



# CSE 311 Lecture 10: Set Theory

Emina Torlak and Kevin Zatloukal

# Topics

## English proofs and proof strategies

A quick wrap-up of [Lecture 09](#).

## Set theory basics

Set membership ( $\in$ ), subset ( $\subseteq$ ), and equality ( $=$ ).

## Set operations

Set operations and their relation to Boolean algebra.

## More sets

Power set, Cartesian product, and Russell's paradox.

## Working with sets

Representing sets as bitvectors and applications of bitvectors.

# English proofs and proof strategies

A quick wrap-up of [Lecture 09](#).



# Benefits of English proofs

This is more work to write

```
%a = add %i, 1
%b = mod %a, %n
%c = add %arr, %b
%d = load %c
%e = add %arr, %i
store %e, %d
```

than this

```
arr[i] = arr[(i+1) % n];
```

Higher level language is easier  
because it skips details.

# Benefits of English proofs

This is more work to write

```
%a = add %i, 1
%b = mod %a, %n
%c = add %arr, %b
%d = load %c
%e = add %arr, %i
store %e, %d
```

than this

```
arr[i] = arr[(i+1) % n];
```

Higher level language is easier because it skips details.

Formal proofs are the low level language: each part must be spelled out in precise detail.

# Benefits of English proofs

This is more work to write

```
%a = add %i, 1
%b = mod %a, %n
%c = add %arr, %b
%d = load %c
%e = add %arr, %i
store %e, %d
```

than this

```
arr[i] = arr[(i+1) % n];
```

Higher level language is easier because it skips details.

Formal proofs are the low level language: each part must be spelled out in precise detail.

English proofs are the high level language.

An English proof is correct if the *reader* is convinced they can “compile” it to a formal proof if necessary.

# Proof strategies

Sometimes, it's too hard to prove a theorem directly using inference rules, equivalences, and domain properties.

When that's the case, try one of the following alternative strategies:

- Proof by contrapositive,
- Disproof by counterexamples, and
- Proof by contradiction.



# Proof by contrapositive

If we assume  $\neg q$  and derive  $\neg p$ , then we have proven that  $\neg q \rightarrow \neg p$ , which is equivalent to proving  $p \rightarrow q$ .

1.1.  $\neg q$      **Assumption**

...

1.3.  $\neg p$

2.  $\neg q \rightarrow \neg p$      **Direct Proof Rule**

3.  $p \rightarrow q$      **Contrapositive: 2**

# Counterexamples

To *disprove*  $\forall \mathbf{x}. \mathbf{P}(\mathbf{x})$ , prove  $\exists \mathbf{x}. \neg \mathbf{P}(\mathbf{x})$ .

Works by DeMorgan's Law:  $\neg \forall x. P(x) \equiv \exists x. \neg P(x)$ .

All we need to do is find an  $x$  for which  $P(x)$  is false.

This  $x$  is called a *counterexample*.

**Example: disprove that “Every prime number is odd”.**

2 is a prime number that is not odd.

# Proof by contradiction

If we assume  $p$  and derive  $F$  (a contradiction), then we have proven  $\neg p$ .

1.1.  $p$       **Assumption**

...

1.3.  $F$

2.  $p \rightarrow F$       **Direct Proof Rule**

3.  $\neg p \vee F$       **Law of Implication: 2**

4.  $\neg p$       **Identity: 3**

# An example proof by contradiction

Prove that “No integer is both even and odd.”

English proof:  $\neg\exists x. \text{Even}(x) \wedge \text{Odd}(x) \equiv \forall x. \neg(\text{Even}(x) \wedge \text{Odd}(x))$ .

**Proof by contradiction**

# An example proof by contradiction

Prove that “No integer is both even and odd.”

English proof:  $\neg\exists x. \text{Even}(x) \wedge \text{Odd}(x) \equiv \forall x. \neg(\text{Even}(x) \wedge \text{Odd}(x))$ .

## Proof by contradiction

Let  $x$  be an arbitrary integer and suppose that it is both even and odd.

# An example proof by contradiction

Prove that “No integer is both even and odd.”

English proof:  $\neg\exists x. \text{Even}(x) \wedge \text{Odd}(x) \equiv \forall x. \neg(\text{Even}(x) \wedge \text{Odd}(x))$ .

## Proof by contradiction

Let  $x$  be an arbitrary integer and suppose that it is both even and odd.

