

Discrete Mathematics in Computer Science

Sets

Malte Helmert, Gabriele Röger

University of Basel

Important Building Blocks of Discrete Mathematics

- sets
- relations
- functions

Sets

Definition

A **set** is an **unordered collection** of **distinct** objects.

Sets

Definition

A **set** is an **unordered collection** of **distinct** objects.

- **unordered**: no notion of a “first” or “second” object,
e. g. $\{Alice, Bob, Charly\} = \{Charly, Bob, Alice\}$

Sets

Definition

A **set** is an **unordered collection** of **distinct** objects.

- **unordered**: no notion of a “first” or “second” object,
e. g. $\{Alice, Bob, Charly\} = \{Charly, Bob, Alice\}$
- **distinct**: each object contained **at most once**,
e. g. $\{Alice, Bob, Charly\} = \{Alice, Charly, Bob, Alice\}$

Notation

- Specification of sets
 - **explicit**, listing all elements, e. g. $A = \{1, 2, 3\}$
 - **implicit** with **set-builder notation**, specifying a **property** characterizing all elements, e. g. $A = \{x \mid x \in \mathbb{N}_0 \text{ and } 1 \leq x \leq 3\}$,
 $B = \{n^2 \mid n \in \mathbb{N}_0\}$
 - **implicit**, as a **sequence with dots**, e. g. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
 - **implicit** with an **inductive definition**

Notation

- Specification of sets
 - **explicit**, listing all elements, e. g. $A = \{1, 2, 3\}$
 - **implicit** with **set-builder notation**, specifying a **property** characterizing all elements, e. g. $A = \{x \mid x \in \mathbb{N}_0 \text{ and } 1 \leq x \leq 3\}$,
 $B = \{n^2 \mid n \in \mathbb{N}_0\}$
 - **implicit**, as a **sequence with dots**, e. g. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
 - **implicit** with an **inductive definition**
- $e \in M$: e is in set M (an **element** of the set)
- $e \notin M$: e is not in set M

Notation

- Specification of sets
 - **explicit**, listing all elements, e. g. $A = \{1, 2, 3\}$
 - **implicit** with **set-builder notation**, specifying a **property** characterizing all elements, e. g. $A = \{x \mid x \in \mathbb{N}_0 \text{ and } 1 \leq x \leq 3\}$,
 $B = \{n^2 \mid n \in \mathbb{N}_0\}$
 - **implicit**, as a **sequence with dots**, e. g. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
 - **implicit** with an **inductive definition**
- $e \in M$: e is in set M (an **element** of the set)
- $e \notin M$: e is not in set M
- **empty set** $\emptyset = \{\}$

Notation

- Specification of sets
 - **explicit**, listing all elements, e. g. $A = \{1, 2, 3\}$
 - **implicit** with **set-builder notation**, specifying a **property** characterizing all elements, e. g. $A = \{x \mid x \in \mathbb{N}_0 \text{ and } 1 \leq x \leq 3\}$,
 $B = \{n^2 \mid n \in \mathbb{N}_0\}$
 - **implicit**, as a **sequence with dots**, e. g. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
 - **implicit** with an **inductive definition**
- $e \in M$: e is in set M (an **element** of the set)
- $e \notin M$: e is not in set M
- **empty set** $\emptyset = \{\}$

Question: Is it true that $1 \in \{\{1, 2\}, 3\}$?

Special Sets

- **Natural numbers** $\mathbb{N}_0 = \{0, 1, 2, \dots\}$

Special Sets

- **Natural numbers** $\mathbb{N}_0 = \{0, 1, 2, \dots\}$
- **Integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Special Sets

- **Natural numbers** $\mathbb{N}_0 = \{0, 1, 2, \dots\}$
- **Integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- **Positive integers** $\mathbb{Z}_+ = \mathbb{N}_1 = \{1, 2, \dots\}$

Special Sets

- **Natural numbers** $\mathbb{N}_0 = \{0, 1, 2, \dots\}$
- **Integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- **Positive integers** $\mathbb{Z}_+ = \mathbb{N}_1 = \{1, 2, \dots\}$
- **Rational numbers** $\mathbb{Q} = \{n/d \mid n \in \mathbb{Z}, d \in \mathbb{N}_1\}$

Special Sets

- **Natural numbers** $\mathbb{N}_0 = \{0, 1, 2, \dots\}$
- **Integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- **Positive integers** $\mathbb{Z}_+ = \mathbb{N}_1 = \{1, 2, \dots\}$
- **Rational numbers** $\mathbb{Q} = \{n/d \mid n \in \mathbb{Z}, d \in \mathbb{N}_1\}$
- **Real numbers** $\mathbb{R} = (-\infty, \infty)$

Why do we use interval notation?

Why didn't we introduce it before?

Discrete Mathematics in Computer Science

Russell's Paradox

Malte Helmert, Gabriele Röger

University of Basel

Excursus: Barber Paradox

Barber Paradox

In a town there is only one barber,
who is male.

