COMP9020

Foundations of Computer Science
COMP9020 17s2 Staff

Lecturer: Paul Hunter
Email: paul.hunter@unsw.edu.au
Consults: To be advised
Research: Theoretical CS: Algorithms, Formal verification

Course admin: Manas Patra
Email: m.patra@unsw.edu.au
Course Aims

“Computer science no more about computers than astronomy is about telescopes”

– E. Dijkstra

The course aims to increase your level of mathematical maturity to assist with the fundamental problem of finding, formulating, and proving properties of programs.
Course Aims

The actual content is taken from a list of subjects that constitute the basis of the tool box of every serious practitioner of computing:

- numbers, sets, words                       week 2
- functions and relations                   weeks 3–4
- graph theory                              week 5
- logic                                     week 6
- induction and recursion                  weeks 7–8
- program analysis                           week 9
- combinatorics                            week 10
- probability and expectation             weeks 11–12
Course Material

All course information is placed on the course website

www.cse.unsw.edu.au/~cs9020/

Lecture slides and Problem Sets (from last semester) are publicly readable.

Textbook:
- KA Ross and CR Wright: Discrete Mathematics

Supplementary textbook:
- E Lehman, FT Leighton, A Meyer: Mathematics for Computer Science
Assessment Summary

60% exam, 30% assignments, 10% quizzes:

- 10 weekly quizzes, worth up to 2 marks each
- 3 assignments, worth up to 10 marks each
- final exam (2 hours) worth up to 60 marks

Quizzes available after lecture, due before next lecture. Assignments due at the end of weeks 5, 9 (after stuvac), 13.

You must achieve 40% on the final exam to pass

Your final score will be taken from your 5 best quiz results, 3 assignments and final exam.
More information

View the course outline at:

www.cse.unsw.edu.au/~cs9020/outline.html

 Particularly the sections on Student conduct and Plagiarism.
COMP9020 Week 2
Session 2, 2017
Numbers, Sets, Alphabets

- Textbook (R & W) - Ch. 1, Sec. 1.1-1.5, 1.7
- Supplementary Exercises Ch. 1 (R & W)
**Notation for Numbers**

**Definition**

Integers $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$

Reals $\mathbb{R}$

$\lfloor . \rfloor : \mathbb{R} \rightarrow \mathbb{Z} \quad \text{— floor of } x, \text{ the greatest integer } \leq x$

$\lceil . \rceil : \mathbb{R} \rightarrow \mathbb{Z} \quad \text{— ceiling of } x, \text{ the least integer } \geq x$

**Example**

$\lfloor \pi \rfloor = 3 = \lceil e \rceil \quad \pi, e \in \mathbb{R}; \quad \lfloor \pi \rfloor, \lceil e \rceil \in \mathbb{Z}$
Simple properties

- \(\lfloor -x \rfloor = -\lfloor x \rfloor\), hence \(\lceil x \rceil = -\lfloor -x \rfloor\)
- \(\lfloor x + t \rfloor = \lfloor x \rfloor + t\) and \(\lceil x + t \rceil = \lceil x \rceil + t\), for all \(t \in \mathbb{Z}\)

Fact

Let \(k, m, n \in \mathbb{Z}\) such that \(k > 0\) and \(m \geq n\). The number of multiples of \(k\) in the interval \([n, m]\) is

\[
\left\lfloor \frac{m}{k} \right\rfloor - \left\lfloor \frac{n - 1}{k} \right\rfloor
\]
Exercise

Examples

1.1.4
(b) $2\lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor = -1$

$2 \lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor = 0$

(d) $\lceil \sqrt{3} \rceil - \lfloor \sqrt{3} \rfloor = 1$; the same for every non-integer

1.1.19(a)
Give $x, y$ s.t. $\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor$

$\lfloor 3\pi \rfloor + \lfloor e \rfloor = 9 + 2 = 11 < 12 = \lfloor 9.42\ldots + 2.71\ldots \rfloor = \lfloor 3\pi + e \rfloor$
Exercise

Examples

1.1.4
(b) \(2 \lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor = -1\)
\[2 \lfloor 0.6 \rfloor - \lfloor 1.2 \rfloor = 0\]
(d) \(\lceil \sqrt{3} \rceil - \lfloor \sqrt{3} \rfloor = 1\); the same for every non-integer

1.1.19(a)
Give \(x, y\) s.t. \(\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor\)
\[\lfloor 3\pi \rfloor + \lfloor e \rfloor = 9 + 2 = 11 < 12 = \lfloor 9.42 \ldots + 2.71 \ldots \rfloor = \lfloor 3\pi + e \rfloor\]
Divisibility

Let \( m, n \in \mathbb{Z} \).