Then  $x = 2a$  for some integer  $a$  and  $x = 2b + 1$  for some integer  $b$ .

# An example proof by contradiction

Prove that “No integer is both even and odd.”

English proof:  $\neg\exists x. \text{Even}(x) \wedge \text{Odd}(x) \equiv \forall x. \neg(\text{Even}(x) \wedge \text{Odd}(x))$ .

## Proof by contradiction

Let  $x$  be an arbitrary integer and suppose that it is both even and odd.

Then  $x = 2a$  for some integer  $a$  and  $x = 2b + 1$  for some integer  $b$ .

Therefore  $2a = 2b + 1$  and hence  $a = b + \frac{1}{2}$ .

# An example proof by contradiction

Prove that “No integer is both even and odd.”

English proof:  $\neg\exists x. \text{Even}(x) \wedge \text{Odd}(x) \equiv \forall x. \neg(\text{Even}(x) \wedge \text{Odd}(x))$ .

## Proof by contradiction

Let  $x$  be an arbitrary integer and suppose that it is both even and odd.

Then  $x = 2a$  for some integer  $a$  and  $x = 2b + 1$  for some integer  $b$ .

Therefore  $2a = 2b + 1$  and hence  $a = b + \frac{1}{2}$ .

But two integers cannot differ by  $\frac{1}{2}$  so this is a contradiction.



# An example proof by contradiction

Prove that “No integer is both even and odd.”

English proof:  $\neg\exists x. \text{Even}(x) \wedge \text{Odd}(x) \equiv \forall x. \neg(\text{Even}(x) \wedge \text{Odd}(x))$ .

## Proof by contradiction

Let  $x$  be an arbitrary integer and suppose that it is both even and odd.

Then  $x = 2a$  for some integer  $a$  and  $x = 2b + 1$  for some integer  $b$ .

Therefore  $2a = 2b + 1$  and hence  $a = b + \frac{1}{2}$ .

But two integers cannot differ by  $\frac{1}{2}$  so this is a contradiction.

Therefore no integer is both even and odd.  $\square$

# Fun strategy: proof by computer

Use an automated theorem prover:

```
; No integer is both even and odd.

(define-fun even ((x Int)) Bool
  (exists ((y Int)) (= x (* 2 y))))

(define-fun odd ((x Int)) Bool
  (exists ((y Int)) (= x (+ (* 2 y) 1))))

(define-fun claim () Bool
  (not (exists ((x Int)) (and (even x) (odd x)))))

(assert (not claim)) ; proof by contradiction

(check-sat)
```

# Fun strategy: proof by computer

Use an automated theorem prover:

```
; No integer is both even and odd.

(define-fun even ((x Int)) Bool
  (exists ((y Int)) (= x (* 2 y))))

(define-fun odd ((x Int)) Bool
  (exists ((y Int)) (= x (+ (* 2 y) 1))))

(define-fun claim () Bool
  (not (exists ((x Int)) (and (even x) (odd x)))))

(assert (not claim)) ; proof by contradiction

(check-sat)
```

While this example works, proofs of arbitrary formulas in predicate logic *cannot* be automated. But *interactive theorem provers* can still help by checking your formal proof and filling in some low-level details for you.

# Fun fact: counterexamples & contradiction in verification

Automated verifiers work by counterexample and contradiction proofs.

Recall that program verification involves proving that a program  $P$  satisfies a specification  $S$  on all inputs  $x$ :  $\forall x. p(x) \rightarrow s(x)$ , where  $p$  and  $s$  are formulas encoding the semantics of  $P$  and  $S$ .

# Fun fact: counterexamples & contradiction in verification

Automated verifiers work by counterexample and contradiction proofs.

Recall that program verification involves proving that a program  $P$  satisfies a specification  $S$  on all inputs  $x$ :  $\forall x. p(x) \rightarrow s(x)$ , where  $p$  and  $s$  are formulas encoding the semantics of  $P$  and  $S$ .

The program verifier sends the formula  $\exists \mathbf{x}. \mathbf{p}(\mathbf{x}) \wedge \neg \mathbf{s}(\mathbf{x})$  to the prover.

$\neg \forall x. p(x) \rightarrow s(x) \equiv \exists x. \neg(p(x) \rightarrow s(x)) \equiv \exists x. \neg(\neg p(x) \vee s(x)) \equiv \exists x. p(x) \wedge \neg s(x)$ .

