Foundations of Computing I

Agi Kurucz

- Room S1.17
- *E-mail:* agi.kurucz@kcl.ac.uk
- *URL:* http://www.inf.kcl.ac.uk/staff/kuag/

Course structure

11 weeks, with a reading week in between:

- **Lectures:** 2 hours per week
- **Large tutorials:** 1 hour per week, right after the lectures
- **Small group tutorials:**
  - 1 hour every second week, alternating with SGTs for ELA
  - different times for different groups
  - first SGTs for FC1 are on week 3
- **Assessment:**
  - **Midterm class test (10%):** Wednesday 30 November
  - **Exam (90%):** in January (resit in August)

Course material

- **All** the material needed for a good mark is covered by the lecture slides, tutorial problem sheets, and courseworks.
  Everything is (or will be) available on **KEATS.**

  Please download and print out

  - each package of slides **before** the corresponding lecture
  - each problem sheet **before** the corresponding tutorial
    (answers will be put onto KEATS the following day for LGTs,
    and at the end of the week for SGTs)

- Recommended textbooks:

  K.H. Rosen, *Discrete Mathematics and Its Applications.*
  6th ed., McGraw Hill, 2007. ISBN 9780072880083

  E. Kinber and C. Smith, *Theory of Computing: A Gentle Introduction.*
  Prentice Hall, 2001. ISBN 0130279617

Module assessment

- **Class test (10%):**

  It will be a half an hour multiple-choice test, on Wednesday 30 November. The class is divided to several groups, please check your personal timetable.

  Two mock tests (with solutions) will be provided by midterm.

  As this is the first time the class test is taken, there are no past tests available.

- **Exam (90%):** in January (resit in August).

  There will be 4 questions, carrying equal marks. You'll have to answer 3 of the 4 questions.

  You may find a link to past papers on KEATS. Solutions to some of them will be provided by the end of term.

  A mock exam paper (with solutions) will be provided by the end of term.

  Also, if you put together the 4 optional courseworks, you may obtain another sample exam paper.

Optional coursework

- Submitting the coursework solutions is **NOT compulsory**, the optional courseworks do **NOT** contribute to the module mark.
- **Four** optional courseworks will be given to help you to practice the material. Each coursework is like a question in the January exam paper.
- Their solutions will be published usually **two weeks after** their issue dates, so you will be able to compare your solutions with the given ones.
- Most coursework exercises are such that they can have many different correct solutions, not just the given ones.
- Of course, you are welcome to discuss your solutions with the lecturer or with the TAs. If you want your coursework solutions to be 'marked' as if it were an exam question, you are welcome to submit either a hardcopy or via email to the lecturer **any time during the term.**

FOUNDATIONS?? What is this module for?

- This module attempts to bring the **mathematical** skills of the class to the same level, and to provide the common mathematical background for many of your other modules: data structures, algorithms, databases, compilers, computer security, operating systems, ...
- The module also aims to develop your problem solving skills, and your ability to express yourself in a more precise manner.
- If you had Mathematics A-level: You may find that several parts of the course cover material you already know to some extent, and you might be bored. But please watch out, there can be something new any time.
- If you did NOT have Mathematics A-level: **DON'T PANIC!**
  You are NOT expected to know topics that you have never seen before, everything is developed from scratch.

  And much of Maths A-level is not relevant to this module anyway: say, nowhere in the module will we use differentiation nor any trigonometry.

Learning the material

- You are **NOT** supposed to understand everything during the lectures. (Sorry, but it would be too easy that way.)
  The lecture material is prepared to guide you through the chosen topics.
- The only way to master maths material is by **doing it yourself.**
- During the tutorials right after the lectures, you are expected to work through the provided exercises **yourself.** The exercises are carefully chosen to help your understanding of the introduced concepts. It is often helpful to go through the lecture slides once more in your attempt of solving the exercises. The lecturer and the TAs are in attendance to help you if you have any difficulties, and to discuss your solutions. They are not present to solve the exercises instead of you. The solutions are put onto KEATS the following day.
- More exercises are provided for the small group tutorials, and in the optional courseworks. If you think you need even more, please consult the recommended textbooks. And finally: please **use Google** (there is an extensive amount of online material on the covered topics).