‘\( m \mid n \)’ — \( m \) is a divisor of \( n \), defined by \( n = k \cdot m \) for some \( k \in \mathbb{Z} \)

Also stated as: ‘\( n \) is divisible by \( m \)’, ‘\( m \) divides \( n \)’, ‘\( m \) multiple of \( n \)’

\( m \nmid n \) — negation of \( m \mid n \)

Notion of divisibility applies to all integers — positive, negative and zero.

\( 1 \mid m, -1 \mid m, m \mid m, m \mid -m \), for every \( m \)

\( n \mid 0 \) for every \( n \); \( 0 \nmid n \) except \( n = 0 \)
Numbers $> 1$ divisible only by 1 and itself are called **prime**.

**Greatest common divisor** $\gcd(m, n)$

Numbers $m, n$ s.t. $\gcd(m, n) = 1$ are said to be **relatively prime**.

**Least common multiple** $\text{lcm}(m, n)$

**NB**

$\gcd(m, n)$ and $\text{lcm}(m, n)$ are always taken as positive, even if $m$ or $n$ is negative.

\[
\begin{align*}
\gcd(-4, 6) &= \gcd(4, -6) = \gcd(-4, -6) = \gcd(4, 6) = 2 \\
\text{lcm}(-5, -5) &= \ldots = 5
\end{align*}
\]

**NB**

*Number theory (the study of prime numbers, divisibility etc.) is important in cryptography, for example.*
Absolute Value

\[ |x| = \begin{cases} 
  x & \text{, if } x \geq 0 \\
  -x & \text{, if } x < 0 
\end{cases} \]

Fact

\[ \gcd(m, n) \cdot \text{lcm}(m, n) = |m| \cdot |n| \]
Examples

1.2.2 True or False. Explain briefly.
(a) $n|1$
(b) $n|n$
(c) $n|n^2$

1.2.7(b) $\text{gcd}(0, n) = ?$

1.2.12 Can two even integers be relatively prime?

1.2.9 Let $m, n$ be positive integers.
(a) What can you say about $m$ and $n$ if $\text{lcm}(m, n) = m \cdot n$?
(b) What if $\text{lcm}(m, n) = n$?
Examples

1.2.2 True or False. Explain briefly.
(a) $n|1$ — only if $n = 1$ (for $n \in \mathbb{Z}$ also $n = -1$)
(b) $n|n$ — always
(c) $n|n^2$ — always

1.2.7(b) $\gcd(0, n) = |n|$

1.2.12 Can two even integers be relatively prime? No. (why?)

1.2.9 Let $m, n$ be positive integers.
(a) What can you say about $m$ and $n$ if $\text{lcm}(m, n) = m \cdot n$?
They must be relatively prime since always $\text{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$
(b) What if $\text{lcm}(m, n) = n$?
$m$ must be a divisor of $n$
Examples

1.2.2  True or False. Explain briefly.
(a) $n|1$ — only if $n = 1$ (for $n \in \mathbb{Z}$ also $n = -1$)
(b) $n|n$ — always
(c) $n|n^2$ — always

1.2.7(b) $\gcd(0, n) = |n|$

1.2.12 Can two even integers be relatively prime? No. (why?)

1.2.9 Let $m, n$ be positive integers.
(a) What can you say about $m$ and $n$ if $\text{lcm}(m, n) = m \cdot n$?
   They must be relatively prime since always $\text{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$
(b) What if $\text{lcm}(m, n) = n$?
   $m$ must be a divisor of $n$
Examples

1.2.2 True or False. Explain briefly.
(a) $n|1$ — only if $n = 1$ (for $n \in \mathbb{Z}$ also $n = -1$)
(b) $n|n$ — always
(c) $n|n^2$ — always

1.2.7(b) $\gcd(0, n) = |n|$

1.2.12 Can two even integers be relatively prime? No. (why?)

1.2.9 Let $m, n$ be positive integers.
(a) What can you say about $m$ and $n$ if $\text{lcm}(m, n) = m \cdot n$?
They must be relatively prime since always $\text{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$
(b) What if $\text{lcm}(m, n) = n$?
$m$ must be a divisor of $n$
Euclid’s gcd Algorithm

\[ f(m, n) = \begin{cases} 
m & \text{if } m = n \\
f(m - n, n) & \text{if } m > n \\
f(m, n - m) & \text{if } m < n \\
\end{cases} \]

**Fact**

For \( m > 0, n > 0 \) the algorithm always terminates. (Proof?)