# Fun fact: counterexamples & contradiction in verification

**Automated verifiers work by counterexample and contradiction proofs.**

Recall that program verification involves proving that a program  $P$  satisfies a specification  $S$  on all inputs  $x$ :  $\forall x. p(x) \rightarrow s(x)$ , where  $p$  and  $s$  are formulas encoding the semantics of  $P$  and  $S$ .

**The program verifier sends the formula  $\exists \mathbf{x}. \mathbf{p}(\mathbf{x}) \wedge \neg \mathbf{s}(\mathbf{x})$  to the prover.**

$\neg \forall x. p(x) \rightarrow s(x) \equiv \exists x. \neg(p(x) \rightarrow s(x)) \equiv \exists x. \neg(\neg p(x) \vee s(x)) \equiv \exists x. p(x) \wedge \neg s(x)$ .

**If the prover finds a counterexample, we know the program is incorrect.**

The counterexample is a concrete input (test case) on which the program violates the spec.

# Fun fact: counterexamples & contradiction in verification

**Automated verifiers work by counterexample and contradiction proofs.**

Recall that program verification involves proving that a program  $P$  satisfies a specification  $S$  on all inputs  $x$ :  $\forall x. p(x) \rightarrow s(x)$ , where  $p$  and  $s$  are formulas encoding the semantics of  $P$  and  $S$ .

**The program verifier sends the formula  $\exists \mathbf{x}. p(\mathbf{x}) \wedge \neg s(\mathbf{x})$  to the prover.**

$\neg \forall x. p(x) \rightarrow s(x) \equiv \exists x. \neg(p(x) \rightarrow s(x)) \equiv \exists x. \neg(\neg p(x) \vee s(x)) \equiv \exists x. p(x) \wedge \neg s(x)$ .

**If the prover finds a counterexample, we know the program is incorrect.**

The counterexample is a concrete input (test case) on which the program violates the spec.

**If no counterexample exists, we know the program is correct.**

Because this is proof by contradiction! The prover assumed  $\exists x. p(x) \wedge \neg s(x)$  and arrived at false (“unsat”).

# Set theory basics

Set membership ( $\in$ ), subset ( $\subseteq$ ), and equality ( $=$ ).



# What is a set?

A set is a collection of objects called *elements*.

Write  $a \in B$  to say that  $a$  is an element in the set  $B$ .

Write  $a \notin B$  to say that  $a$  isn't an element of  $B$ .

## Examples

$$A = \{1\}$$

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

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

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

$$E = \{1, 2, 7, \alpha, \emptyset, \text{dog}, \img alt="cat face icon" data-bbox="388 538 412 572"}\}$$

## 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.  $1$ ,  $-17$ ,  $\frac{32}{48}$ ,  $\pi$ ,  $\sqrt{2}$

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

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

# Sets can be elements of other sets

For example, consider the sets

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

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

Then we have

$$B \in A$$

$$\emptyset \in A$$

# Definitions: equality and subset

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

$$A = B \equiv \forall x. x \in A \leftrightarrow x \in B$$

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

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

Note:  $A = B \equiv A \subseteq B \wedge B \subseteq A$ .

# Example: understanding equality

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

$$A = B \equiv \forall x. x \in A \leftrightarrow x \in B$$

Which sets are equal to each other?

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

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

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

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

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

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

# Example: understanding equality

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

$$A = B \equiv \forall x. x \in A \leftrightarrow x \in B$$

Which sets are equal to each other?

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

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

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

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

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

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

**C, D, E** are equal to each other.

Order of elements doesn't matter, and duplicates don't matter.

*F* is *not* equal to *C, D, E* because  $\{3\} \neq 3$ !

# Example: understanding subsets

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

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

Example sets

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

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

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

Are these subset formulas true or false?

$$\emptyset \subseteq A$$

$$A \subseteq B$$

$$C \subseteq B$$

# Example: understanding subsets

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

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

Example sets

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

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

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

Are these subset formulas true or false?

$$\emptyset \subseteq A \quad \mathbf{T}$$

$$A \subseteq B$$

$$C \subseteq B$$



# Example: understanding subsets

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

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

Example sets

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

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

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

Are these subset formulas true or false?

$$\emptyset \subseteq A \quad \mathbf{T}$$

$$A \subseteq B \quad \mathbf{F}$$

$$C \subseteq B$$

# Example: understanding subsets

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

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

Example sets

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

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

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

Are these subset formulas true or false?

$$\emptyset \subseteq A \quad \mathbf{T}$$

$$A \subseteq B \quad \mathbf{F}$$

$$C \subseteq B \quad \mathbf{T}$$

# Building sets from predicates

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

$S$  is the set of all  $x$  in the domain of  $P$  for which  $P(x)$  is true.