Recommended background reading

- **J.L. Hein,** *Discrete Structures, Logic, and Computability.*
  2nd ed., Jones and Bartlett Publishers, 2002.
  ISBN 0-7637-1843-2

- **R. Johnsonbaugh,** *Discrete Mathematics.*
  7th ed., Pearson Prentice Hall, 2009.
  ISBN 0-13-135430-2

- **D. Makinson,** *Sets, Logic and Maths for Computing.* Springer, 2008.
  ISBN 978-1-84628-844-9

- **H.R. Lewis and C.H. Papadimitriou,** *Elements of the Theory of Computation.*
  2nd ed., Prentice Hall, 1998.
  ISBN 0-13-272741-2

Foundations of computing: topics

- Sets
- Relations
- Functions
- Basic combinatorial principles
- Discrete probability
- Graphs
- Trees
- Finite automata
- Regular languages

Sets: what is a set?

To communicate, we sometimes need to agree on the meaning of certain terms. If the same idea is mentioned several times in a discussion, we often replace it with some new terminology and shorthand notation.

A **set** is a collection of things, any things, called its **elements**.

If S is a set and x is an element in S, then we write

$$\boxed{x \in S}.$$

If x is **not** an element in S, then we write

$$\boxed{x \notin S}.$$

If **both** $x \in S$ **and** $y \in S$, we often denote this fact by the shorthand notation

$$\boxed{x, y \in S}.$$

Describing sets by listing

To describe a set we need to describe its elements in some way.

- The simplest way to describe a set is to **explicitly name its elements**.

  FOR EXAMPLE: We can form a set A by collecting three 'things':
  Cinderella, *Tasmania* and *Tuesday*.

  Any set defined this way is denoted by listing its elements, separated by commas, and surrounding the listing with braces:

$$\boxed{A = \{\textit{Cinderella}, \textit{Tasmania}, \textit{Tuesday}\}}.$$

- **Anything** can be an element of a set.

  In particular, a set can be an element of another set.

  FOR EXAMPLE: The set $B = \{x, \{x, y\}\}$ has two elements:
  - one element is x,
  - and the other element is the set $\{x, y\}$.

  (So we can write $x \in B$ and $\{x, y\} \in B$.)

Important features of sets

The only thing that matters about a set:

what is **IN** it and what is **NOT IN** it.

- **Repeated occurrences of elements don't matter:**

  $\{H, E, L, L, O\}$, $\{H, H, H, E, L, L, O\}$, and $\{H, E, L, O\}$ describe the **same** set (namely, the set having four elements: the letters H, E, L, and O).

  So it is best to be economical and list everything only once: $\{H, E, L, O\}$.

- **The order of listing doesn't matter either:**

  $\{H, E, L, O\}$, $\{E, H, L, O\}$, $\{E, H, O, L\}$, and $\{O, L, E, H\}$

  all describe the **same** set.

Special sets

- The set with no elements is called the **empty set**. The empty set is denoted by $\{\ \}$ or more often by the symbol

$$\boxed{\emptyset}\ .$$

  The empty set has no elements. So no matter what thing x denotes, $x \notin \emptyset$.

  On the other hand, the empty set can be an element of another set.

  FOR EXAMPLE: $\emptyset \in \{a, \emptyset, \mathit{Joe}\}$ or $\emptyset \in \{\emptyset\}$.

- Any set with one element is called a **singleton**.

  FOR EXAMPLE: $\{a\}$ and $\{\mathit{Monday}\}$ are singletons,
  but $\{x, \emptyset\}$ is not.

Equality of sets

Two sets are **equal** if they have the same elements.

