Utrecht University

Logic for Computer Science

03 – Set theory

Wouter Swierstra

University of Utrecht

Last time

- Propositional logic
- Truth tables

Today

- Naive set theory

Organization

- Today is the first Remindo quiz – I hope you find it useful.
- Next week's quiz is on material covered today and Thursday - see the exercise page for the exact schedule.

Any questions?

Sets

There are plenty of words to talk about collections of things:

- A *pack* of wolves;
- A *den* of thieves;
- A *class* at school;
- A *fleet* of ships;

Sets

There are plenty of words to talk about collections of things:

- A *pack* of wolves;
- A *den* of thieves;
- A *class* at school;
- A *fleet* of ships;

Yet in logic, we have a single notion for a collection of things called a **set**.

Simple sets

Simple sets can be defined by listing all their **elements**:

- {true, false}
- {3, 12, 19}
- {Wouter, Nina, Vedran}

Here we write curly braces around the set, separating the individual elements using comma's.

Simple sets

Simple sets can be defined by listing all their **elements**:

- {true, false}
- {3, 12, 19}
- {Wouter, Nina, Vedran}

Here we write curly braces around the set, separating the individual elements using comma's.

The elements of set need not have anything in common:

- {2, Wouter, Nina, true}

Bigger sets

Listing all the elements can get quite tedious.

That's why we often use shorthand notation

- {0,2,4,…,50} for all the even numbers under 51;
- {a,b,c,…,z} for all the letters of the alphabet

This is less precise – but usually it is clear from the context what we mean exactly.

Infinite sets

Sets need not have a **finite** number of elements:

- {0,1,2,...} the natural numbers, $\mathbb{N}$
- {..., -2,-1,0,1,2,...} the integers, $\mathbb{Z}$

Building one set from another

We can also define new sets from existing ones.

One way to do so is by selecting the elements of a new set based on a property they share.

We then write { x : where x has some property }:

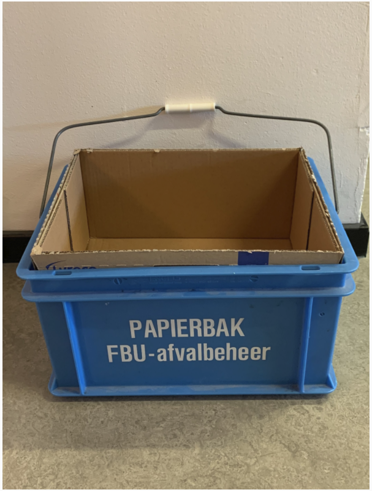
- {a : where a is a descendent of Prinses Beatrix }
- {n : where n is a prime number}
- {n/m : where n and m are integers and m is non-zero }

Special notation

- There is one set with no elements, $\emptyset$, which we refer to as the **empty set**
- The **cardinality** of a set A counts the number of elements; we write |A| to refer to the number of elements in the set A. Sometimes this is also written #A
- A set can contain sets as its elements:
  - {{a,b},{c}}
  - {{{{a},{b}}}}
- A set with exactly one element is called a **singleton**:
  - {a}
  - {true}
  - {{Wouter}}

Question: What is the set $\{\emptyset\}$? What is its cardinality? Is it the same as $\emptyset$?

∅ vs {∅}



Brainteaser

I have two wallets. If I add up the value of all the coins they contain, I have 1 euro. One wallet has twice as many coins as the other. What coins do the wallets contain?

Answer? After the break.

Elements and subsets

Elements

We can write the following propositions about sets:

- If x is an element of the set A, we write $x \in A$
- If x is **not** an element of the set A, we write $x \notin A$

Examples:

- $7 \in \{3,7,12\}$
- $7 \notin \{2,6,11\}$

Inclusion

When all the elements of a set A are also elements of a set B, we say that A is a **subset** of B, written $A \subseteq B$.

More formally: $A \subseteq B$ holds if and only if, for all x

$$x \in A \Rightarrow x \in B$$

Inclusion

When all the elements of a set A are also elements of a set B, we say that A is a **subset** of B, written $A \subseteq B$.

More formally: $A \subseteq B$ holds if and only if, for all x

$$x \in A \Rightarrow x \in B$$

Note how we're using *propositional logic* to describe the relation between two sets.

Equal sets

Two sets A and B are **equal** (written, $A = B$) when both $A \subseteq B$ and $B \subseteq A$

More formally: for all x, $x \in A \Leftrightarrow x \in B$

Question: Are these two sets equal?