The domain of  $P$  is often called the **universe**  $U$ .

# Building sets from predicates

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

$S$  is the set of all  $x$  in the domain of  $P$  for which  $P(x)$  is true. The domain of  $P$  is often called the **universe**  $U$ .

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

$S$  is the set of all  $x$  in  $A$  for which  $P(x)$  is true.

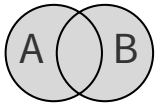
# Set operations

Set operations and their relation to Boolean algebra.

# Union, intersection, and set difference

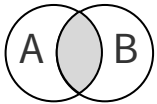
## Union

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



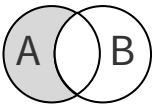
## Intersection

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



## Set difference

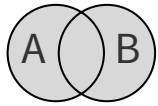
$$A \setminus B = \{x : (x \in A) \wedge (x \notin B)\}$$



# Union, intersection, and set difference

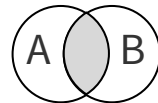
## Union

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



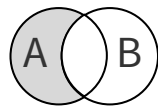
## Intersection

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



## Set difference

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



Given the following sets ...

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

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

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

Use set operations to make:

$$[6] =$$

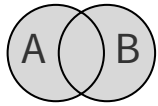
$$\{3\} =$$

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

# Union, intersection, and set difference

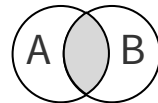
## Union

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



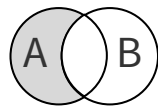
## Intersection

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



## Set difference

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



Given the following sets ...

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

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

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

Use set operations to make:

$$[6] = A \cup B \cup C$$

$$\{3\} =$$

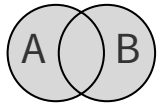
$$\{1, 2\} =$$



# Union, intersection, and set difference

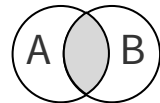
## Union

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



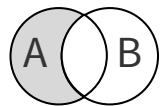
## Intersection

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



## Set difference

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



Given the following sets ...

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

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

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

Use set operations to make:

$$[6] = A \cup B \cup C$$

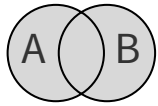
$$\{3\} = A \cap B = A \cap C$$

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

# Union, intersection, and set difference

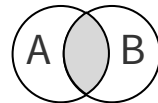
## Union

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



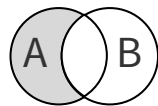
## Intersection

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



## Set difference

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



Given the following sets ...

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

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

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

Use set operations to make:

$$[6] = A \cup B \cup C$$

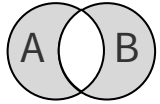
$$\{3\} = A \cap B = A \cap C$$

$$\{1, 2\} = A \setminus B = A \setminus C$$

# Symmetric difference and complement

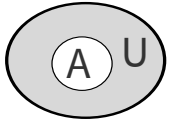
## Symmetric difference

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



## Complement (with respect to universe $U$ )

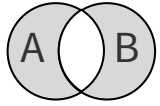
$$\bar{A} = \{x : x \notin A\} = \{x : \neg(x \in A)\}$$



# Symmetric difference and complement

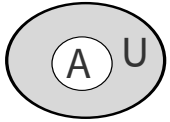
## Symmetric difference

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



## Complement (with respect to universe $U$ )

$$\bar{A} = \{x : x \notin A\} = \{x : \neg(x \in A)\}$$



Given the sets and universe ...

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

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

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

What is

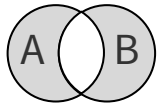
$$A \oplus B =$$

$$\bar{A} =$$

# Symmetric difference and complement

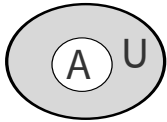
## Symmetric difference

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



## Complement (with respect to universe U)

$$\bar{A} = \{x : x \notin A\} = \{x : \neg(x \in A)\}$$



Given the sets and universe ...