**Fact**

For \( m, n \in \mathbb{Z} \), if \( m > n \) then \( \gcd(m, n) = \gcd(m - n, n) \)

**Proof.**

For all \( d \in \mathbb{Z} \), \( (d|m \text{ and } d|n) \) if, and only if, \( (d|m - n \text{ and } d|n) \):

“⇒”: if \( d|m \text{ and } d|n \) then \( m = a \cdot d \text{ and } n = b \cdot d \), for some \( a, b \) then \( m - n = (a - b) \cdot d \), hence \( d|m - n \)

“⇐”: if \( d|m - n \text{ and } d|n \) then . . . \( d|m \) (why?)
A set is defined by the collection of its elements. Sets are typically described by:
(a) Explicit enumeration of their elements

\[ S_1 = \{a, b, c\} = \{a, a, b, b, b, c\} = \{b, c, a\} = \ldots \text{ three elements} \]

\[ S_2 = \{a, \{a\}\} \text{ two elements} \]

\[ S_3 = \{a, b, \{a, b\}\} \text{ three elements} \]

\[ S_4 = \{\} \text{ zero elements} \]

\[ S_5 = \{\{\}\}\} \text{ one element} \]

\[ S_6 = \{\{\}, \{\{\}\}\}\} \text{ two elements} \]
(b) Specifying the properties their elements must satisfy; the elements are taken from some ‘universal’ domain. A typical description involves a **logical** property $P(x)$

$$S = \{ x : x \in X \text{ and } P(x) \} = \{ x \in X : P(x) \}$$

We distinguish between an element and the set comprising this single element. Thus always $a \neq \{a\}$.
Set $\{\}$ is empty (no elements);
set $\{\{\}\}$ is nonempty — it has one element.
There is only one empty set; only one set consisting of a single $a$;
only one set of all natural numbers.
(c) Constructions from other sets (already defined)

- Union, intersection, set difference, symmetric difference, complement

- **Power set** $\text{Pow}(X) = \{ A : A \subseteq X \}$

- Cartesian product (below)

- Empty set $\emptyset$

  $\emptyset \subseteq X$ for all sets $X$.

$S \subseteq T$ — $S$ is a **subset** of $T$; includes the case of $T \subseteq T$

$S \subset T$ — a **proper** subset: $S \subseteq T$ and $S \neq T$

**NB**

*An element of a set and a subset of that set are two different concepts*

$$a \in \{a, b\}, \quad a \not\in \{a, b\}; \quad \{a\} \subseteq \{a, b\}, \quad \{a\} \not\in \{a, b\}$$
Cardinality

Number of elements in a set $X$ (various notations):

$$|X| = #(X) = \text{card}(X)$$

**Fact**

*Always* $|\text{Pow}(X)| = 2^{|X|}$

- $|\emptyset| = 0$, $\text{Pow}(\emptyset) = \{\emptyset\}$, $|\text{Pow}(\emptyset)| = 1$
- $\text{Pow}(\text{Pow}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$, $|\text{Pow}(\text{Pow}(\emptyset))| = 2$ ... 

- $|\{a\}| = 1$, $\text{Pow}(\{a\}) = \{\emptyset, \{a\}\}$, $|\text{Pow}(\{a\})| = 2$ ... 

- $[m, n]$ — interval of integers; it is empty if $n < m$
- $|[m, n]| = n - m + 1$, for $n \geq m$
Examples

1.3.2 Find the cardinalities of sets

1. $|\left\{ \frac{1}{n} : n \in [1, 4] \right\}| \equiv \ ?$

2. $|\left\{ n^2 - n : n \in [0, 4] \right\}| \equiv \ ?$

3. $|\left\{ \frac{1}{n^2} : n \in \mathbb{P} \text{ and } 2|n \text{ and } n < 11 \right\}| \equiv \ ?$

4. $|\left\{ 2 + (-1)^n : n \in \mathbb{N} \right\}| \equiv \ ?$
Examples

1.3.2 Find the cardinalities of sets

1. $|\left\{ \frac{1}{n} : n \in [1, 4) \right\}| = 4$ — four ‘indices’, no repetitions of values

