Discrete Mathematics I

Logic and Sets

Juhász Zsófia
jzsofia@inf.elte.hu
(Based on Mérai László's slides in Hungarian)

Department of Computer Algebra

Discrete mathematics

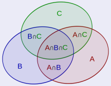
The subfields of Discrete mathematics include:

- Logic
- Set theory
- Combinatorics
- Graph theory
- Number theory
- Algebra
- Cryptography
- Algorithm theory
- Theory of computation
- Information theory
- Game theory
- Discrete geometry
- Operations research
- Probability theory

What do we study in this Course?

Four main topics:

1. **Foundations:** logic, sets, relations

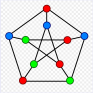


2. **Complex numbers**

$$(\cos t + i*\sin t)^n = \cos n*t + i*\sin n*t$$

3. **Combinatorics**

4. **Graphs**



A little bit of Logic . . .

Logical operations

Statements (or propositions) in logic can be connected by logical operations:

Logical operations

- Negation, notation: $\neg A$.
- And (or conjunction), notation: $A \wedge B$.
- Or (inclusive or or disjunction), notation: $A \vee B$.
- If ... then ... (or implication or conditional), notation: $A \Rightarrow B$.
- ... if and only if ... (or equivalence, biconditional), notation: $A \Leftrightarrow B$.

The logical operations can be defined by their truth tables:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Logical operations: different kinds of 'or'

Just like in everyday language, in logic, different types of **or** are used:

Different types of 'or'

- Inclusive or: $A \vee B$ is true if and only if *at least either of* A and B is true.

  e.g.: 'If you like jazz or rock, join our music club.'

- Exclusive or: $A \oplus B$ is true if and only if *exactly one of* A and B is true.

  e.g.: 'Here we need to turn left or right.'

- Conflicting or: $A||B$ is true if and only if *at most one of* A and B is true.

  e.g.: Drink or drive!'

A	B	$A \vee B$	$A \oplus B$	$A\|\|B$
T	T	T	F	F
T	F	T	T	T
F	T	T	T	T
F	F	F	F	T

Logical operations: implication

In logic, implication ($A \Rightarrow B$) does *not mean causality*: the truth value of $A \Rightarrow B$ depends only on the truth values of A and B.

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

Examples

- $2 \cdot 2 = 4 \Rightarrow i^2 = -1$.
- $2 \cdot 2 = 5 \Rightarrow i^2 = -2$
- $2 \cdot 2 = -3 \Rightarrow$ Dogs are mammals.

A logical operator can be expressed in more than one ways:

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$$

Properties of logical operations

Proposition (Properties of logical operations)

For every proposition A, B and C the following hold:

1. $A \vee A \Leftrightarrow A, \quad A \wedge A \Leftrightarrow A$ *(idempotence)*
2. $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C, \quad A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$ *(associativity)*
3. $(A \vee B) \Leftrightarrow (B \vee A), \quad (A \wedge B) \Leftrightarrow (B \wedge A)$ *(commutativity)*
4. $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C), \quad A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ *(distributivity)*
5. $(A \vee B) \wedge A \Leftrightarrow A, \quad (A \wedge B) \vee A \Leftrightarrow A$ *(absorption laws)*
6. $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B, \quad \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ *(De Morgan's laws)*
7. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ *(law of contrapositive)*
8. $((A \Rightarrow B) \wedge A) \Rightarrow B$ *(modus ponens)*
9. $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ *(syllogism)*
10. $((A \Rightarrow B) \wedge (B \Rightarrow A)) \Leftrightarrow (A \Leftrightarrow B)$

Proof (Example: associativity of $\vee$)

3. $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$

A	B	C	$B \vee C$	$A \vee (B \vee C)$	$A \vee B$	$(A \vee B) \vee C$	$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	T	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	T	T	F	T	T
F	F	F	F	F	F	F	T

Quantifiers

Quantifiers

- $\exists$ (existential quantifier): there exist(s)', 'there is/are'.
- $\forall$ (universal quantifier): '(for) every', '(for) all'.