We denote the fact that two sets A and B are equal by writing

$$\boxed{A = B}.$$

If the sets A and B are **not equal,** we write

$$\boxed{A \neq B}.$$

FOR EXAMPLE: $\{u, g, h\} = \{h, u, g\}$

$\{a, b, c\} \neq \{a, c\}$

$\{\textit{Monday}\} \neq \emptyset$

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

$\{2\} \neq \{\{2\}\}$

Finite and infinite sets

Suppose we start counting the elements of a nonempty set S, one element per second. If a point of time is reached when all the elements of S have been counted (we might need to have one of our descendants to finish up), then we say that S is **finite**.

If the counting never stops, then S is an **infinite** set.

EXAMPLES OF INFINITE SETS:

- $\mathbf{N} = \{0, 1, 2, 3, \dots\}$ — **natural numbers**,
- $\mathbf{N}^+ = \{1, 2, 3, \dots\}$ — **positive natural numbers**,
- odd natural numbers,
- $\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ — **integers**,
- $\mathbf{Q}$ — the set of **rational numbers**,
- $\mathbf{R}$ — the set of **real numbers**,
- $\mathbf{R}^+$ — the set of **positive real numbers**.

Describing sets by properties

Describing an infinite set by listing, using . . . , might sometimes be possible (like we did with **N**), but even then a bit imprecise.

But listing, say, rational numbers can be quite tricky. Instead of listing elements, we can describe a property that the elements of the set satisfy.

If $\mathcal{P}$ is a property, then the set S whose elements have property $\mathcal{P}$ is denoted by

$$\boxed{S = \{x \mid x \text{ has property } \mathcal{P}\}}.$$

We read this as

"S **is the set of all** x **such that** x **has property** $\mathcal{P}$."

Or, if we also know that all the elements in S come from a larger set A, then we can write

$$\boxed{S = \{x \in A \mid x \text{ has property } \mathcal{P}\}}.$$

Describing sets by properties: an example

Let *Odd* be the set of all odd integers. Then we can describe *Odd* in several ways:

$$\begin{aligned} \mathit{Odd} &= \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\} \\ &= \{x \mid x \text{ is an odd integer}\} \\ &= \{x \in \mathbf{Z} \mid x \text{ is odd}\} \\ &= \{x \mid x = 2k + 1 \text{ for some integer } k\} \\ &= \{x \mid x = 2k + 1 \text{ for some } k \in \mathbf{Z}\} \end{aligned}$$

We can also use expressions for the elements on the left hand side:

$$\begin{aligned} \mathit{Odd} &= \{2k + 1 \mid k \text{ is an integer}\} \\ &= \{2k + 1 \mid k \in \mathbf{Z}\} \end{aligned}$$

Russell's paradox

Not every property is suitable for describing sets. Here is a tricky one.

Let T be the **set** of all sets that are not elements of themselves:

$$T = \{A \mid A \text{ is a set and } A \notin A\}.$$

QUESTION: Is $T \in T$ or not?

Well, either $T \in T$ or $T \notin T$. Let us examine both cases:

- If $T \in T$, then the property we used to describe T must hold for T.
  But then $T \notin T$. So this case is impossible.
- If $T \notin T$, then the property we used to describe T does hold for T.
  So it is not the case that 'T is a set and $T \notin T$.'
  So either T is not a set, or $T \in T$.
  But as T is a set, $T \in T$ follows. So this case is impossible as well.

Describing sets by induction

An inductive description of a set S consists of three steps:

(1) **Basis:**
Specify one or more elements of S.

(2) **Inductive step:**
Give one or more rules to construct new elements of S from existing elements of S.

(3) **Closure:**
State that S consists only of the elements obtained by the basis and inductive steps, nothing else is in S.
(This step is usually assumed rather than stated explicitly.)

Describing sets by induction: examples

- The set **N** of natural numbers can be defined inductively:

  Basis: $0 \in \mathbf{N}$

  Inductive step: If $n \in \mathbf{N}$ then $n + 1 \in \mathbf{N}$.