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

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

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

What is

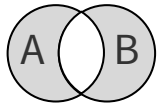
$$A \oplus B = \{3, 4, 6\}$$

$$\bar{A} =$$

# Symmetric difference and complement

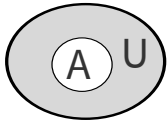
## Symmetric difference

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



## Complement (with respect to universe $U$ )

$$\bar{A} = \{x : x \notin A\} = \{x : \neg(x \in A)\}$$



Given the sets and universe ...

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

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

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

What is

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

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

# This is Boolean algebra again

Union  $\cup$  is defined using  $\vee$ .

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

Intersection  $\cap$  is defined using  $\wedge$ .

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

Complement works like  $\neg$ .

$$\overline{A} = \{x : x \notin A\} = \{x : \neg(x \in A)\}$$

# This is Boolean algebra again

Union  $\cup$  is defined using  $\vee$ .

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

Intersection  $\cap$  is defined using  $\wedge$ .

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

Complement works like  $\neg$ .

$$\bar{A} = \{x : x \notin A\} = \{x : \neg(x \in A)\}$$

This means that all equivalences from Boolean algebra translate directly into set theory, and you can use them in your proofs!



# DeMorgan's laws

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

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

How would we prove these?

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

# DeMorgan's laws

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

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

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of "U",  $\neg(x \in A \vee x \in B)$ .

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of “ $\cup$ ”,  $\neg(x \in A \vee x \in B)$ .

Applying DeMorgan's laws, we get  $x \notin A \wedge x \notin B$ .

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of “ $\cup$ ”,  $\neg(x \in A \vee x \in B)$ .

Applying DeMorgan's laws, we get  $x \notin A \wedge x \notin B$ .

So,  $x \in \bar{A} \wedge x \in \bar{B}$  by definition of complement.



# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show  
 $x \in C \rightarrow x \in D$  and  
 $x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of “ $\cup$ ”,  $\neg(x \in A \vee x \in B)$ .

Applying DeMorgan's laws, we get  $x \notin A \wedge x \notin B$ .

So,  $x \in \bar{A} \wedge x \in \bar{B}$  by definition of complement.

Finally,  $x \in \bar{A} \cap \bar{B}$  by definition of “ $\cap$ ”, and we

have shown that  $x \in \overline{A \cup B} \rightarrow x \in \bar{A} \cap \bar{B}$ .

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of “ $\cup$ ”,  $\neg(x \in A \vee x \in B)$ .

Applying DeMorgan's laws, we get  $x \notin A \wedge x \notin B$ .

So,  $x \in \bar{A} \wedge x \in \bar{B}$  by definition of complement.

Finally,  $x \in \bar{A} \cap \bar{B}$  by definition of “ $\cap$ ”, and we

have shown that  $x \in \overline{A \cup B} \rightarrow x \in \bar{A} \cap \bar{B}$ .

Next, let  $x \in \bar{A} \cap \bar{B}$  be arbitrary.

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

Proof that  $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of “ $\cup$ ”,  $\neg(x \in A \vee x \in B)$ .

Applying DeMorgan's laws, we get  $x \notin A \wedge x \notin B$ .

So,  $x \in \bar{A} \wedge x \in \bar{B}$  by definition of complement.

Finally,  $x \in \bar{A} \cap \bar{B}$  by definition of “ $\cap$ ”, and we

have shown that  $x \in \overline{A \cup B} \rightarrow x \in \bar{A} \cap \bar{B}$ .

Next, let  $x \in \bar{A} \cap \bar{B}$  be arbitrary.

...

# DeMorgan's laws

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

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

How would we prove these?

## Proof technique:

To prove  $C = D$ , show

$x \in C \rightarrow x \in D$  and

$x \in D \rightarrow x \in C$ .

## Proof that $\overline{A \cup B} = \bar{A} \cap \bar{B}$ :

Let  $x \in \overline{A \cup B}$  be arbitrary.

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

By definition of “ $\cup$ ”,  $\neg(x \in A \vee x \in B)$ .

Applying DeMorgan's laws, we get  $x \notin A \wedge x \notin B$ .

So,  $x \in \bar{A} \wedge x \in \bar{B}$  by definition of complement.

Finally,  $x \in \bar{A} \cap \bar{B}$  by definition of “ $\cap$ ”, and we

have shown that  $x \in \overline{A \cup B} \rightarrow x \in \bar{A} \cap \bar{B}$ .

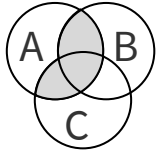
Next, let  $x \in \bar{A} \cap \bar{B}$  be arbitrary.