2. $|\left\{ n^2 - n : n \in [0, 4) \right\}| = 4$ — one ‘repetition’ of value

3. $|\left\{ \frac{1}{n^2} : n \in \mathbb{P} \text{ and } 2|n \text{ and } n < 11 \right\}| = 5$

4. $|\left\{ 2 + (-1)^n : n \in \mathbb{N} \right\}| = 2$ — what are the two elements?
Sets of Numbers

Natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$
Positive integers $\mathbb{P} = \{1, 2, \ldots\}$
Common notation $\mathbb{N}_{>0} = \mathbb{Z}_{>0} = \mathbb{N} \setminus \{0\}$

Integers $\mathbb{Z} = \{\ldots, -n, -(n-1), \ldots, -1, 0, 1, 2, \ldots\}$
Rational numbers (fractions) $\mathbb{Q} = \{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \}$
Real numbers (decimal or binary expansions) $\mathbb{R}$

\[ r = a_1a_2\ldots a_k . b_1b_2\ldots \]

In $\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z}$ different symbols denote different numbers.
In $\mathbb{Q}$ and $\mathbb{R}$ the standard representation is not necessarily unique.
Proper ways to introduce reals include Dedekind cuts and Cauchy sequences, neither of which will be discussed here. Natural numbers etc. are either axiomatised or constructed from sets

\( 0 \overset{\text{def}}{=} \{\} \), \( n + 1 \overset{\text{def}}{=} n \cup \{n\} \)

If we need to emphasise that an object (expression, formula) is defined through an equality we use the symbol \(\overset{\text{def}}{=}\). It denotes that the object on the left is defined by the formula/expression given on the right.
Number sets and their containments

\[ P \subset N \subset Z \subset Q \subset R \]

Derived sets of positive numbers

\[ P = N_{>0} = Z_{>0} = \{ n : n \geq 1 \} \subset Q_{>0} = \{ r : r = \frac{k}{l} > 0 \} \subset R_{>0} \]

Derived sets of integers

\[ 2\mathbb{Z} = \{ 2x : x \in \mathbb{Z} \} \quad \text{the even numbers} \]

\[ 3\mathbb{Z} + 1 = \{ 3x + 1 : x \in \mathbb{Z} \} \]
Intervals of numbers (applies to any type)

\[ [a, b] = \{ x | a \leq x \leq b \}; \quad (a, b) = \{ x | a < x < b \} \]

\[ [a, b] \supseteq [a, b], \quad (a, b) \supseteq (a, b) \]

**NB**

\((a, a) = (a, a) = [a, a) = \emptyset; \text{ however } [a, a] = \{ a \}.\)

Intervals of \(\mathbb{P}, \mathbb{N}, \mathbb{Z}\) are finite: if \(m \leq n\)

\[ [m, n] = \{ m, m + 1, \ldots, n \} \quad |[m, n]| = n - m + 1 \]
Examples

1.3.10 Number of elements in the sets

1. \{−1, 1\}
2. [−1, 1]
3. (−1, 1)
4. \{ n ∈ \mathbb{Z} : −1 ≤ n ≤ 1 \}
### 1.3.10 Number of elements in the sets

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>${-1, 1}$</td>
<td>2</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>$[-1, 1]$</td>
<td>3 (if over $\mathbb{Z}$); $\infty$ (if over $\mathbb{Q}$ or $\mathbb{R}$)</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>$(-1, 1)$</td>
<td>1 (if over $\mathbb{Z}$); $\infty$ (if over $\mathbb{Q}$ or $\mathbb{R}$)</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>${ n \in \mathbb{Z} : -1 \leq n \leq 1 }$</td>
<td>3</td>
</tr>
</tbody>
</table>
Set Operations

Union \( A \cup B \); Intersection \( A \cap B \)

Note that there is a correspondence between set operations and logical operators (to be discussed in Week 6):
One can match set \( A \) with that subset of the universal domain, where the property \( a \) holds, then match \( B \) with the subset where \( b \) holds. Then
\( A \cup B \Leftrightarrow a \) or \( b \);
\( A \cap B \Leftrightarrow a \) and \( b \)

We say that \( A, B \) are disjoint if \( A \cap B = \emptyset \)