- $\{1, 2, 3\}$
- $\{3, 1, 2\}$

Equal sets

Two sets A and B are **equal** (written, $A = B$) when both $A \subseteq B$ and $B \subseteq A$

More formally: for all x, $x \in A \Leftrightarrow x \in B$

Question: Are these two sets equal?

- {1, 2, 3}
- {3, 1, 2}

Question: And what about these two sets?

- {Edam, Gouda, Stolwijk}
- {Gouda, Edam, Gouda, Edam, Stolwijk, Gouda}

Equal sets

Two sets A and B are **equal** (written, $A = B$) when both $A \subseteq B$ and $B \subseteq A$

More formally: for all x, $x \in A \Leftrightarrow x \in B$

Question: Are these two sets equal?

- {1, 2, 3}
- {3, 1, 2}

Question: And what about these two sets?

- {Edam, Gouda, Stolwijk}
- {Gouda, Edam, Gouda, Edam, Stolwijk, Gouda}

The order of elements and number of occurrences do not matter!

Unequal sets

We write $A \not\subseteq B$ when A is not a subset of B; or more formally, $\neg(A \subseteq B)$.

If A and B are not equal, we write $A \neq B$.

If $A \neq B$ and $A \subseteq B$ we write $A \subset B$. Then A is a **strict** subset of B.

Properties of the subset relation

- **Reflexivity** for all sets A, $A \subseteq A$
- **Transitivity** for all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$
- **Anti-symmetry** for all sets A and B, if $A \subseteq B$ and $B \subseteq A$ then $A = B$.
- For any set A, $\emptyset \subseteq A$.

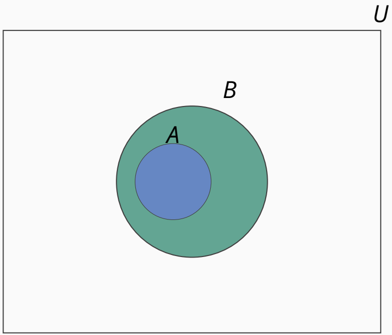
Question: How can we prove these properties?

Venn diagrams and set operations

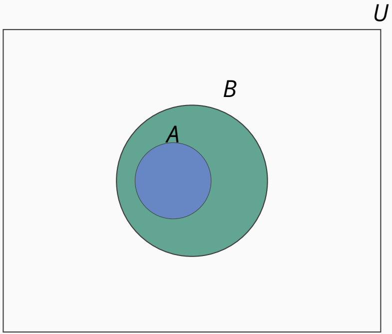
Venn diagrams

Working with formulas can sometimes be a bit confusing.

It can help to **visualize** a relation between sets by drawing a **Venn diagram**:



Venn diagrams

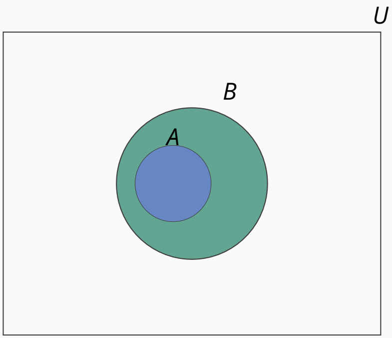


Here we have set U containing all possible elements (the *universe of discourse*).

The set B is a subset of U (here B is drawn in green).

The set A is a subset of B (here A is drawn in blue).

Venn diagrams



In this way, we can refer to the sets corresponding to the different regions of this diagram, such as:

- the elements of B that are not in A;
- the elements in U that are not in A or B;
- etc.

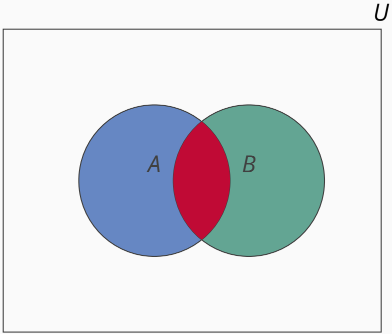
Combining sets

Just as we defined a series of logical operators ($\Rightarrow$, $\wedge$, $\vee$, and $\neg$) to construct more interesting expressions, we can also define operators to construct more interesting sets, such as:

- $A \cap B$
- $A \cup B$
- $A \setminus B$
- $\bar{A}$

We will use familiar logical connectives to describe them and Venn diagrams to visualize them.

