concat}(L, R)) && \text{def of len} \\ &= 1 + \text{len}(L) + \text{len}(R) && \text{IH} \\ &= \text{len}(a :: L) + \text{len}(R) && \text{def of len} \end{aligned}$$

Since R was arbitrary, we have shown $P(a :: L)$.

By induction, we have shown the claim holds for all $S \in \mathbf{List}$.