NB
\( A \cup B = B \Leftrightarrow A \subseteq B \)
\( A \cap B = B \Leftrightarrow A \supseteq B \)
Other set operations

- $A \setminus B$ — **difference**, set difference, relative complement
  It corresponds (logically) to $a$ but not $b$

- $A \oplus B$ — **symmetric difference**
  \[
  A \oplus B \overset{\text{def}}{=} (A \setminus B) \cup (B \setminus A)
  \]
  It corresponds to $a$ and not $b$ or $b$ and not $a$; also known as xor (exclusive or)

- $A^c$ — set **complement** w.r.t. the ‘universe’
  It corresponds to ‘not $a’
Venn Diagrams

p23–26: are a simple graphical tool to reason about the algebraic properties of set operations.
Laws of Set Operations

Commutativity
\[ A \cup B = B \cup A \]
\[ A \cap B = B \cap A \]

Associativity
\[ (A \cup B) \cup C = A \cup (B \cup C) \]
\[ (A \cap B) \cap C = A \cap (B \cap C) \]

Distribution
\[ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \]
\[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \]

Idempotence
\[ A \cup A = A \]
\[ A \cap A = A \]

Identity
\[ A \cup \emptyset = A \]
\[ A \cap \emptyset = \emptyset \]

Double Complementation
\[ (A^c)^c = A \]

De Morgan laws
\[ (A \cup B)^c = A^c \cap B^c \]
\[ (A \cap B)^c = A^c \cup B^c \]
Examples

1.4.4  \( \Sigma = \{a, b\} \)

(d) All subsets of \( \Sigma \): ?

(e) \(|\text{Pow}(\Sigma)| ?=\n
1.4.7  \( A \oplus A \overset{?}{=} , \quad A \oplus \emptyset \overset{?}{=} \)

1.4.8 Relate the cardinalities \(|A \cup B|, |A \cap B|, |A \setminus B|, |A \oplus B|, |A|, |B|\)
Examples

1.4.4 $\Sigma = \{a, b\}$
(d) All subsets of $\Sigma$: $\emptyset, \{a\}, \{b\}, \{a, b\}$
(e) $|\text{Pow}(\Sigma)| = 4$

1.4.7 $A \oplus A \neq \emptyset, \quad A \oplus \emptyset = A$ for all $A$

1.4.8 Relate the cardinalities

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

hence $|A \cup B| + |A \cap B| = |A| + |B|$

$|A \setminus B| = |A| - |A \cap B|$

$|A \oplus B| = |A| + |B| - 2|A \cap B|$
Cartesian Product

\[ S \times T \overset{\text{def}}{=} \{(s, t) : s \in S, \ t \in T\} \quad \text{where } (s, t) \text{ is an ordered pair} \]

\[ \times_{i=1}^{n} S_i \overset{\text{def}}{=} \{(s_1, \ldots, s_n) : s_k \in S_k, \text{ for } 1 \leq k \leq n\} \]

\[ S^2 = S \times S, \quad S^3 = S \times S \times S, \ldots, \quad S^n = \times_{1}^{n} S, \ldots \]

\[ \emptyset \times S = \emptyset, \text{ for every } S \]

\[ |S \times T| = |S| \cdot |T|, \quad \times_{i=1}^{n} S_i = \prod_{i=1}^{n} |S_i| \]
Formal Languages

\[ \Sigma \] — alphabet, a finite, nonempty set

**Examples (of various alphabets and their intended uses)**

| \( \Sigma = \{a, b, \ldots, z\} \) | for single words (in lower case) |
| \( \Sigma = \{\#, -, a, b, \ldots, z\} \) | for composite terms |
| \( \Sigma = \{0, 1\} \) | for binary integers |
| \( \Sigma = \{0, 1, \ldots, 9\} \) | for decimal integers |

The above cases all have a natural ordering; this is not required in general, thus the set of all Chinese characters forms a (formal) alphabet.
Definition

**word** — any finite string of symbols from $\Sigma$
**empty word** — $\lambda$

Example

$\omega = aba$, $\omega = 01101 \ldots 1$, etc.