Examples

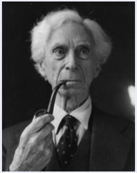
1. $\exists x \in \mathbb{R} : x^2 = 5$
   'There is a real number x such that $x^2 = 5$.'
2. $\forall x \in \mathbb{R} : x^2 \geq 0$
   'For every real number x we have $x^2 \geq 0$'.
3. $\forall n \in \mathbb{Z}\ \exists x \in \mathbb{R} : x > n$
   'For every integer n there exists a real number x such that $x > n$'.

Sets

A famous paradox in naive set theory

Russell's paradox (Bertrand Russell, 1872 - 1970)

Call every set good which is not an element of itself; call every set bad which is an element of itself. Define set A as the set of all good sets.
Is A a good or a bad set?



- A is a good set. $\Rightarrow$ (by the definition of A) A is an element of itself. $\Rightarrow$ A is a bad set. $\lightning$
- A is bad set. $\Rightarrow$ (by the definition of A) A is not an element of itself. $\Rightarrow$ A is a good set. $\lightning$

The possible ways in which sets can be defined need to be restricted and clearly determined. $\Rightarrow$ **Axiomatic set theory:** Zermelo-Fraenkel set theory axioms.

Sets: basics

Basic, undefined concepts (so called predicates) in Set theory:

- Set (Informally we can think of a set as a mental shell around the objects it contains.)
- $\mathbf{x} \in \mathbf{A}$: x is an element of set A (or x belongs to A).

Note: The elements of a set can be any kinds of 'objects', even sets. A set in which all the elements are also sets is sometimes also called a system of sets.

The **axioms** of Set theory define some basic properties of sets which do not need to be proved, but are accepted as true.

Example

Axiom of extensionality

Two sets are equal if and only if they contain exactly the same elements.

Note: An element of a set does not have a 'multiplicity': an object is either an element of a set or not, it cannot be an element twice...

Sets

Defining a (finite) set by listing its elements:
A finite set can be defined by listing its elements between a pair of curly brackets $\{\ \}$. For example:

- $\{a\}$ denotes the set which contains only a single element a and
- $\{a, b\}$ is the set containing exactly the elements a and b (in particular, if $a = b$, then $\{a\} = \{a, b\} = \{b\}$).

  ...

Definition (empty set)

The set which contains no elements is called the empty set and it is denoted by $\emptyset$ or $\{\}$.

Note

- Please note that $\emptyset \neq \{\emptyset\}$!
- By the Axiom of extensionality the empty set is unique.

Subsets of a set

Definition (subset, proper subset)

A set A is called a subset of set B, in notation: $A \subseteq B$, if every element of A is also an element of B, that is if

$$\forall x : x \in A \Rightarrow x \in B.$$

If $A \subseteq B$ and $A \neq B$, then A is a proper subset of B, in notation: $A \subsetneq B$.

Note:

- The empty set is a subset of every set.
- Every set is a subset (but not a proper subset) of itself.

Proposition (Properties of the subset relation; proof is hw)

For every set A, B and C:

1. $A \subseteq A$ *(reflexivity).*
2. $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$ *(transitivity).*
3. $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$ *(anti-symmetry).*

Defining sets using the set builder notation

Axiom schema of specification (**Subset axiom scheme** or **Axiom schema of restricted comprehension**)**:** Let A be a set and $\mathscr{F}(x)$ be a formula (i.e. $\mathscr{F}$ is a 'property' that can be described by precise mathematical terms, i.e. by a formula). Then the collection of all those elements x of A for which $\mathscr{F}(x)$ is true (i.e. which satisfy property $\mathscr{F}$) is a set. This set is denoted as follows:

$$\{x \in A : \mathscr{F}(x)\} = \{x \in A \mid \mathscr{F}(x)\}$$

Note:

- For $\{x \in A : \mathscr{F}(x)\}$ the notations $\{x : x \in A \wedge \mathscr{F}(x)\}$ and $\{x : x \in A, \mathscr{F}(x)\}$ are also commonly used.
- This notation (all the above variants) is often referred to as set builder notation.

Examples

- $\{x \in \mathbb{N} : 3 \leq x < 10\} = \{3, 4, 5, 6, 7, 8, 9\}$.
- $\{n \in \mathbb{Z} : \exists m \, (m \in \mathbb{Z} \wedge n = m^2)\}$: the set of square numbers.