...

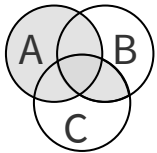
Finally,  $x \in \bar{A} \cap \bar{B}$ , so  $x \in \bar{A} \cap \bar{B} \rightarrow x \in \overline{A \cup B}$ , which completes the proof.  $\square$

# Distributivity laws

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



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



# A simple set proof

Prove that for any sets **A** and **B**, we have  $(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{A}$ .

Recall that  $X \subseteq Y \equiv \forall x. x \in X \rightarrow x \in Y$

**Proof:**

# A simple set proof

Prove that for any sets **A** and **B**, we have  $(\mathbf{A} \cap \mathbf{B}) \subseteq \mathbf{A}$ .

Recall that  $X \subseteq Y \equiv \forall x. x \in X \rightarrow x \in Y$

**Proof:**

Let  $A$  and  $B$  be arbitrary sets and  $x$  an arbitrary element of  $A \cap B$ .

# A simple set proof

Prove that for any sets  $A$  and  $B$ , we have  $(A \cap B) \subseteq A$ .

Recall that  $X \subseteq Y \equiv \forall x. x \in X \rightarrow x \in Y$

**Proof:**

Let  $A$  and  $B$  be arbitrary sets and  $x$  an arbitrary element of  $A \cap B$ .  
Then, by definition of  $A \cap B$ , we have that  $x \in A$  and  $x \in B$ .



# A simple set proof

Prove that for any sets **A** and **B**, we have  $(A \cap B) \subseteq A$ .

Recall that  $X \subseteq Y \equiv \forall x. x \in X \rightarrow x \in Y$

**Proof:**

Let  $A$  and  $B$  be arbitrary sets and  $x$  an arbitrary element of  $A \cap B$ .

Then, by definition of  $A \cap B$ , we have that  $x \in A$  and  $x \in B$ .

It follows that  $x \in A$ , as required.  $\square$

## Set proofs can use Boolean algebra equivalences

Prove that for any sets  $A$  and  $B$ , we have  $(A \cap B) \cup (A \cap \bar{B}) = A$ .

**Proof:**

## Set proofs can use Boolean algebra equivalences

Prove that for any sets  $A$  and  $B$ , we have  $(A \cap B) \cup (A \cap \bar{B}) = A$ .

**Proof:**

Let  $A$  and  $B$  be arbitrary sets.

# Set proofs can use Boolean algebra equivalences

Prove that for any sets  $A$  and  $B$ , we have  $(A \cap B) \cup (A \cap \bar{B}) = A$ .

## Proof:

Let  $A$  and  $B$  be arbitrary sets.

Since set operations are defined using logical connectives, the equivalences of Boolean algebra can be used directly, as follows:

# Set proofs can use Boolean algebra equivalences

Prove that for any sets  $A$  and  $B$ , we have  $(A \cap B) \cup (A \cap \bar{B}) = A$ .

## Proof:

Let  $A$  and  $B$  be arbitrary sets.

Since set operations are defined using logical connectives, the equivalences of Boolean algebra can be used directly, as follows:

$$\begin{aligned}(A \cap B) \cup (A \cap \bar{B}) &= A \cap (B \cup \bar{B}) && \text{Distributivity} \\ &= A \cap U && \text{Complementarity} \\ &= A && \text{Identity}\end{aligned}$$

# Set proofs can use Boolean algebra equivalences

Prove that for any sets  $A$  and  $B$ , we have  $(A \cap B) \cup (A \cap \bar{B}) = A$ .

## Proof:

Let  $A$  and  $B$  be arbitrary sets.

Since set operations are defined using logical connectives, the equivalences of Boolean algebra can be used directly, as follows:

$$\begin{aligned}(A \cap B) \cup (A \cap \bar{B}) &= A \cap (B \cup \bar{B}) && \text{Distributivity} \\ &= A \cap U && \text{Complementarity} \\ &= A && \text{Identity}\end{aligned}$$

Universe  $U$  corresponds to 1 and  $\emptyset$  corresponds to 0.

# More sets

Power set, Cartesian product, and Russell's paradox.

# Power set

Power set of a set  $A$  is the set of all subsets of  $A$ .

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

## Examples

Let Days =  $\{M, W, F\}$ .

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

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



# Power set

Power set of a set  $A$  is the set of all subsets of  $A$ .