$\text{length}(\omega) — \# \text{ of symbols in } \omega$
$\text{length}(aaa) = 3$, $\text{length}(\lambda) = 0$

The only operation on words (discussed here) is **concatenation**, written as juxtaposition $\nu \omega, \omega \nu \omega, ab\omega, \omega b\nu, \ldots$

NB

$\lambda \omega = \omega = \omega \lambda$
$\text{length}(\nu \omega) = \text{length}(\nu) + \text{length}(\omega)$
Notation: $\Sigma^k$ — set of all words of length $k$
We often identify $\Sigma^0 = \{\lambda\}$, $\Sigma^1 = \Sigma$
$\Sigma^*$ — set of all words (of all lengths)
$\Sigma^+$ — set of all nonempty words (of any positive length)

$$\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \ldots; \quad \Sigma^{\leq n} = \bigcup_{i=0}^{n} \Sigma^i$$

$$\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \ldots = \Sigma^* \setminus \{\lambda\}$$

A **language** is a subset of $\Sigma^*$. Typically, only the subsets that can be formed (or described) according to certain rules are of interest. Such a collection of ‘descriptive/formative’ rules is called a **grammar**.

**Examples:** Programming languages, Database query languages
Examples

1.3.10 Number of elements in the sets (cont’d)

(e) \( \Sigma^* \) where \( \Sigma = \{a, b, c\} \) \( \rightarrow \) \( |\Sigma^*| = \infty \)

(f) \( \{ \omega \in \Sigma^* : \text{length}(\omega) \leq 4 \} \) where \( \Sigma = \{a, b, c\} \)

\[ |\Sigma_{\leq 4}| = 3^0 + 3^1 + \ldots + 3^4 = \frac{3^5 - 1}{3 - 1} = \frac{243 - 1}{2} = 121 \]
Examples

1.3.10 Number of elements in the sets (cont’d)

(e) $\Sigma^*$ where $\Sigma = \{a, b, c\}$ — $|\Sigma^*| = \infty$

(f) $\{ \omega \in \Sigma^* : \text{length}(\omega) \leq 4 \}$ where $\Sigma = \{a, b, c\}$
$|\Sigma^{\leq 4}| = 3^0 + 3^1 + \ldots + 3^4 = \frac{3^5-1}{3-1} = \frac{243-1}{2} = 121$
Functions

We deal with functions as a set-theoretic concept, it being a special kind of correspondence (between two sets) $f : S \rightarrow T$ describes pairing of the sets: it means that $f$ assigns to every element $s \in S$ a unique element $t \in T$. To emphasise that a specific element is sent, we can write $f : x \mapsto y$, which means the same as $f(x) = y$

$S$ — **domain** of $f$, symbol: $\text{Dom}(f)$

$T$ — **codomain** of $f$, symbol: $\text{Codom}(f)$

$\{ f(x) : x \in \text{Dom}(f) \}$ — **image** of $f$, symbol: $\text{Im}(f)$

$$\text{Im}(f) \subseteq \text{Codom}(f)$$

We observe that every function maps its domain **into** its codomain, but only **onto** its image.
Examples

1.5.3 Regarding \( \text{length} : \{a, b\}^* \rightarrow \mathbb{N} \)
(c) \( \text{length}(\lambda) \)?
(d) \( \text{Im}(\text{length}) \)?

1.5.4 \( \Sigma^* \) as above and \( g(n) \overset{\text{def}}{=} \{ \omega \in \Sigma^* : \text{length}(\omega) \leq n \}, \ n \in \mathbb{N} \)
Here \( g(n) \) is a function that has a complex object as its value for any given argument — it maps \( \mathbb{N} \) into \( \text{Pow}(\Sigma^*) \)
(a) \( g(0) \)?
(b) \( g(1) \)?
(c) \( g(2) \)?
(d) Are all \( g(n) \) finite?
Examples

1.5.3 Regarding $\text{length}: \{a, b\}^* \rightarrow \mathbb{N}$
(c) $\text{length}(\lambda) = 0$
(d) $\text{Im}(\text{length}) = \mathbb{N}$

1.5.4 $\Sigma^*$ as above and $g(n) \overset{\text{def}}{=} \{ \omega \in \Sigma^* : \text{length}(\omega) \leq n \}, \ n \in \mathbb{N}$
Here $g(n)$ is a function that has a complex object as its value for any given argument — it maps $\mathbb{N}$ into $\text{Pow}(\Sigma^*)$
(a) $g(0) = \{ \lambda \}$
(b) $g(1) = \{ \lambda, a, b \}$
(c) $g(2) = \{ \lambda, a, b, aa, ab, ba, bb \}$
In general $g(n) = \bigcup_{i=0}^{n} \Sigma^i = \Sigma^{\leq n}$
(d) Are all $g(n)$ finite?
Yes; $|g(n)| = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$
Examples