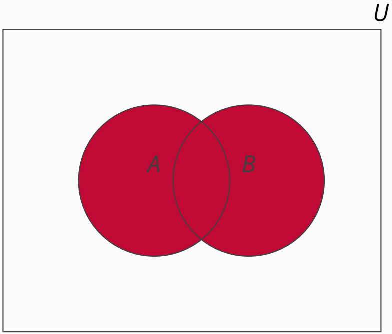
Intersection



The **intersection** of two sets, A and B, consists of those elements that are **both** in A and in B.

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

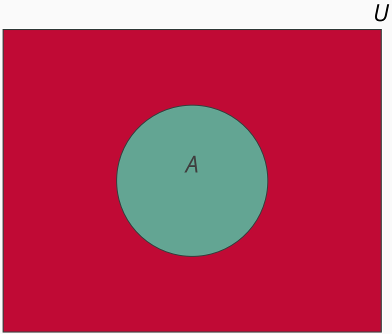
Union



The **union** of two sets, A and B, consists of those elements that are in A **or** in B.

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

Complement

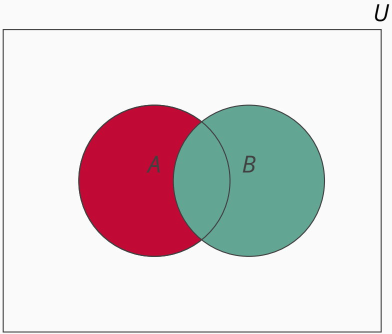


The **complement** of a set A consists of those elements that are **not** in A.

The complement of a set A is written as $\bar{A}$

$$\bar{A} = \{x \ : \ x \notin A\}$$

Difference

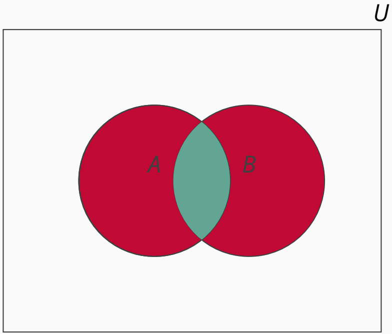


The **difference** of two sets A and B consists of those elements of A that are **not** in B.

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

Question: Is $A \setminus B$ the same as $B \setminus A$? What about $A \cap B$? Or $A \cup B$?

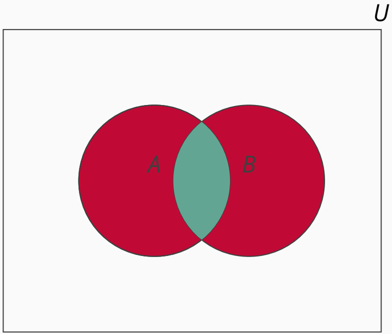
Symmetric difference



The **symmetric difference** of two sets A and B consists of those elements that are **not** in **both** A and B.

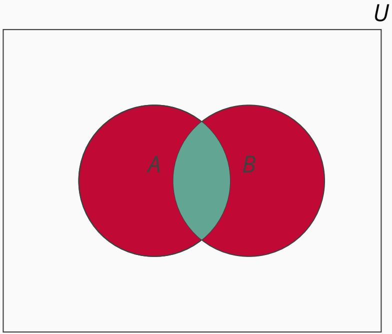
$$A \bigtriangledown B = \{x \ : \ (x \in A \lor x \in B) \land x \notin A \cap B\}$$

Symmetric difference



Question: How can we describe the symmetric difference in terms of the operations we have seen so far?

Symmetric difference

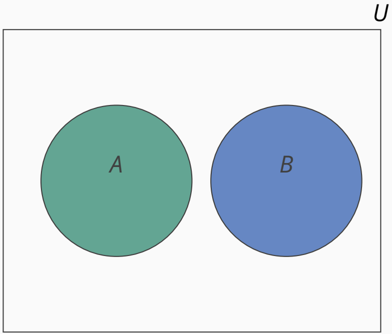


Question: How can we describe the symmetric difference in terms of the operations we have seen so far?

There are many ways to do this:

$(A \setminus B) \cup (B \setminus A)$ or $(A \cup B) \setminus (A \cap B)$ or ...

Disjoint sets



Two sets A and B are called **disjoint** if they do not have any elements in common.

$A \cap B = \emptyset$

Powerset

The **powerset** operation is harder to visualise in a Venn diagram.

For any set A, the **powerset** *P*(A) consists of all possible subsets of A.

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

Example: the powerset of the set {true, false} consists of:

- $\emptyset$
- { true }
- { false }
- {true, false}

Question: If a set A has n elements, how many elements does P(A) have? What is P($\emptyset$)?

