COMP9020 Week 1
Session 1, 2018
Numbers, Sets, Alphabets

- Textbook (R & W) - Ch. 1, Sec. 1.1-1.5, 1.7
- Problem set 1
- Supplementary Exercises Ch. 1 (R & W)

COMP9020 18s1 Course Convenor

Name:	Michael Thielscher
Email:	mit@unsw.edu.au
Consults:	Thu 4:00-5:00pm Fri 12:00-1:00pm
	Room: K17 401J/K K17 401J
Research:	Artificial Intelligence, Robotics, General Game Playing
Pastimes:	Fiction, Films, Food, Football
Admin:	Michael Schofield
Email:	michael.schofield@unsw.edu.au

Course Aims

The course aims to increase your level of mathematical maturity to assist with the fundamental problem of **finding, formulating, and proving** properties of programs.
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 1
- logic — week 2–3
- function and relation theory — week 4, 6

- graph theory — week 7
- induction and recursion — week 8
- program analysis — week 9
- combinatorics, probability, expectation — week 10–12

Course Material

All course information is placed on the WebCMS3 course website

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

Need to login to access course materials.

Textbook:

- KA Ross and CR Wright: Discrete Mathematics

Supplementary textbook:

- E Lehman, FT Leighton, A Meyer:
  Mathematics for Computer Science

Lectures, Problem Sets

Lectures will:

- present theory
- demonstrate problem-solving methods

Lecture slides will be made available before lecture

Feel free to ask questions, but No Idle Chatting

The **weekly homework** aims to:

- clarify any problems with lecture material
- work through exercises related to lecture topics

Problem sets available on web at the time of the lecture

Sample solutions will be posted in the following week
Do them yourself! and Don't fall behind!
NB: Quizzes may refer to the current homework!

Assessment Summary

1. quizzes (due weeks 3, 5, 7, 9, 11, 13) — max. marks 20
2. mid-term test (45 mins in week 6) — max. marks 20
3. final exam (2 hours in the exam period) — max. marks 60

NB

Your final mark for this course will be the **maximum** *of*

- *quizzes + mid-term + final*
- *quizzes + 80*(final/60)*
- *mid-term + 80*(final/60)*
- *100*(final/60)*

$\Rightarrow$ If you do better in the final exam, your quizzes and/or mid-term test result will be ignored
$\Rightarrow$ The quizzes and mid-term test can only improve your final mark

The online quizzes are:

- released after the lectures in weeks 2, 4, 6, 8, 10, 12
- due **Thursdays, 11:59pm** in weeks 3, 5, 7, 9, 11, 13

You get your own individual 8 questions for each quiz.

- each correct answer is worth 0.5 marks
  $\Rightarrow$ max. marks per quiz = 4
- total quiz mark obtained by taking **your 5 best quiz marks**
  $\Rightarrow$ max. total quiz mark = 20

NB

To pass the course, your final overall mark must be 50 or higher **and** *your mark for the final exam must be 25 or higher.*

Students who do not meet these requirements but achieve an overall score $\geq$47 can sit the supplementary exam, in which they have to achieve a mark $\geq$50 to pass with a final mark of 50.

Notation for Numbers

Definition

Integers $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$
Reals $\mathbb{R}$
$\lfloor . \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ — **floor** of x, the greatest integer $\leq x$
$\lceil . \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$ — **ceiling** of x, the least integer $\geq x$

Example

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

Simple properties

- $\lfloor -x \rfloor = -\lceil x \rceil$, 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

$\boxed{1.1.4}$

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

$2\lceil 0.6 \rceil - \lceil 1.2 \rceil = 0$

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

$\boxed{1.1.19(a)}$

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

$\boxed{1.1.4}$

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

$2\lceil 0.6 \rceil - \lceil 1.2 \rceil = 0$

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

$\boxed{1.1.19(a)}$

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 $m, n \in \mathbb{Z}$.
'$m|n$' — 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'~~ 'n multiple of m'

$m \nmid n$ — negation of $m|n$

Notion of divisibility applies to all integers — positive, negative and zero.
$1|m$, $-1|m$, $m|m$, $m|-m$, for every m
$n|0$ 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.

$$\begin{aligned} \gcd(-4, 6) = \gcd(4, -6) = \gcd(-4, -6) = \gcd(4, 6) &= 2 \\ \text{lcm}(-5, -5) = \ldots &= 5 \end{aligned}$$

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

$\boxed{1.2.2}$ *True* or *False*. Explain briefly.
(a) $n|1$
(b) $n|n$
(c) $n|n^2$

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

$\boxed{1.2.12}$ Can two even integers be relatively prime?