Set operations: set union

Definition (set union)

The union of two sets A and B, denoted by $A \cup B$ is the set consisting of those elements which belong to *at least either of* A *and* B, that is:

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

In general: Let $\mathscr{A}$ be a system of sets (i.e. a set in which the elements are also sets). Then $\bigcup \mathscr{A} = \cup\{A : A \in \mathscr{A}\} = \cup_{A \in \mathscr{A}} A$ is the set of those elements which belong to at least one set in $\mathscr{A}$, that is:

$$\cup \mathscr{A} = \{x \mid \exists A \in \mathscr{A} : x \in A\}.$$

In particular: $A \cup B = \cup\{A, B\}$.

Examples

- $\{a, b, c\} \cup \{b, c, d\} = \{a, b, c, d\}$
- $\bigcup\{\{1, 4, 5\}, \{2, 8\}, \{1, 3\}\} = \{1, 2, 3, 4, 5, 8\}$

Set operations: the properties of set union

Proposition (Properties of set union)

For any sets A, B and C:

1. $A \cup \emptyset = A$
2. $A \cup (B \cup C) = (A \cup B) \cup C$ *(associativity)*
3. $A \cup B = B \cup A$ *(commutativity)*
4. $A \cup A = A$ *(idempotence)*
5. $A \subseteq B \Leftrightarrow A \cup B = B$

Proof

1. $x \in A \cup \emptyset \Leftrightarrow x \in A \vee x \in \emptyset \Leftrightarrow x \in A.$
2. $x \in A \cup (B \cup C) \Leftrightarrow x \in A \vee x \in B \cup C \Leftrightarrow x \in A \vee (x \in B \vee x \in C) \Leftrightarrow (x \in A \vee x \in B) \vee x \in C \Leftrightarrow x \in A \cup B \vee x \in C \Leftrightarrow x \in (A \cup B) \cup C$
3. *Similar.*
4. *Similar.*
5. $\Rightarrow$: $A \subseteq B \Rightarrow A \cup B \subseteq B$, *but* $B \subseteq A \cup B$ *is always true, hence* $A \cup B = B$.
   $\Leftarrow$: *If* $A \cup B = B$, *then all elements of* A *are also elements of* B.

Set operations: set intersection

Definition (set intersection)

The intersection of two sets A and B, denoted by $A \cap B$, is the set containing exactly those elements which are elements of *both* A *and* B:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

In general: Let $\mathscr{A}$ be a system of sets (i.e. a set in which the elements are also sets). Then $\cap\mathscr{A} = \cap\{A : A \in \mathscr{A}\} = \cap_{A\in\mathscr{A}} A$ is defined as:

$$\cap\mathscr{A} = \{x \mid \forall A \in \mathscr{A} : x \in A\}.$$

In particular: $A \cap B = \cap\{A, B\}$.

Examples

- $\{a, b, c\} \cap \{b, c, d\} = \{b, c\}$.
- Let $I_n = \{x \in \mathbb{R} : n \leq x \leq n+1\}$, $\forall\, n \in \mathbb{Z}$ and $\mathscr{I} = \{I_n : n \in \mathbb{Z}\}$. Then
  - $I_2 \cap I_3 = \{3\}$
  - $I_8 \cap I_{11} = \emptyset$
  - $I_n \cap I_{n+1} = \{n+1\}$
  - $\cap\mathscr{I} = \emptyset$

Disjoint and pairwise disjoint systems of sets

Definition ((pairwise) disjoint system of sets)

If $A \cap B = \emptyset$ then A and B are said to be disjoint.
In general: If $\mathscr{A}$ is a system of sets and $\cap\mathscr{A} = \emptyset$, then $\mathscr{A}$ disjoint, or in other words, the elements of $\mathscr{A}$ are disjoint.
If in a system of sets $\mathscr{A}$, any two elements of $\mathscr{A}$ are disjoint, then we say that $\mathscr{A}$ is a pairwise disjoint system of sets, or in other words, the elements of $\mathscr{A}$ are pairwise disjoint.