1.5.3 Regarding \( \text{length} : \{a, b\}^* \rightarrow \mathbb{N} \)
(c) \( \text{length}(\lambda) = 0 \)
(d) \( \text{Im}(\text{length}) = \mathbb{N} \)

1.5.4 \( \Sigma^* \) as above and \( g(n) \overset{\text{def}}{=} \{ \omega \in \Sigma^* : \text{length}(\omega) \leq n \} \), \( n \in \mathbb{N} \)
Here \( g(n) \) is a function that has a complex object as its value for any given argument — it maps \( \mathbb{N} \) into \( \text{Pow}(\Sigma^*) \)
(a) \( g(0) = \{\lambda\} \)
(b) \( g(1) = \{\lambda, a, b\} \)
(c) \( g(2) = \{\lambda, a, b, aa, ab, ba, bb\} \)
In general \( g(n) = \bigcup_{i=0}^{n} \Sigma^i = \Sigma^{\leq n} \)
(d) Are all \( g(n) \) finite?
Yes; \( |g(n)| = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1 \)
(e) Give an example of a set in $\text{Pow}(\Sigma^*)$ that is not in $\text{Im}(g)$

1.5.6 Regarding $\text{gcd} : \mathbb{P} \times \mathbb{P} \rightarrow \mathbb{P}$

(c) $\text{Im}(\text{gcd}) = \mathbb{P}$

1.5.7

$$f(x) = \begin{cases} x^3 & x \geq 1 \\ x & 0 \leq x < 1 \\ -x^3 & x < 0 \end{cases}$$

(c) $\text{Im}(f) = \mathbb{P}$
Examples (cont’d)

(e) Give an example of a set in \( \text{Pow}(\Sigma^*) \) that is not in \( \text{Im}(g) \)

1.5.6 Regarding \( \text{gcd} : \mathbb{P} \times \mathbb{P} \rightarrow \mathbb{P} \)

(c) \( \text{Im}(\text{gcd}) \) is

1.5.7

\[
f(x) = \begin{cases} 
  x^3 & x \geq 1 \\
  x & 0 \leq x < 1 \\
  -x^3 & x < 0 
\end{cases}
\]

(c) \( \text{Im}(f) \) is
Examples (cont’d)

(e) Give an example of a set in $\text{Pow}(\Sigma^*)$ that is not in $\text{Im}(g)$
   - any infinite subset of $\Sigma^*$ (infinite language)
   - any finite language that excludes some intermediate length words, e.g. $\{\lambda, a\}$, $\{a, b\}$, $\{\lambda, a, aa\}$, ...

1.5.6 Regarding $\gcd : \mathbb{P} \times \mathbb{P} \rightarrow \mathbb{P}$
(c) $\text{Im}(\gcd) = \mathbb{P}$ as $\gcd(n, n) = n$

1.5.7

$$f(x) = \begin{cases} 
  x^3 & x \geq 1 \\
  x & 0 \leq x < 1 \\
  -x^3 & x < 0 
\end{cases}$$

(c) $\text{Im}(f) = \mathbb{R}_{\geq 0}$
Examples (cont’d)

(e) Give an example of a set in $\text{Pow}(\Sigma^*)$ that is not in $\text{Im}(g)$
- any infinite subset of $\Sigma^*$ (infinite language)
- any finite language that excludes some intermediate length words, e.g. $\{\lambda, a\}, \{a, b\}, \{\lambda, a, aa\}, \ldots$

1.5.6 Regarding $\gcd : \mathbb{P} \times \mathbb{P} \rightarrow \mathbb{P}$

(c) $\text{Im}(\gcd) = \mathbb{P}$ as $\gcd(n, n) = n$

1.5.7

$$f(x) = \begin{cases} 
  x^3 & x \geq 1 \\
  x & 0 \leq x < 1 \\
  -x^3 & x < 0 
\end{cases}$$

(c) $\text{Im}(f) = \mathbb{R}_{\geq 0}$
Composition of Functions

Auxiliary notation

\[ f : x \mapsto y, \quad f : A \mapsto B \]

The former means that \( x \) is mapped to \( y \); the latter means that \( B \) is the image of \( A \) under \( f \).