$\boxed{1.2.9}$ 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

$\boxed{1.2.2}$ *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

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

$\boxed{1.2.12}$ Can two even integers be relatively prime? No. (why?)

$\boxed{1.2.9}$ 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 $d \in \mathbb{Z}$, ($d|m$ and $d|n$) if, and only if, ($d|m-n$ and $d|n$):
"$\Rightarrow$": if $d|m$ and $d|n$ then $m = a \cdot d$ and $n = b \cdot d$, for some a, b
then $m - n = (a-b) \cdot d$, hence $d|m-n$
"$\Leftarrow$": if $d|m-n$ and $d|n$ then $\ldots$ $d|m$ (why?)

Sets

A set is defined by the collection of its elements.
Sets are typically described by:
(a) Explicit enumeration of their elements

$$\begin{aligned} S_1 &= \{a,b,c\} = \{a,a,b,b,b,c\} \\ &= \{b,c,a\} = \ldots \quad \text{three elements} \\ S_2 &= \{a,\{a\}\} \quad \text{two elements} \\ S_3 &= \{a,b,\{a,b\}\} \quad \text{three elements} \\ S_4 &= \{\} \quad \text{zero elements} \\ S_5 &= \{\{\{\}\}\} \quad \text{one element} \\ S_6 &= \{\,\{\},\{\{\}\}\,\} \quad \text{two elements} \end{aligned}$$

(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** $\mathrm{Pow}(X) = \{\, A : A \subseteq X \,\}$
- 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

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

Cardinality

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

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

Fact

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

$|\emptyset| = 0 \qquad \mathrm{Pow}(\emptyset) = \{\emptyset\} \qquad |\mathrm{Pow}(\emptyset)| = 1$
$\mathrm{Pow}(\mathrm{Pow}(\emptyset)) = \{\emptyset, \{\emptyset\}\} \qquad |\mathrm{Pow}(\mathrm{Pow}(\emptyset))| = 2 \quad \ldots$

$|\{a\}| = 1 \qquad \mathrm{Pow}(\{a\}) = \{\emptyset, \{a\}\} \qquad |\mathrm{Pow}(\{a\})| = 2 \quad \ldots$

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

Examples

$\boxed{1.3.2}$ Find the cardinalities of sets

1. $|\{\ \frac{1}{n} : n \in [1, 4]\ \}| \stackrel{?}{=}$
2. $|\{\ n^2 - n : n \in [0, 4]\ \}| \stackrel{?}{=}$
3. $|\{\ \frac{1}{n^2} : n \in \mathbb{P}$ and $2|n$ and $n < 11\ \}| \stackrel{?}{=}$
4. $|\{\ 2 + (-1)^n : n \in \mathbb{N}\ \}| \stackrel{?}{=}$

Examples

$\boxed{1.3.2}$ Find the cardinalities of sets

1. $|\{\ \frac{1}{n} : n \in [1, 4]\ \}| = 4$ — four 'indices', no repetitions of values
2. $|\{\ n^2 - n : n \in [0, 4]\ \}| = 4$ — one 'repetition' of value
3. $|\{\ \frac{1}{n^2} : n \in \mathbb{P}$ and $2|n$ and $n < 11\ \}| = 5$
4. $|\{\ 2 + (-1)^n : n \in \mathbb{N}\ \}| = 2$ — 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) $\mathbb{R}$
$r = a_1 a_2 \ldots a_k \,.\, b_1 b_2 \ldots$

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.

NB

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 ($0 \stackrel{def}{=} \{\}$, $n+1 \stackrel{def}{=} n \cup \{n\}$)

NB

If we need to emphasise that an object (expression, formula) is defined through an equality we use the symbol $\stackrel{def}{=}$*. It denotes that the object on the left is defined by the formula/expression given on the right.*

Number sets and their containments

$$\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Derived sets of positive numbers

$$\mathbb{P} = \mathbb{N}_{>0} = \mathbb{Z}_{>0} = \{n : n \geq 1\} \subset \mathbb{Q}_{>0} = \{r : r = \tfrac{k}{l} > 0\} \subset \mathbb{R}_{>0}$$

Derived sets of integers

$$2\mathbb{Z} = \{\ 2x : x \in \mathbb{Z}\ \} \qquad \text{the even numbers}$$
$$3\mathbb{Z} + 1 = \{\ 3x + 1 : x \in \mathbb{Z}\ \}$$