Examples

- The sets $\{1, 2\}$ and $\{3, 4\}$ are disjoint.
- The sets $\{1, 2\}$, $\{2, 3\}$ and $\{1, 3\}$ are disjoint, but not pairwise disjoint.
- The sets $\{1, 2\}$, $\{3, 4\}$ $\{5, 6\}$ are pairwise disjoint.
- Let $I_n = \{x \in \mathbb{R} : n \leq x \leq n+1\}$, $\forall\, n \in \mathbb{Z}$ and $\mathscr{I} = \{I_n : n \in \mathbb{Z}\}$. Then $\mathscr{I}$ is a disjoint system of sets, but it is not a pairwise disjoint system.

Set operations: the properties of set intersection

Proposition (Properties of set intersection; proof hw)

For any sets A, B *and* C*:*

1. $A \cap \emptyset = \emptyset$
2. $A \cap (B \cap C) = (A \cap B) \cap C$ *(associativity)*
3. $A \cap B = B \cap A$ *(commutativity)*
4. $A \cap A = A$ *(idempotence)*
5. $A \subseteq B \Leftrightarrow A \cap B = A$

Proof

Proof is hw: similar to the proof of the properties of union.

Distributivity of set union and set intersection

Proposition (Distributivity of set union and set intersection)

For any sets A, B and C:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof

1. $x \in A \cap (B \cup C) \Leftrightarrow x \in A \wedge x \in B \cup C \Leftrightarrow$
   $\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Leftrightarrow x \in A \cap B \vee x \in A \cap C \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$
2. *HW. (Similar to 1.)*

Set difference and set complement

Definition (set difference)

The difference of two sets A and B is denoted by $A \setminus B$ and is defined as $A \setminus B = \{x \in A : x \notin B\}$.

Definition (complement of a set)

For a given universal set U and $A \subseteq U$, the complement of A is denoted by $\overline{A} = A'$ and is defined as $\overline{A} = A' = U \setminus A$.

Proposition (Expressing set difference using set complement)

For any sets A and B: $A \setminus B = A \cap \overline{B}$.

Proof

$x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B \Leftrightarrow x \in A \wedge x \in \overline{B} \Leftrightarrow x \in A \cap \overline{B}$

Properties of set complement

Proposition (Properties of set complement; proof hw)

Denote by U the universal set. Then for every set $A, B \subseteq U$ the following hold:

1. $\overline{\overline{A}} = A$;
2. $\overline{\emptyset} = U$;
3. $\overline{U} = \emptyset$;
4. $A \cap \overline{A} = \emptyset$;
5. $A \cup \overline{A} = U$;
6. $A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$;
7. $\overline{A \cap B} = \overline{A} \cup \overline{B}$;
8. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Properties 7 and 8 are called De Morgan's laws.

Proof ($\overline{A \cap B} = \overline{A} \cup \overline{B}$)

7. $x \in \overline{A \cap B} \Leftrightarrow \neg x \in A \cap B \Leftrightarrow \neg(x \in A \wedge x \in B) \Leftrightarrow$
$\Leftrightarrow \neg(x \in A) \vee \neg(x \in B) \Leftrightarrow x \in \overline{A} \vee x \in \overline{B} \Leftrightarrow x \in \overline{A} \cup \overline{B}$

Symmetric difference of sets

Definition (symmetric difference)

The symmetric difference of two sets A and B is denoted by $A \triangle B$ and is defined as

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

.

Proposition (Alternative expression of the symmetric difference; proof HW)

For any sets A and B: $A \triangle B = (A \cup B) \setminus (B \cap A)$.

Power set of a set

Definition (power set)

Let A be a set. The set of all subsets of A is called the power set of A and it is denoted by 2^A or by $\mathscr{P}(A)$.

- $A = \emptyset$, $2^\emptyset = \{\emptyset\}$
- $A = \{a\}$, $2^{\{a\}} = \{\emptyset, \{a\}\}$
- $A = \{a, b\}$, $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Notation: For a finite set A, the number of elements in A is denoted by $|A|$.

Proposition (Size of the power set of a finite set; proof later)

For any finite set A *we have* $|2^A| = 2^{|A|}$.