**NB**

*Observe the difference between \( \mapsto \) and \( \mapsto \)*

Composition of functions is described as

\[ g \circ f : x \mapsto g(f(x)), \quad \text{requiring } \text{Im}(f) \subseteq \text{Dom}(g) \]
If a function maps a set into itself, i.e. when $\text{Dom}(f) = \text{Codom}(f)$ (and thus $\text{Im}(f) \subseteq \text{Dom}(f)$), the function can be composed with itself — iterated

$$f \circ f, f \circ f \circ f, \ldots,$$

also written $f^2, f^3, \ldots$

Composition is associative

$$h \circ (g \circ f) = (h \circ g) \circ f,$$

can write $h \circ g \circ f$

**Identity** function on $S$

$$\text{Id}_S(x) = x, x \in S; \text{Dom}(i) = \text{Codom}(i) = \text{Im}(i) = S$$

For $g : S \to T$ $g \circ \text{Id}_S = g$, $\text{Id}_T \circ g = g$
gcd Example

Reconsider gcd as a **higher-order function**, defined by

\[
gcd(f)(m, n) = \begin{cases} 
    m & \text{if } m = n \\
    f(m - n, n) & \text{if } m > n \\
    f(m, n - m) & \text{if } m < n 
\end{cases}
\]

Its type is now \( \text{gcd} : (\mathbb{P}^2 \rightarrow \mathbb{P}) \rightarrow (\mathbb{P}^2 \rightarrow \mathbb{P}) \) that is, it maps each partial function (from pairs of positive integers to a positive integer) to a (partial) function of the same type. The worst such function is the “nowhere defined” function

\[
f_{\perp}(m, n) = \perp.
\]

**NB**

A **partial function** \( f : S \twoheadrightarrow T \) is a function \( f : S' \rightarrow T \) for \( S' \subseteq S \).
gcd Example cont’d

Consider the sequence

\[ f_\bot, \gcd(f_\bot), \gcd(\gcd(f_\bot)), \ldots, \gcd(\gcd(\ldots (f_\bot) \ldots)), \ldots \]

and observe that the \(i\)'th element of this sequence is an approximation of the \(\gcd\) function that works as long as the depth of the recursion is less than \(i - 1\). Since we proved that the original \(\gcd\) function terminates, we can deduce that the limit of this sequence exists, and is the original \(\gcd\). It also is the least fixpoint of \(\gcd\) i.e. the “simplest” solution \(f\) to the equation \(f = \gcd(f)\).

This, in a nutshell, explains how the semantics of recursive procedures is defined in CS. How all this works is somewhat beyond the scope of COMP9020 but still serves the purpose of motivating why we discuss functions and their composition, iteration.
Supplementary Exercises

1.8.2(b) When is \((A \setminus B) \setminus C = A \setminus (B \setminus C)\)?

1.8.9 How many third powers are \(\leq 1,000,000\) and end in 9? (Solve without calculator!)
1.8.2(b) When is \((A \setminus B) \setminus C = A \setminus (B \setminus C)\)?

From Venn diagram
\[(A \setminus B) \setminus C = A \cap B^c \cap C^c; \quad A \setminus (B \setminus C) = (A \cap B^c) \cup (A \cap C)\].

Equality would require that \(A \cap C \subseteq A \cap B^c \cap C^c\); however, these two sets are disjoint, thus \(A \cap C = \emptyset\) is a necessary condition for the equality.

One verifies that \(A \cap C = \emptyset\) is also a sufficient condition and that, in this case, both set expressions simplify to \(A \setminus B\).

1.8.9 How many third powers are \(\leq 1,000,000\) and end in 9? (Solve without calculator!)

\(n^3 = 9 \pmod{10}\) only when \(n = 9 \pmod{10}\), and \(n^3 \leq 1,000,000\) when \(n \leq 100\). Hence all such \(n\) are 9, 19, \ldots, 99.

Try the same question for \(n^4\).
Summary

- Notation for numbers
  \[ [m], \lfloor m \rfloor, m|n, |a|, [a, b], (a, b), \gcd, \lcm \]
- Sets and set operations
  \[ |A|, \in, \cup, \cap, \setminus, \oplus, A^c, \Pow(A), \subseteq, \subset, \times \]
- Formal languages: alphabets and words
  \[ \lambda, \Sigma^*, \Sigma^+, \Sigma^1, \Sigma^2, \ldots \]
- Functions
  (co-)domain, image, composition \( f \circ g \)