Partitions

A **partition** of a set A is a pair of sets A_1 and A_2, such that:

- $A_1 \cup A_2 = A$
- $A_1 \cap A_2 = \emptyset$

Such a partition breaks the original set A into two different pieces, without losing any elements.

Example: We can partition the natural numbers into the sets of even and odd numbers:

- $E = \{ x : x \bmod 2 = 0 \}$
- $O = \{ x : x \bmod 2 = 1 \}$

Since clearly $E \cup O = \mathbb{N}$ and $E \cap O = \emptyset$

Ordered pairs and cartesian products

Given two sets A and B, we can form their **Cartesian product**, A × B, consisting of pairs of an element from A and one from B.

$$A \times B = \{(x, y) \ : \ x \in A \wedge y \in B\}$$

Example: For instance, we can form the familiar 2 dimensional plane by considering all points in $\mathbb{R} \times \mathbb{R}$.

Modelling a black-and-white screen

Suppose we have a black and white computer display with dimensions 1680×1050. We would define a set that describes the possible screen configurations.

One way to model this is to list all the positions of the white pixels. We might write $\{(0,0),(1,0)\}$ for the screen where there are two white pixels at the origin and at position $(1,0)$.

Question: Describe a set containing all possible configurations of this display (and nothing else).

Modelling a black-and-white screen

Suppose we have a black and white computer display with dimensions 1680×1050. We would define a set that describes the possible screen configurations.

One way to model this is to list all the positions of the white pixels. We might write $\{(0,0),(1,0)\}$ for the screen where there are two white pixels at the origin and at position $(1,0)$.

Question: Describe a set containing all possible configurations of this display (and nothing else).

- Let W be the set $\{0,1,\dots,1679\}$;
- Let H be the set $\{0,1,\dots,1049\}$;
- The set $W \times H$ contains all the possible pixels, i.e. the set corresponding to an entirely white screen;
- The powerset $P(W \times H)$ describes all possible subsets, that is, all possible ways to choose the white pixels on this screen.

Example: modelling a black-and-white screen

Suppose we have a black and white computer display with dimensions 1680×1050. We would define a set that describes the possible screen configurations.

Recap

- How would you even start to solve this problem without the material taught in this class?
- The language of sets gives you a precise way to talk about the data your programs manipulate.
- It may seem abstract sometimes –- but these patterns and building blocks pop up again and again.

Modelling with sets

Consider the following three statements:

- All candy has sugar;
- John only eats healthy food;
- No healthy food contains sugar.

How can we model these statements using sets?

Modelling with sets

Consider the following three statements:

- All candy has sugar;
- John only eats healthy food;
- No healthy food contains sugar.

How can we model these statements using sets?

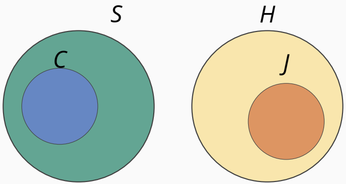
Introduce four sets: C (candy), S (food with sugar), J (food John eats), H (healthy food). The three above statements can be written as:

- $C \subseteq S$
- $J \subseteq H$
- $S \cap H = \emptyset$

Modelling with sets

Introduce four sets: C (candy), S (food with sugar), J (food John eats), H (healthy food). The three above statements can be written as:

- $C \subseteq S$
- $J \subseteq H$
- $S \cap H = \emptyset$



From a Venn diagram like this, it is easy to see that John does not eat candy.

Properties and paradoxes

Properties

Just as we saw last time for propositions, there are many properties relating sets:

Commutativity

- $A \cup B = B \cup A$
- $A \cap B = B \cap A$

Associativity

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

Idempotence

- $A \cup A = A$
- $A \cap A = A$

Properties

Distributivity

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

Double complement

- $(A^c)^c = A$

Empty set laws

- $A \cup \emptyset = A$
- $A \cap \emptyset = \emptyset$

... and many others

Question: How can we prove such a law?

Sets and propositions

Almost all these laws follow from our definition of the operators and the corresponding law for propositional operators.

For example:

$A \cup B$

(by definition of $\cup$)

$= \{ x : x \in A \vee x \in B \}$

(commutativity of $\vee$)

$= \{ x : x \in B \vee x \in A \}\}$

(by definition of $\cup$)

$= B \cup A$

Hence sets and propositional logic have a very similar algebraic structure!

Hold on a minute...

Hold on a minute...

And that's exactly what I'll talk about in the next lecture on *boolean algebra*.

Naive set theory

Georg Cantor (1848--1918)

Naive set theory

This lecture covered what is sometimes called *naive set theory*.

What is so naive about naive set theory?