Intervals of numbers (applies to any type)

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

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

NB

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

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

$$[m, n] = \{m, m+1, \ldots, n\} \qquad |[m, n]| = n - m + 1$$

Examples

$\boxed{1.3.10}$ Number of elements in the sets

1. $\{-1, 1\}$
2. $[-1, 1]$
3. $(-1, 1)$
4. $\{\ n \in \mathbb{Z} :\ -1 \leq n \leq 1\ \}$

Examples

$\boxed{1.3.10}$ Number of elements in the sets

1. $\{-1, 1\}$ — 2
2. $[-1, 1]$ — 3 (if over $\mathbb{Z}$); ∞ (if over $\mathbb{Q}$ or $\mathbb{R}$)
3. $(-1, 1)$ — 1 (if over $\mathbb{Z}$); ∞ (if over $\mathbb{Q}$ or $\mathbb{R}$)
4. $\{\, n \in \mathbb{Z} : -1 \leq n \leq 1 \,\}$ — 3

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 3):
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

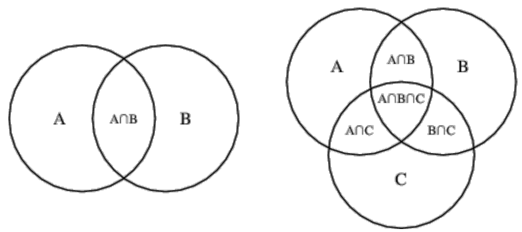
- $A \setminus B$ — **difference**, set difference, relative complement
  It corresponds (logically) to a but not b
- $A \oplus B$ — **symmetric difference**

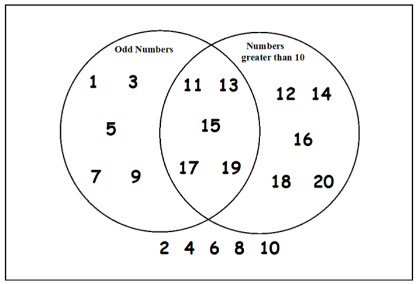
$$A \oplus B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A)$$

  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

$\boxed{1.4.4}$ $\Sigma = \{a, b\}$
(d) All subsets of Σ: ?
(e) $|\text{Pow}(\Sigma)| \stackrel{?}{=}$
$\boxed{1.4.7}$ $A \oplus A \stackrel{?}{=}$, $\quad A \oplus \emptyset \stackrel{?}{=}$
$\boxed{1.4.8}$ Relate the cardinalities $|A \cup B|$, $|A \cap B|$, $|A \setminus B|$, $|A \oplus B|$, $|A|$, $|B|$

Examples

$\boxed{1.4.4}$ $\Sigma = \{a, b\}$
(d) All subsets of Σ : $\emptyset, \{a\}, \{b\}, \{a, b\}$
(e) $|\text{Pow}(\Sigma)| = 4$
$\boxed{1.4.7}$ $A \oplus A \stackrel{?}{=} \emptyset$, $\quad A \oplus \emptyset \stackrel{?}{=} A$ for all A
$\boxed{1.4.8}$ 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

$S \times T \stackrel{\text{def}}{=} \{ (s, t) : s \in S,\ t \in T \}$ where (s, t) is an **ordered** pair

$\bigtimes_{i=1}^{n} S_i \stackrel{\text{def}}{=} \{ (s_1, \ldots, s_n) : s_k \in S_k, \text{ for } 1 \leq k \leq n \}$

$S^2 = S \times S, \quad S^3 = S \times S \times S, \ldots, \quad S^n = \times_1^n S, \ldots$

$\emptyset \times S = \emptyset$, for every S
$|S \times T| = |S| \cdot |T|, \quad |\times_{i=1}^{n} S_i| = \prod_{i=1}^{n} |S_i|$

Formal Languages

Σ — **alphabet**, a finite, nonempty set

Examples (of various alphabets and their intended uses)

$\Sigma = \{a, b, \ldots, z\}$ for single words (in lower case)
$\Sigma = \{\sqcup, -, a, b, \ldots, z\}$ 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 Σ
empty word — λ

Example

$\omega = aba$, $\omega = 01101\ldots1$, etc.

length(ω) — # of symbols in ω
length$(aaa) = 3$, 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

$\lambda\omega = \omega = \omega\lambda$
length$(\nu\omega)$ = length(ν) + length(ω)

Notation: Σ^k — set of all words of length k
We often identify $\Sigma^0 = \{\lambda\}$, $\Sigma^1 = \Sigma$
Σ^* — set of all words (of all lengths)
Σ^+ — 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 Σ^*. 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

