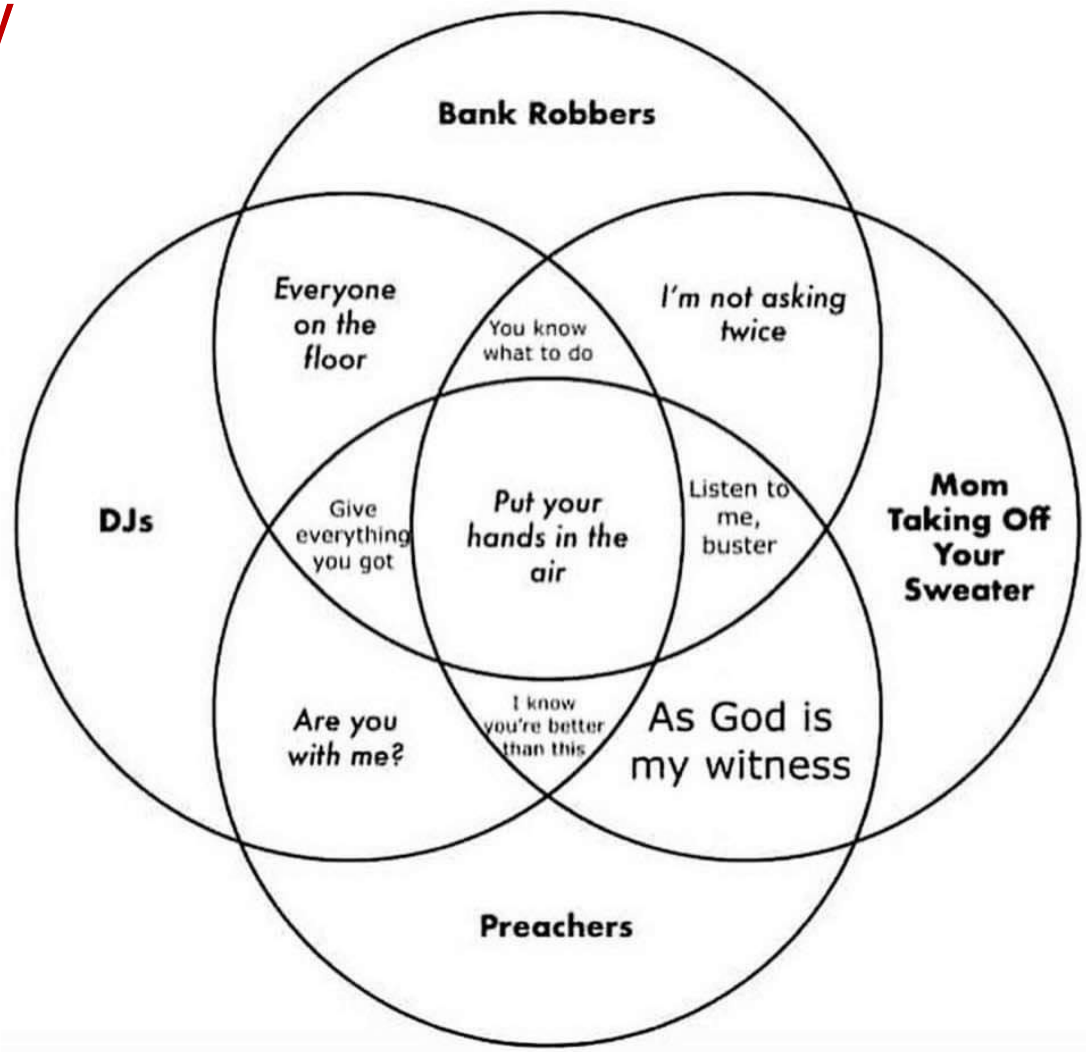
CSE 311: Foundations of Computing

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

$A = \{1\}$

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

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

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

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

Some Common Sets

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

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

$\mathbb{Q}$ is the set of **Rational Numbers**; e.g. ½, -17, 32/48

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

[n] is the set **{1, 2, …, n}** when **n** is a natural number

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

Sets can be elements of other sets

For example

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

$B = \{1,2\}$

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:

- $\{1\} = \{1, 1, 1\}$
- $\varnothing$ 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}

<u>QUESTIONS</u>

$A \subseteq B$?
$C \subseteq B$?
$\varnothing \subseteq A$?

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: $(A = B) \equiv (A \subseteq B) \wedge (B \subseteq A)$

$A \supseteq B$ means $B \subseteq A$

$A \subset B$ 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 ∀: 3

   5.2. $y \in B \rightarrow y \in A$ Elim ∀: 4

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

5. $\forall x\,(x \in A \leftrightarrow x \in B)$ Intro ∀
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** $P(x) := \text{“}x \in S\text{”}$

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. $\forall x\, (x \in A \rightarrow x \in B)$ Intro ∀: 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. $x \in A$ 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 ∀: 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. $x \in A$ Assumption

1.1.2. $P(x)$ Def of A

1.1.?. $Q(x)$??

1.1.?. $x \in B$ Def of 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

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

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).

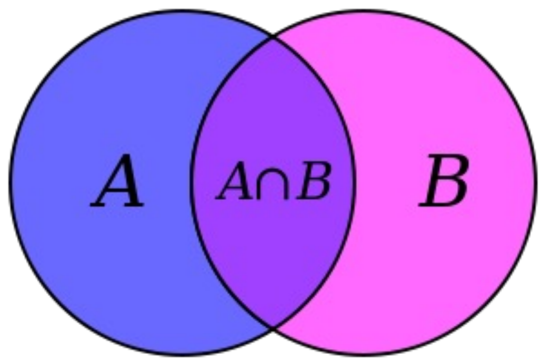
…

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 $\mathrm{A} \cup \bar{\mathrm{A}} = U$

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 $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

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 ⊆ B.