It is very easy to create problematic sets with the definitions we have seen so far…

The barber

Imagine a village with a barber where no men have beards.

Some villagers shave themselves; others are shaved by the barber.

The barber

Imagine a village with a barber where no men have beards.

Some villagers shave themselves; others are shaved by the barber.

In fact, the barber shaves exactly those men who do **not** shave themselves.

The barber

Imagine a village with a barber where no men have beards.

Some villagers shave themselves; others are shaved by the barber.

In fact, the barber shaves exactly those men who do **not** shave themselves.

Question: Does the barber shave himself?

The barber

Imagine a village with a barber where no men have beards.

Some villagers shave themselves; others are shaved by the barber.

In fact, the barber shaves exactly those men who do **not** shave themselves.

Question: Does the barber shave himself?

The barber both should and should not shave himself we have a **paradox**.

Naive set theoery

What does this have to do with set theory?

We have seen how to build sets in various ways. We might even consider the set of all sets. Or the set of all sets containing themselves; or the set of sets that do not contain themselves:

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

Naive set theoery

What does this have to do with set theory?

We have seen how to build sets in various ways. We might even consider the set of all sets. Or the set of all sets containing themselves; or the set of sets that do not contain themselves:

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

Is $C \in C$? Or is $C \notin C$?

Naive set theoery

What does this have to do with set theory?

We have seen how to build sets in various ways. We might even consider the set of all sets. Or the set of all sets containing themselves; or the set of sets that do not contain themselves:

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

Is $C \in C$? Or is $C \notin C$?

- If $C \in C$, by the definition of C, we have $C \notin C$ – but that is a contradiction!

Naive set theoery

What does this have to do with set theory?

We have seen how to build sets in various ways. We might even consider the set of all sets. Or the set of all sets containing themselves; or the set of sets that do not contain themselves:

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

Is $C \in C$? Or is $C \notin C$?

- If $C \in C$, by the definition of C, we have $C \notin C$ – but that is a contradiction!
- If $C \notin C$, by the definition of C, we know that $C \in C$ – but that also a contradiction!

Naive set theoery

What does this have to do with set theory?

We have seen how to build sets in various ways. We might even consider the set of all sets. Or the set of all sets containing themselves; or the set of sets that do not contain themselves:

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

Is $C \in C$? Or is $C \notin C$?

- If $C \in C$, by the definition of C, we have $C \notin C$ – but that is a contradiction!
- If $C \notin C$, by the definition of C, we know that $C \in C$ – but that also a contradiction!

We have a problem: neither $C \in C$ nor $C \notin C$ holds.

This is known as **Russell's Paradox**.

Russell’s Paradox

Bertrand Russell (1872–-1970)

Russell's Paradox

To avoid Russell's paradox, Bertrand Russell and Alfred Whitehead wrote *Principia Mathematica* the principles of mathematics to try and nail down logic once and for all.

It tried to resolve Russell's Paradox by introducing *ramified type theory*, where there are more restrictions on creating the 'set of all sets'.

Principia Mathematica

$\ast 54{\cdot}43$. $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$$\vdash . \ast 54{\cdot}26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$$

$$[\ast 51{\cdot}231] \qquad \equiv . \iota`x \cap \iota`y = \Lambda .$$

$$[\ast 13{\cdot}12] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$$

$$\vdash . (1) . \ast 11{\cdot}11{\cdot}35 . \supset$$

$$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$$

$$\vdash . (2) . \ast 11{\cdot}54 . \ast 52{\cdot}1 . \supset \vdash . \text{Prop}$$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

A formal proof from Principia Mathematica

Recap

- Set theory is a simple and convenient way to model all kinds of structures that you see in Mathematics and Computer Science.
- The heart of simple set theory is easy to grasp yet surprisingly powerful.
- We can define operations for combining sets and relations between them – such as the subset relation

Problems...

But the definition of the subset relation is not completely formal:

Subsets

We say that $A \subseteq B$ holds if and only if, for all x

$$x \in A \Rightarrow x \in B$$

But in regular propositional logic, we cannot express such a property of *all* elements of A...

Or *no* element of A...

Or *some* element of A...

Problems...

But the definition of the subset relation is not completely formal:

Subsets

We say that $A \subseteq B$ holds if and only if, for all x

$$x \in A \Rightarrow x \in B$$

But in regular propositional logic, we cannot express such a property of *all* elements of A...

Or *no* element of A...

Or *some* element of A...

To do this, we need **predicate logic**...

Material

- Modelling Computing Systems, Chapter 2