Week 1 Set operations, Formal Logic

Tuesday, 26 May 2020 11:14 PM

Natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$
Positive integers $\mathbb{P} = \{1, 2, \ldots\}$

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

Number sets and their containments

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

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 $\geq x$

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

$$\left\lfloor \frac{m}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor$$

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', 'n multiple of m'

$1|m$, $-1|m$, $m|m$, $m|-m$, 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 $\mathrm{lcm}(m, n)$

Fact

$\gcd(m,n) \cdot \operatorname{lcm}(m,n) = |m| \cdot |n|$

Euclid's gcd Algorithm

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

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

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

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

Set Operations

NB

$A \cup B = B \Leftrightarrow A \subseteq B \qquad A \cap B = B \Leftrightarrow A \supseteq B$

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

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

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	$(A \cup B)^c = A^c \cap B^c$
	$(A \cap B)^c = A^c \cup B^c$

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

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

Functions

$f : S \longrightarrow T$ 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 $f(x) = y$

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

word — any finite string of symbols from Σ
empty word — λ

length(ω) — # of symbols in ω
length$(aaa) = 3$, length$(\lambda) = 0$

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)

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

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

Formal Logic

symbol	**text**
$\wedge$	“and”, “but”, “;”, “:”
$\vee$	“or”, “either . . . or . . .”
$\neg$	“not”, “it is not the case that”

Truth tables:

A	B	A $\wedge$ B
F	F	F
F	T	F
T	F	F
T	T	T

A	B	A $\vee$ B
F	F	F
F	T	T
T	F	T
T	T	T

A	$\neg$ A
F	T
T	F

$p \vee (\neg p \wedge q)$

p	q	$p \vee (\neg p \wedge q)$
F	F	F
F	T	T
T	F	T
T	T	T

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

A	B	A $\Leftrightarrow$ B
F	F	T
F	T	F
T	F	F
T	T	T

Same as $(A \Rightarrow B) \wedge (B \Rightarrow A)$

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

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

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

$\boxed{\text{LLM: Problem 3.2}}$

$$\begin{aligned} p &= \text{"you get an HD on your final exam"} \\ q &= \text{"you do every exercise in the book"} \\ r &= \text{"you get an HD in the course"} \end{aligned}$$

Translate into logical notation:

(a) You get an HD in the course although you do not do every exercise in the book.

(c) To get an HD in the course, you must get an HD on the exam.

(d) You get an HD on your exam, but you don't do every exercise in this book; nevertheless, you get an HD in this course.

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

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