- The set *Odd* of odd integers can be defined inductively:

  Basis: $1 \in \mathit{Odd}$

  Inductive step: If $n \in \mathit{Odd}$ then $n + 2 \in \mathit{Odd}$ and $n - 2 \in \mathit{Odd}$.

- The set $A = \{3k + 1 \mid k \in \mathbf{N}\}$ can be defined inductively:

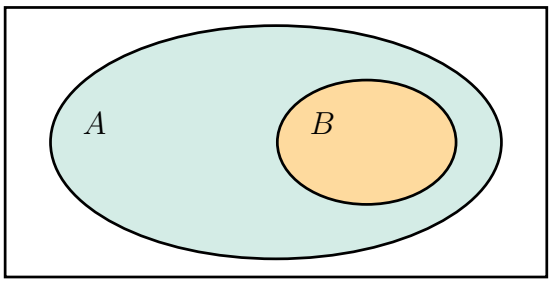
  Basis: $1 \in A$

  Inductive step: If $x \in A$ then $x + 3 \in A$.

Subsets

A set B is a **subset** of a set A, if every element of B is also an element of A.

Notation: $\boxed{B \subseteq A}$.



Venn diagram of $B \subseteq A$

FOR EXAMPLE: $\{a, c\} \subseteq \{a, b, c, d\}$ $\{0, 1, 5\} \subseteq \mathbf{N}$ $\mathbf{N} \subseteq \mathbf{Z}$ $\mathbf{N} \subseteq \mathbf{N}$

- We **always** have, for every set S: $\boxed{S \subseteq S}$ $\boxed{\emptyset \subseteq S}$
- If B is a subset of A, and there is some element in A that is **not** in B, then we say that B is a **proper subset** of A, and write $\boxed{B \subset A}$.
  In other words, $B \subset A$ if $B \subseteq A$ but $B \neq A$.

How to show that $A \subseteq B$?

Let $A = \{x \mid x \text{ is a prime number and } 42 \leq x \leq 51\}$,

$B = \{x \mid x = 4k + 3 \text{ and } k \in \mathbf{N}\}$.

EXERCISE 1: Show that $A \subseteq B$.

SOLUTION: We need to show that for **every** element in A is also in B.
Take some $x \in A$. Then x is a prime number and $42 \leq x \leq 51$.
So either $x = 43$ or $x = 47$.

- We can have $43 = 4 \cdot 10 + 3$. So the choice of $k = 10$ shows that $43 \in B$.
- We can have $47 = 4 \cdot 11 + 3$. So the choice of $k = 11$ shows that $47 \in B$ as well.

Therefore, we have shown that $A \subseteq B$.

EXERCISE 2: Show that $A \subset B$.

SOLUTION: We have just shown that $A \subseteq B$. So it remains **to find an element** $x \in B$ such that $x \notin A$. For example, $x = 3$ is such:

- As $0 \in \mathbf{N}$ and $3 = 4 \cdot 0 + 3$, we have $3 \in B$.
- On the other hand, $42 \not\leq 3$, so we have $3 \notin A$.

How to show that $A \not\subseteq B$?

Let $A = \{3k + 1 \mid k \in \mathbf{N}\}$,

$B = \{4k + 1 \mid k \in \mathbf{N}\}$.

EXERCISE: Show that $A \not\subseteq B$, that is, A is **not** a subset of B.

SOLUTION: We need **to find an element** in $x \in A$ such that $x \notin B$.
For example, $x = 4$ is such:

- $4 = 3 \cdot 1 + 1$. So $k = 1$ shows that $4 \in A$.
- We need to show that $4 \notin B$, that is, there is **no** $k \in \mathbf{N}$ such that $4 = 4k + 1$.
  Let us see. If $k = 0$, then $4k + 1 = 4 \cdot 0 + 1 = 1 \neq 4$.
  If $k \geq 1$, then $4k + 1 \geq 4 \cdot 1 + 1 = 5 > 4$.
  So it is not possible to find a $k \in \mathbf{N}$ such that $4 = 4k + 1$, and so $4 \notin B$.