The barber shaves all men in the town,
and only those,
who do not shave themselves.



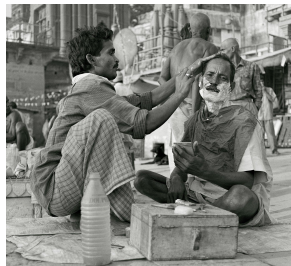
Excursus: Barber Paradox

Barber Paradox

In a town there is only one barber,
who is male.

The barber shaves all men in the town,
and only those,
who do not shave themselves.

Who shaves the barber?



Excursus: Barber Paradox

Barber Paradox

In a town there is only one barber,
who is male.

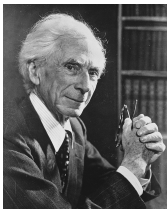
The barber shaves all men in the town,
and only those,
who do not shave themselves.

Who shaves the barber?



We can exploit the self-reference to derive a contradiction.

Russell's Paradox

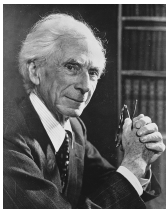


Bertrand Russell

Question

Is the collection of all sets that do not contain themselves as a member a set?

Russell's Paradox



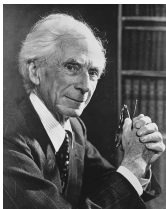
Bertrand Russell

Question

Is the collection of all sets that do not contain themselves as a member a set?

Is $S = \{M \mid M \text{ is a set and } M \notin M\}$ a set?

Russell's Paradox



Bertrand Russell

Question

Is the collection of all sets that do not contain themselves as a member a set?

Is $S = \{M \mid M \text{ is a set and } M \notin M\}$ a set?

Assume that S is a set.

If $S \notin S$ then $S \in S \rightsquigarrow$ Contradiction

If $S \in S$ then $S \notin S \rightsquigarrow$ Contradiction

Hence, there is no such set S .

Discrete Mathematics in Computer Science

Relations on Sets

Malte Helmert, Gabriele Röger

University of Basel

Equality

Definition (Axiom of Extensionality)

Two sets A and B are **equal** (written $A = B$) if every element of A is an element of B and vice versa.

Two sets are equal if they contain the same elements.

Equality

Definition (Axiom of Extensionality)

Two sets A and B are **equal** (written $A = B$) if every element of A is an element of B and vice versa.

Two sets are equal if they contain the same elements.

We write $A \neq B$ to indicate that A and B are **not** equal.

Subsets and Supersets

- $A \subseteq B$: A is a **subset** of B ,
i. e., every element of A is an element of B
- $A \subset B$: A is a **strict subset** of B ,
i. e., $A \subseteq B$ and $A \neq B$.
- $A \supseteq B$: A is a **superset** of B if $B \subseteq A$.
- $A \supset B$: A is a **strict superset** of B if $B \subset A$.

Subsets and Supersets

- $A \subseteq B$: A is a **subset** of B ,
i. e., every element of A is an element of B
- $A \subset B$: A is a **strict subset** of B ,
i. e., $A \subseteq B$ and $A \neq B$.
- $A \supseteq B$: A is a **superset** of B if $B \subseteq A$.
- $A \supset B$: A is a **strict superset** of B if $B \subset A$.

We write $A \not\subseteq B$ to indicate that A is **not** a subset of B .

Analogously: $\not\subset$, $\not\supseteq$, $\not\supset$

Power Set

Definition (Power Set)

The **power set** $\mathcal{P}(S)$ of a set S is the set of all subsets of S .
That is,

$$\mathcal{P}(S) = \{M \mid M \subseteq S\}.$$

Example: $\mathcal{P}(\{a, b\}) =$

Discrete Mathematics in Computer Science

Set Operations

Malte Helmert, Gabriele Röger

University of Basel

Set Operations

Set operations allow us to express sets in terms of other sets

Set Operations

Set operations allow us to express sets in terms of other sets

- **intersection** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$



If $A \cap B = \emptyset$ then A and B are **disjoint**.

Set Operations

Set operations allow us to express sets in terms of other sets

- **intersection** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$



If $A \cap B = \emptyset$ then A and B are **disjoint**.

- **union** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



Set Operations

Set operations allow us to express sets in terms of other sets

- **intersection** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$



If $A \cap B = \emptyset$ then A and B are **disjoint**.

- **union** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



- **set difference** $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$



Set Operations

Set operations allow us to express sets in terms of other sets

- **intersection** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$



If $A \cap B = \emptyset$ then A and B are **disjoint**.

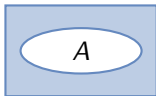
- **union** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



- **set difference** $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$



- **complement** $\bar{A} = B \setminus A$, where $A \subseteq B$ and B is the set of all considered objects (in a given context)



Properties of Set Operations: Commutativity

Theorem (Commutativity of \cup and \cap)

For all sets A and B it holds that

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

Properties of Set Operations: Commutativity

Theorem (Commutativity of \cup and \cap)

For all sets A and B it holds that

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

Question: Is the set difference also commutative,
i. e. is $A \setminus B = B \setminus A$ for all sets A and B ?