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

## Examples

Let Days =  $\{M, W, F\}$ .

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

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

# Power set

Power set of a set  $A$  is the set of all subsets of  $A$ .

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

## Examples

Let Days =  $\{M, W, F\}$ .

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

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

# Cartesian product

The Cartesian product of two sets is the set of all of their ordered pairs.

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

## Examples

$\mathbb{R} \times \mathbb{R}$  is the real plane.

$\mathbb{Z} \times \mathbb{Z}$  is the set of all pairs of integers.

# Cartesian product

The Cartesian product of two sets is the set of all of their ordered pairs.

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

## Examples

$\mathbb{R} \times \mathbb{R}$  is the real plane.

$\mathbb{Z} \times \mathbb{Z}$  is the set of all pairs of integers.

If  $A = \{1, 2\}$ ,  $B = \{a, b, c\}$ ,

then  $A \times B =$

# Cartesian product

The Cartesian product of two sets is the set of all of their ordered pairs.

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

## Examples

$\mathbb{R} \times \mathbb{R}$  is the real plane.

$\mathbb{Z} \times \mathbb{Z}$  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

The Cartesian product of two sets is the set of all of their ordered pairs.

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

## Examples

$\mathbb{R} \times \mathbb{R}$  is the real plane.

$\mathbb{Z} \times \mathbb{Z}$  is the set of all pairs of integers.

If  $A = \{1, 2\}$ ,  $B = \{a, b, c\}$ ,

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

$A \times \emptyset =$

# Cartesian product

The Cartesian product of two sets is the set of all of their ordered pairs.

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

## Examples

$\mathbb{R} \times \mathbb{R}$  is the real plane.

$\mathbb{Z} \times \mathbb{Z}$  is the set of all pairs of integers.

If  $A = \{1, 2\}$ ,  $B = \{a, b, c\}$ ,

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

$A \times \emptyset = \{(a, b) : a \in A \wedge b \in \emptyset\} = \{(a, b) : a \in A \wedge \text{F}\} = \emptyset.$

# Russell's paradox

Let  $S$  be the set of all sets that don't contain themselves.

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



# Russell's paradox

Let  $S$  be the set of all sets that don't contain themselves.

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

The definition of  $S$  is contradictory, hence the paradox.

# Russell's paradox

Let  $S$  be the set of all sets that don't contain themselves.

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

The definition of  $S$  is contradictory, hence the paradox.

Suppose that  $S \in S$ . Then, by definition of  $S$ ,  $S \notin S$ , which is a contradiction.

# Russell's paradox

Let  $S$  be the set of all sets that don't contain themselves.

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

The definition of  $S$  is contradictory, hence the paradox.

Suppose that  $S \in S$ . Then, by definition of  $S$ ,  $S \notin S$ , which is a contradiction.

Suppose that  $S \notin S$ . Then, by definition of  $S$ ,  $S \in S$ , which is a contradiction too.

# Russell's paradox

Let  $S$  be the set of all sets that don't contain themselves.

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

The definition of  $S$  is contradictory, hence the paradox.

Suppose that  $S \in S$ . Then, by definition of  $S$ ,  $S \notin S$ , which is a contradiction.

Suppose that  $S \notin S$ . Then, by definition of  $S$ ,  $S \in S$ , which is a contradiction too.

To avoid the paradox ...

Define  $S$  with respect to a universe of discourse.

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

With this definition,  $S \notin S$  and there is no contradiction because  $S \notin U$ .

# Working with sets

Representing sets as bitvectors and applications of bitvectors.

# Representing sets as bitvectors

Suppose that universe  $U$  is  $\{1, 2, \dots, n\}$ .

We can represent every set  $B \subseteq U$  as a vector of bits:

$$b_1 b_2 \dots b_n \text{ where } b_i = 1 \text{ if } i \in B$$
$$b_i = 0 \text{ if } i \notin B$$

This is called the *characteristic vector* of set  $B$ .

# Representing sets as bitvectors

Suppose that universe  $U$  is  $\{1, 2, \dots, n\}$ .

We can represent every set  $B \subseteq U$  as a vector of bits:

$$b_1 b_2 \dots b_n \text{ where } b_i = 1 \text{ if } i \in B$$
$$b_i = 0 \text{ if } i \notin B$$

This is called the *characteristic vector* of set  $B$ .