Therefore, we have shown $A \not\subseteq B$.

How to show whether $A = B$ or $A \neq B$?

$$\boxed{A = B \text{ means that } A \subseteq B \textbf{ and } B \subseteq A.}$$

So:

- If the task is to show that $\boxed{A = B}$,

  then we need to show **BOTH** $\boxed{A \subseteq B}$ **AND** $\boxed{B \subseteq A}$.

- If the task is to show that $\boxed{A \neq B}$,

  then we **EITHER** need **to find an element** in A that is not in B,

  OR to find an element in B that is not in A.

The power set of a set

The **set of all subsets** of a set S is called the **power set of** S which we denote by

$$\boxed{P(S)}.$$

So $P(S) = \{A \mid A \subseteq S\}$.

FOR EXAMPLE:

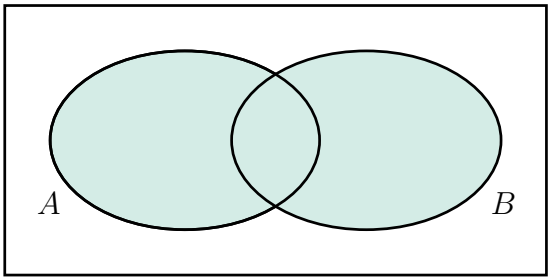
- As for EVERY set S, we always have $\emptyset \subseteq S$ and $S \subseteq S$,
  we always have $\boxed{\emptyset \in P(S)}$ and $\boxed{S \in P(S)}$.
- $P\big(\{u, v, w\}\big) = \big\{\emptyset, \{u\}, \{v\}, \{w\}, \{u, v\}, \{u, w\}, \{v, w\}, \{u, v, w\}\big\}$
- $P\big(\{\textit{Joe}, \textit{Tuesday}\}\big) = \big\{\emptyset, \{\textit{Joe}\}, \{\textit{Tuesday}\}, \{\textit{Joe}, \textit{Tuesday}\}\big\}$
- $P(\mathbf{N}) = \{X \mid X \subseteq \mathbf{N}\}$. So, say, $\{453, 11, 5\} \in P(\mathbf{N})$,
  but $\{3, -1\} \notin P(\mathbf{N})$.

Set operations: union

The **union** of sets A and B is the set

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

$A \cup B$ consists of those elements that are either in A, or in B, or in both.



Venn diagram of $A \cup B$

FOR EXAMPLE: $A = \{4, 7, 8\}$ and $B = \{10, 4, 9\}$.

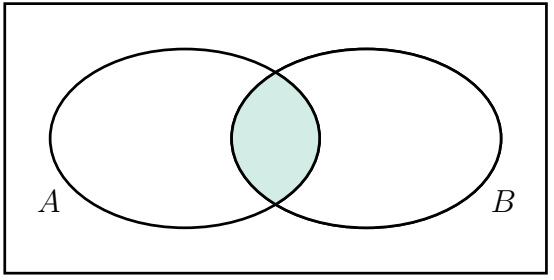
Then $A \cup B = \{4, 7, 8, 9, 10\}$.

Set operations: intersection

The **intersection** of sets A and B is the set

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

$A \cap B$ consists of those elements that are both in A and in B.



Venn diagram of $A \cap B$

FOR EXAMPLE: $A = \{4, 7, 8\}$ and $B = \{10, 4, 9\}$.

Then $A \cap B = \{4\}$.

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

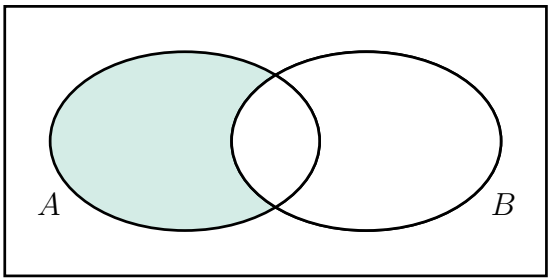
Set operations: difference

The **difference** of sets A and B is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

$A - B$ consists of those elements that are in A but not in B.