Properties of Set Operations: Associativity

Theorem (Associativity of \cup and \cap)

For all sets A, B and C it holds that

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

Properties of Set Operations: Distributivity

Theorem (Union distributes over intersection and vice versa)

For all sets A, B and C it holds that

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

Properties of Set Operations: De Morgan's Law



Augustus De Morgan

British mathematician (1806-1871)

Theorem (De Morgan's Law)

For all sets A and B it holds that

- $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and
- $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

Discrete Mathematics in Computer Science

Finite Sets

Malte Helmert, Gabriele Röger

University of Basel

Cardinality of Sets

The **cardinality** $|S|$ measures the size of set S .

A set is **finite** if it has a finite number of elements.

Definition (Cardinality)

The **cardinality** of a finite set is the **number of elements** it contains.

Cardinality of Sets

The **cardinality** $|S|$ measures the size of set S .

A set is **finite** if it has a finite number of elements.

Definition (Cardinality)

The **cardinality** of a finite set is the **number of elements** it contains.

- $|\emptyset| =$
- $|\{x \mid x \in \mathbb{N}_0 \text{ and } 2 \leq x < 5\}| =$
- $|\{3, 0, \{1, 3\}\}| =$

Cardinality of the Union of Sets

Theorem

For finite sets A and B it holds that $|A \cup B| = |A| + |B| - |A \cap B|$.

Cardinality of the Union of Sets

Theorem

For finite sets A and B it holds that $|A \cup B| = |A| + |B| - |A \cap B|$.

Corollary

If finite sets A and B are *disjoint* then $|A \cup B| = |A| + |B|$.

Cardinality of the Power Set

Theorem

Let S be a finite set. Then $|\mathcal{P}(S)| = 2^{|S|}$.

Proof sketch.

We can construct a subset S' by iterating over all elements e of S and deciding whether e becomes a member of S' or not.

We make $|S|$ independent decisions, each between two options. Hence, there are $2^{|S|}$ possible outcomes.

Every subset of S can be constructed this way and different choices lead to different sets. Thus, $|\mathcal{P}(S)| = 2^{|S|}$. □

Alternative Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

Alternative Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| = n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Alternative Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| = n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Inductive Step ($n \rightarrow n + 1$):

Let S' be an arbitrary set with $|S'| = n + 1$ and let e be an arbitrary member of S' .

Let further $S = S' \setminus \{e\}$ and $X = \{S'' \cup \{e\} \mid S'' \in \mathcal{P}(S)\}$.

Then $\mathcal{P}(S') = \mathcal{P}(S) \cup X$. As $\mathcal{P}(S)$ and X are disjoint and $|X| = |\mathcal{P}(S)|$, it holds that $|\mathcal{P}(S')| = 2|\mathcal{P}(S)|$.

Since $|S| = n$, we can use the IH and get

$$|\mathcal{P}(S')| = 2 \cdot 2^{|S|} = 2 \cdot 2^n = 2^{n+1} = 2^{|S'|}.$$



Enumerating all Subsets

Determine a one-to-one mapping between numbers $0, \dots, 2^{|S|} - 1$ and all subsets of finite set S :

$$S = \{a, b, c\}$$

- Consider the binary representation of numbers $0, \dots, 2^{|S|} - 1$.
- Associate every bit with a different element of S .
- Every number is mapped to the set that contains exactly the elements associated with the 1-bits.

decimal	binary	set
	cba	
0	000	$\{\}$
1	001	$\{a\}$
2	010	$\{b\}$
3	011	$\{a, b\}$
4	100	$\{c\}$
5	101	$\{a, c\}$
6	110	$\{b, c\}$
7	111	$\{a, b, c\}$

Computer Representation as Bit String

Same representation as in enumeration of all subsets:

- **Required:** Fixed universe U of possible elements
- Represent sets as bitstrings of length $|U|$
- Associate every bit with one object from the universe
- Each bit is 1 iff the corresponding object is in the set

Computer Representation as Bit String

Same representation as in enumeration of all subsets:

- **Required:** Fixed universe U of possible elements
- Represent sets as bitstrings of length $|U|$
- Associate every bit with one object from the universe
- Each bit is 1 iff the corresponding object is in the set

Example:

- $U = \{o_0, \dots, o_9\}$
- Associate the i -th bit (0-indexed, from left to right) with o_i
- $\{o_2, o_4, o_5, o_9\}$ is represented as:
0010110001

Computer Representation as Bit String

Same representation as in enumeration of all subsets:

- **Required:** Fixed universe U of possible elements
- Represent sets as bitstrings of length $|U|$
- Associate every bit with one object from the universe
- Each bit is 1 iff the corresponding object is in the set

Example:

- $U = \{o_0, \dots, o_9\}$
- Associate the i -th bit (0-indexed, from left to right) with o_i
- $\{o_2, o_4, o_5, o_9\}$ is represented as:
0010110001

How can the set operations be implemented?