**Given characteristic vectors for  $A$  and  $B$ , what is the vector for**

$$A \cup B =$$

$$A \cap B =$$

# Representing sets as bitvectors

Suppose that universe  $U$  is  $\{1, 2, \dots, n\}$ .

We can represent every set  $B \subseteq U$  as a vector of bits:

$$b_1 b_2 \dots b_n \text{ where } b_i = 1 \text{ if } i \in B$$
$$b_i = 0 \text{ if } i \notin B$$

This is called the *characteristic vector* of set  $B$ .

**Given characteristic vectors for  $\mathbf{A}$  and  $\mathbf{B}$ , what is the vector for**

$$A \cup B = (a_1 \vee b_1) \dots (a_n \vee b_n)$$

$$A \cap B =$$



# Representing sets as bitvectors

Suppose that universe  $U$  is  $\{1, 2, \dots, n\}$ .

We can represent every set  $B \subseteq U$  as a vector of bits:

$$b_1 b_2 \dots b_n \text{ where } b_i = 1 \text{ if } i \in B$$
$$b_i = 0 \text{ if } i \notin B$$

This is called the *characteristic vector* of set  $B$ .

**Given characteristic vectors for  $\mathbf{A}$  and  $\mathbf{B}$ , what is the vector for**

$$A \cup B = (a_1 \vee b_1) \dots (a_n \vee b_n)$$

$$A \cap B = (a_1 \wedge b_1) \dots (a_n \wedge b_n)$$

# Unix/Linux file permissions

```
$ ls -l  
drwxr-xr-x ... Documents/  
-rw-r--r-- ... file1
```

**Permissions maintained as bitvectors.**

Letter means the bit is 1.

”-“ means the bit is zero.

# Bitwise operations

$$\begin{array}{r} 01101101 \\ \vee 00110111 \\ \hline 01111111 \end{array}$$

$z = x \mid y$

$$\begin{array}{r} 00101010 \\ \wedge 00001111 \\ \hline 00001010 \end{array}$$

$z = x \& y$

$$\begin{array}{r} 01101101 \\ \oplus 00110111 \\ \hline 01011010 \end{array}$$

$z = x \hat{=} y$

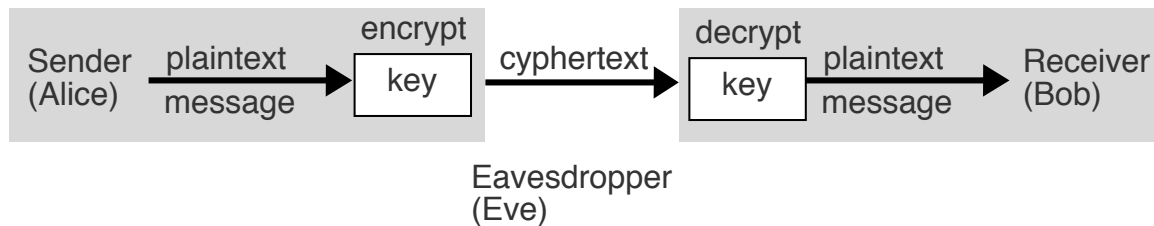
Note that  $(x \oplus y) \oplus y = x$ .

# Private key cryptography

Alice wants to communicate a message  $m$  secretly to Bob, so that eavesdropper Eve who sees their conversation can't understand  $m$ .

Alice and Bob can get together ahead of time and privately share a secret key  $K$ .

How can they communicate securely in this setting?



# One-time pad

Alice and Bob privately share a random  $n$ -bitvector  $\mathbf{K}$ .

Eve doesn't know  $K$ .

Later, Alice has  $n$ -bit message  $\mathbf{m}$  to send to Bob.

Alice computes  $C = m \oplus K$ .

Alice sends  $C$  to Bob.

Bob computes  $m = C \oplus K$ , which is  $(m \oplus K) \oplus K = m$ .

Eve can't figure out  $\mathbf{m}$  from  $\mathbf{C}$  unless she can guess  $\mathbf{K}$ .

And that's very unlikely for large  $n$  ...

# Summary

**Sets are a basic notion in mathematics and computer science.**

Collections of objects called elements.

Can be compared for equality ( $=$ ) and containment ( $\subseteq$ ).

**Set operations correspond to Boolean algebra operations.**

You can prove theorems about sets using Boolean algebra laws.

**Sets can be represented efficiently using bitvectors.**

This representation is used heavily in the real world.

With this representation, set operations reduce to fast bitwise operations.