$\boxed{1.3.10}$ Number of elements in the sets (cont'd)

(e) Σ^* 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)
$f : S \longrightarrow T$ 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: $\mathrm{Dom}(f)$
T — **codomain** of f, symbol: $\mathrm{Codom}(f)$
$\{ f(x) : x \in \mathrm{Dom}(f) \}$ — **image** of f, symbol: $\mathrm{Im}(f)$

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

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

Examples

$\boxed{1.5.3}$ Regarding length : $\{a, b\}^* \longrightarrow \mathbb{N}$
(c) $\mathrm{length}(\lambda) \stackrel{?}{=}$
(d) $\mathrm{Im}(\mathrm{length}) \stackrel{?}{=}$

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

Examples

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

$\boxed{1.5.4}$ Σ^* as above and $g(n) \stackrel{\mathrm{def}}{=} \{ \omega \in \Sigma^* : \mathrm{length}(\omega) \leq n \}$, $n \in \mathbb{N}$
Here $g(n)$ is a function that has a complex object as its value for any given argument — it maps $\mathbb{N}$ into $\mathrm{Pow}(\Sigma^*)$
(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 (cont'd)

(e) Give an example of a set in $\mathrm{Pow}(\Sigma^*)$ that is not in $\mathrm{Im}(g)$
$\boxed{1.5.6}$ Regarding gcd : $\mathbb{P} \times \mathbb{P} \longrightarrow \mathbb{P}$
(c) $\mathrm{Im}(\mathrm{gcd}) \stackrel{?}{=}$
$\boxed{1.5.7}$

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

(c) $\mathrm{Im}(f) \stackrel{?}{=}$

Examples (cont'd)

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

- any infinite subset of Σ^* (infinite language)
- any finite language that excludes some intermediate length words, e.g. $\{\lambda, a\}, \{a, b\}, \{\lambda, a, aa\}, \ldots$

$\boxed{1.5.6}$ Regarding $\gcd : \mathbb{P} \times \mathbb{P} \longrightarrow \mathbb{P}$

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

$\boxed{1.5.7}$

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

(c) $\mathrm{Im}(f) = \mathbb{R}_{\geq 0}$

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 $\longrightarrow$ and $\mapsto$

Composition of functions is described as

$$g \circ f : x \mapsto g(f(x)), \quad \text{requiring } \mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$$

If a function maps a set into itself, i.e. when $\mathrm{Dom}(f) = \mathrm{Codom}(f)$ (and thus $\mathrm{Im}(f) \subseteq \mathrm{Dom}(f)$), the function can be composed with itself — **iterated**

$$f \circ f, f \circ f \circ f, \ldots, \quad \text{also written } f^2, f^3, \ldots$$

Composition is associative

$$h \circ (g \circ f) = (h \circ g) \circ f, \quad \text{can write } h \circ g \circ f$$

Identity function on S

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

For $g : S \longrightarrow T \quad g \circ \mathrm{Id}_S = g, \ \mathrm{Id}_T \circ g = g$

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 $\gcd : (\mathbb{P}^2 \nrightarrow \mathbb{P}) \longrightarrow (\mathbb{P}^2 \nrightarrow \mathbb{P})$
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** *$f : S \nrightarrow T$ is a function $f : S' \longrightarrow T$ for $S' \subseteq S$*

gcd Example cont'd

Consider the sequence

$$f_\perp, \text{gcd}(f_\perp), \text{gcd}(\text{gcd}(f_\perp)), \ldots, \text{gcd}(\text{gcd}(\ldots(f_\perp)\ldots)), \ldots$$

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 $f = \text{gcd}(f)$. 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

$\boxed{1.8.2(b)}$ When is $(A \setminus B) \setminus C = A \setminus (B \setminus C)$?

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

Supplementary Exercises

$\boxed{1.8.2(b)}$ When is $(A \setminus B) \setminus C = A \setminus (B \setminus C)$?
From Venn diagram
$(A \setminus B) \setminus C = A \cap B^c \cap C^c$; $A \setminus (B \setminus C) = (A \cap B^c) \cup (A \cap C)$.
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 $A \setminus B$.
$\boxed{1.8.9}$ 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
  $\lfloor m \rfloor$, $\lceil m \rceil$, $m|n$, $|a|$, $[a,b]$, (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
  λ, Σ^*, Σ^+, Σ^1, $\Sigma^2, \ldots$
- Functions
  (co-)domain, image, composition $f \circ g$