Discrete Mathematics in Computer Science

A2. Sets: Foundations

Malte Helmert, Gabriele Röger

University of Basel

September 23, 2024

A2.1 Sets

Important Building Blocks of Discrete Mathematics

- sets
- relations
- functions

These topics will mainly be the content of part B of the course.

We cover some foundations on sets already now because we will use them for illustrating proof techniques.

Sets

Definition

A set is an unordered collection of distinct objects.

- unorderd: 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. $\{Alice, Bob, Charly\} = \{Alice, Charly, Bob, Alice\}$

German: Menge

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 $1 \in \{\{1, 2\}, 3\}$?

German: Element, leere Menge

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?

German: Natürliche ($\mathbb{N}_0$), ganze ($\mathbb{Z}$), rationale ($\mathbb{Q}$), reelle ($\mathbb{R}$) Zahlen

A2.2 Russell's Paradox

Excursus: Barber Paradox

Barber Paradox

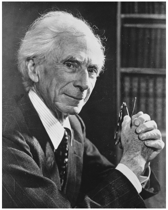
In a town there is only one barber, who is male.

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?

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.

$\rightarrow$ Not every property used in set-builder notation defines a set.

A2.3 Relations on Sets

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 $B \subset A$.

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

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

German: Teilmenge, echte Teilmenge, Obermenge, echte Obermenge

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

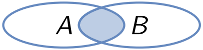
German: Potenzmenge

A2.4 Set Operations

Set Operations

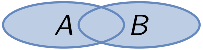
Set operations allow us to express sets in terms of other sets

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

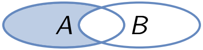


  If $A \cap B = \emptyset$ then A and B are **disjoint**.

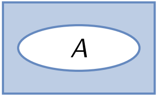
- **union** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



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



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



German: Schnitt, disjunkt, Vereinigung, Differenz, Komplement

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?

German: Kommutativität

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*
- $(A \cap B) \cap C = A \cap (B \cap C)$.

German: Assoziativität

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

German: Distributivität

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

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

A2.5 Cardinality of Finite Sets

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.

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

German: Kardinalität oder Mächtigkeit

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, $|\mathcal{P}(S)| = 2^{|S|}$. □

Summary

- Sets are unordered collections of distinct objects.
- Important set relations: equality ($=$), subset ($\subseteq$), superset ($\supseteq$) and strict variants ($\subset$ and $\supset$)
- The power set of a set S is the set of all subsets of S.
- Important set operations are intersection, union, set difference and complement.
  - Union and intersection are commutative and associative.
  - Union distributes over intersection and vice versa.
  - De Morgan's law for complement of union or intersection.
- The number of elements in a finite set is called its cardinality.