De Morgan's Laws

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

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

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 $\subseteq$ 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 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 $\subseteq$ B.

De Morgan's Laws

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

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

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 $\subseteq$ B.

De Morgan's Laws

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

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

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 $\subseteq$ B.

De Morgan's Laws

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

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

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 $\subseteq$ B.

De Morgan's Laws

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

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

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 $\neg(x \in A) \land \neg(x \in B)$, which is equivalent to $\neg(x \in A \lor x \in B)$ 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 $\subseteq$ B.

Proofs About Set Equality

A lot of *repetitive* work to show → and ←.

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 compliment,
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 → and ←.

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 compliment,
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 $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

The stated biconditional holds since:

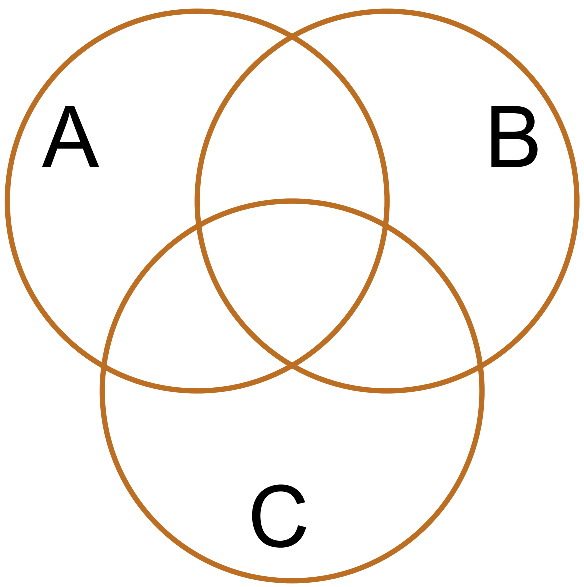
$x \in (A \cup B)^C$	$\equiv \neg(x \in A \cup B)$	Def of Comp
	$\equiv \neg(x \in A \vee x \in B)$	Def of Union
	$\equiv \neg(x \in A) \wedge \neg(x \in B)$	De Morgan
	$\equiv x \in A^C \wedge x \in B^C$	Def of Comp
	$\equiv x \in A^C \cap B^C$	Def of Intersection

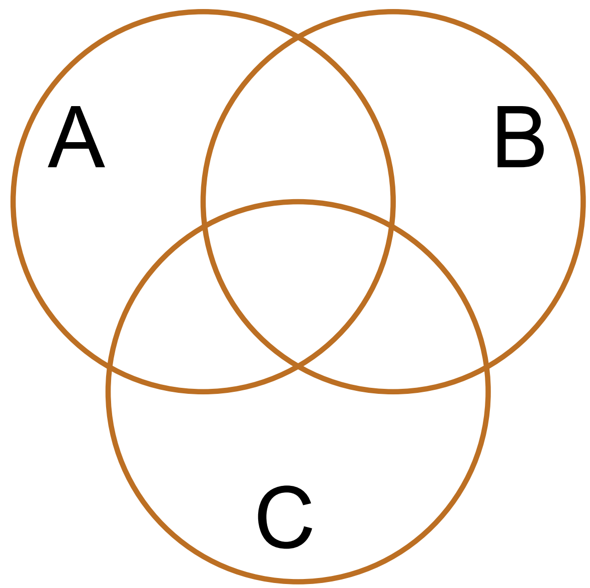
Chains of equivalences are often easier to read like this rather than as English text

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:

$x \in A \cap (B \cup C)$

$\equiv (x \in A) \wedge (x \in B \cup C)$	Def of Intersection
$\equiv (x \in A) \wedge ((x \in B) \vee (x \in C))$	Def of Union
$\equiv ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))$	Distributive
$\equiv (x \in A \cap B) \vee (x \in A \cap C)$	Def of Intersection
$\equiv x \in (A \cap B) \cup (A \cap C)$	Def of Union

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 ∪ with ∨, ∩ with ∧, and $\cdot^C$ with ¬.

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 ∪ with ∨, ∩ with ∧, and $\cdot^C$ with ¬.

"Proof": Let x be an arbitrary object.

The stated bi-condition holds since:

x ∈ left side ≡ replace set ops with propositional logic

≡ apply Propositional Logic equivalence

≡ replace propositional logic with set ops

≡ x ∈ 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 Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class

$\mathcal{P}$(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 Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class

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

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

Power Set

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

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

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

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

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

Cartesian Product

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

- $\mathbb{R} \times \mathbb{R}$ 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 × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

Cartesian Product

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

- $\mathbb{R} \times \mathbb{R}$ **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 × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

What is $A \times \emptyset$**?**

Cartesian Product

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

- $\mathbb{R} \times \mathbb{R}$ **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 × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

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

More Set Builder Notation

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

- **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 ∃-quantified**

    this is the one <u>exception</u> to the rule that
    unbound variables are implicitly ∀-quantified

More Set Builder Notation

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

"filter"

- Then $x \in S$ tells us that $\mathrm{P}(x)$ 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** $\mathrm{P}(x)$ **holds**

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

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

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

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, **a** = 2**b** for some integer b. Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$. 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, $\mathbf{a} = 2\mathbf{b}$ for some integer b. Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$. 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. ■

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 $\forall x\ \forall y\ ((\mathrm{Odd}(x) \wedge \mathrm{Odd}(y)) \rightarrow \mathrm{Even}(x+y))$

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**.

Then, 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. ■

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.

This is reminiscent of the truth value of the statement “This statement is false.”

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.

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:

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

these definitions are constructive.

Recursive Definition 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