Appendix: ZF and ZFC

Appendix: Zermelo-Fraenkel axioms of set theory

Note: The Appendix contains the Zermelo-Fraenkel system of axioms and the Axiom of choice. This is not part of the compulsory syllabus, and hence, you will not be assessed on it. It is additional material which you can read optionally if interested.

Axiomatic set theory: Modern set theory is called axiomatic set theory, because it is derived from a set of so called *axioms*, i.e. statements which are accepted as true without proof. The theory is the collection of all theorems that can be inferred from the axioms (using the rules laid out in mathematical logic). There are different axiomatisations of set theory; the most widely used one is the Zermelo-Fraenkel (ZF) set of axioms, often complemented by the Axiom of choice, yielding ZFC.

Predicates in ZF (and ZFC)

The theory has two *predicates*, i.e. undefined basic concepts: that of a *set* and the relation to be an *element of* a set ($\in$).

The axoims describe certain properties of sets, many of them providing methods by which new sets can be constructed based on existing ones.

Zermelo-Fraenkel axioms of set theory

1. **Axiom of extensionality:** Two sets are equal (are the same set) if they have the same elements:

$$\forall x \forall y\, (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$$

2. **Axiom of regularity (or axiom of foundation):** Every nonempty set contains an element that is disjoint from it:

$$\forall x\, (x \neq \emptyset \Rightarrow \exists y (y \in x \wedge y \cap x = \emptyset))$$

3. **Axiom schema of specification (Axiom schema of restricted comprehension):** For any set z and formula φ there exists a set y such that for every set x: x is an element of y if and only if x is an element of z and φ holds for x:

$$\forall z \forall w_1 \forall w_2 \ldots \forall w_n \exists y \forall x\, (x \in y \Leftrightarrow ((x \in z) \wedge \varphi(x, w_1, w_2, ..., w_n, z)))$$

(It is an axiom *schema*, since there is one axiom for each formula φ.)

Zermelo-Fraenkel axioms of set theory continued...

1. **Axiom of pairing:** If x and y are sets, then there exists a set which contains both x and y as elements:

$$\forall x \forall y \exists z ((x \in z) \wedge (y \in z))$$

2. **Axiom of union:** For any set of sets $\mathscr{F}$ there is a set A containing every element that is an element of some element of $\mathscr{F}$:

$$\forall \mathscr{F} \, \exists A \, \forall Y \, \forall x \, ((x \in Y \wedge Y \in \mathscr{F}) \Rightarrow x \in A)$$

3. **Axiom schema of replacement:** The image of a set under any definable function is also a set:

$$\forall w_1, \ldots, w_n \, \forall A \, ((\forall x \in A \, \exists! y \, \varphi(x, y, w_1, \ldots, w_n, A)) \Rightarrow \\ \exists B \, \forall y \, (y \in B \Leftrightarrow \exists x \in A \, \varphi(x, y, w_1, \ldots, w_n, A)))$$

Zermelo-Fraenkel axioms of set theory continued...

1. **Axiom of infinity:** For any set w abbreviate $w \cup \{w\}$, by $S(w)$. (Applying the Axiom of Pairing with $x = y = w$ so that the set z is $\{w\}$ we can see that $\{w\}$ is a set.) Then there exists a set X such that the empty set $\emptyset$ is an element of X and, whenever a set y is an element of X, $S(y)$ is also an element X:

$$\exists X\, (\exists e(\forall z\, \neg(z \in e) \wedge e \in X) \wedge \forall y(y \in X \Rightarrow S(y) \in X))$$

2. **Axiom of the power set:** For any set x, there is a set y that contains every subset of x:

$$\forall x \exists y \forall z (z \subseteq x \Rightarrow z \in y)$$

The above constitute the Zermelo-Fraenkel system of axioms (ZF).

Axiom of choice and ZFC

Adding the Axiom of choice (AC) to ZF we obtain the system of axioms denoted by ZFC:

- **Axiom of choice:** For any set X of nonempty sets there exists a ‚choice' function f which maps each set in X to an element of that set:

$$\forall X \left(\emptyset \notin X \implies \exists f : X \to \bigcup X \quad \forall A \in X \, (f(A) \in A) \right).$$