$A - B$ is also called the **complement of B with respect to A**.



Venn diagram of $A - B$

FOR EXAMPLE: $A = \{4, 7, 8\}$ and $B = \{10, 4, 9\}$.

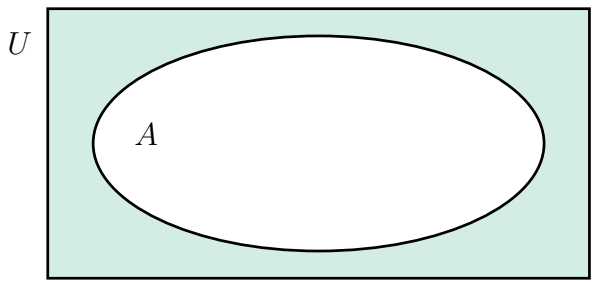
Then $A - B = \{7, 8\}$ and $B - A = \{10, 9\}$.

Set operations: (absolute) complement

In certain contexts we may consider all sets under consideration as being subsets of some given **universal set** U.

Given a universal set U and $A \subseteq U$, the **complement of** A (w.r.t. U) is the set

$$\bar{A} = U - A = \{x \in U \mid x \notin A\}.$$



Venn diagram of $\bar{A}$

Exercise 1.1

Show that, for **any** X, Y and Z, we always have $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

SOLUTION: According to slide 24, we need to show both

(1) $X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z)$ and **(2)** $(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cup Z)$.

Watch out! **It is not enough to give (or draw) some example sets X, Y, Z for which (1) and (2) hold.**

We need to show (1) and (2) using **no** assumptions on the sets X, Y, Z and their elements, using **only** the properties of set operations $\cup$ and $\cap$.

For (1): We need to show that every element of $X \cap (Y \cup Z)$ is also an element of $(X \cap Y) \cup (X \cap Z)$. Take an arbitrary $\text{☺} \in X \cap (Y \cup Z)$. Then both $\text{☺} \in X$ and $\text{☺} \in Y \cup Z$. There are two cases: either $\text{☺} \in Y$ or $\text{☺} \in Z$. In the first case, $\text{☺} \in X \cap Y$. In the second case $\text{☺} \in X \cap Z$. So in either case, $\text{☺} \in (X \cap Y) \cup (X \cap Z)$.

For (2): Take an arbitrary $\text{☹} \in (X \cap Y) \cup (X \cap Z)$. Then there are two cases: either $\text{☹} \in X \cap Y$, or $\text{☹} \in X \cap Z$. In the first case, both $\text{☹} \in X$ and $\text{☹} \in Y$. In the second case, both $\text{☹} \in X$ and $\text{☹} \in Z$. So $\text{☹} \in X$ in both cases, and either $\text{☹} \in Y$ or $\text{☹} \in Z$, depending on the case. Therefore, $\text{☹} \in Y \cup Z$, and so $\text{☹} \in X \cap (Y \cup Z)$.

Exercise 1.2

Show that in general $A \cup \bar{B} \neq \bar{A} \cup B$.

SOLUTION: We need to find and describe **some** sets A and B such that $A \cup \bar{B}$ and $\bar{A} \cup B$ are different sets. There can be many possible solutions, here is one.

Let the universal set be $U = \{1, 2, 3\}$. Let $A = \{1\}$ and $B = \{2\}$.

Then $\bar{A} = \{2, 3\}$ and $\bar{B} = \{1, 3\}$. So $A \cup \bar{B} = \{1, 3\}$ and $\bar{A} \cup B = \{2, 3\}$.

These are two different sets as, for example, $1 \in A \cup \bar{B}$, but $1 \notin \bar{A} \cup B$.