CSE 16 6-23-22

Recall: $\underbrace{\mathbb{N} \subseteq \mathbb{Z}}_{\text{special Properties}} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Fact: (Well ordering Property of $\mathbb{N}$)

Any non-empty subset of $\mathbb{N}$ contains a least element.

i.e. if $A \subseteq \mathbb{N}$ and $A \neq \emptyset$, then there exists $x_0 \in A$ such that

$$x_0 \leq x$$

for all $x \in A$.

This is an Axiom of $\mathbb{N}$.

note: $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ also has this Prop.

Theorem (Division Algorithm)

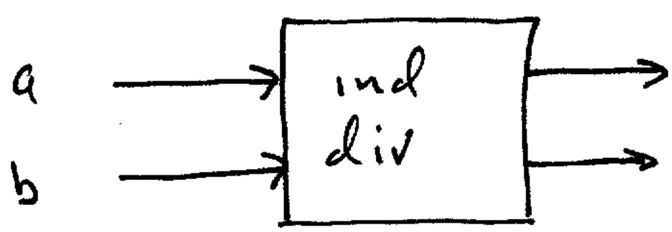
Given $a, b \in \mathbb{Z}^+$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \le r < b$$

dividend divisor

quotient remainder

unlike real division, this operation (integer division) has 2 inputs & 2 outputs



$q = a \text{ div } b = a/b$

$r = a \text{ mod } b = \underbrace{a\%b}_{\text{many comp. lang.}}$

Two things are asserted:

(1) existence of q, r

(2) uniqueness of q, r

<u>Proof of (1)</u>

Let

$$A = \{ a - xb \mid x \in \mathbb{Z} \text{ and } 0 \le a - xb \le a \}$$

observe

$$A \subseteq \{0, 1, 2, \ldots, a\} \subseteq \underbrace{\mathbb{Z}_{\ge 0}}_{\text{has the W.O.P.}}$$

By the W.O.P for $\mathbb{Z}_{\ge 0}$, (since $A \ne \phi$) we have that A contains a least element, call it r. Thus

$$r = a - qb \text{ for some } q \in \mathbb{Z}$$

and $r \ge 0$.

Thus

$$a = qb + r \quad \text{and} \quad 0 \leq r$$

suppose that $r \geq b$. then we have

$$0 \leq r - b = (a - qb) - b = a - (q+1)b < a - qb = r$$

This is impossible since $r = a - qb$ is the least integer of the form $a - xb$ satisfying $0 \leq a - xb \leq a$.

$\therefore$ $r \geq b$ must be false.

$\therefore$ $r < b$ must be true.

Thus

$$a = qb + r \quad \text{and} \quad 0 \leq r < b.$$

$\blacksquare$

Exercise:

try to prove uniqueness, i.e.

suppose

$$a = q_1 b + r_1 \quad \text{and} \quad 0 \leq r_1 < b$$

and

$$a = q_2 b + r_2 \quad \text{and} \quad 0 \leq r_2 < b$$

show that $q_1 = q_2$ and $r_1 = r_2$.

what are numbers?

how to construct $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$

out of sets?

John Von Neuman

Given a set S, the successor of S is

$$S^+ = S \cup \{S\}$$

define:

$$\begin{aligned}
0 &= \emptyset \\
1 &= 0^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\} \\
2 &= 1^+ = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} \\
3 &= 2^+ = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\} \\
&\vdots \\
n &= \{0, 1, 2, \ldots, n-1\} \\
&\vdots
\end{aligned}$$

The set $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ can be proved to satisfy the W.O.P.

(1.10) Russel's Paradox

Can there be a set that contains itself as a member?

Ex. $A = \{A\}$

so

$$A = \{A\} = \{\{A\}\} = \{\{\{A\}\}\}$$

i.e.

$$A = \{\{\{\{\cdots\}\}\}\}$$

our naive defn of set allows this!

Russel's Paradox

define

$$\mathcal{S} = \{x \mid x \text{ is a set}\}$$

the set of all sets!

Evidently $\mathcal{S} \in \mathcal{S}$. On the other hand $\emptyset \notin \emptyset$.

Define

$$\mathcal{R} = \{A \in \mathcal{S} \mid A \notin A\}$$

$\mathcal{R}$ consists of all 'normal' sets.

Clearly either $\mathcal{R} \in \mathcal{R}$ or $\mathcal{R} \notin \mathcal{R}$.

- If $\mathcal{R} \in \mathcal{R}$, then $\mathcal{R}$ must satisfy the defining property of $\mathcal{R}$, namely $\mathcal{R} \notin \mathcal{R}$. ※
- If $\mathcal{R} \notin \mathcal{R}$, then $\mathcal{R}$ does satisfy the property defining $\mathcal{R}$, hence $\mathcal{R} \in \mathcal{R}$. ※

chapter-2 : logic

(1.1) statements

Defn

a **statement** (or **proposition**) is a sentence can be assigned a truth value (**true** or **false**), at least in principle.

statements:

- 'it is raining today'
- $2+3=5$
- $2+3=7$

not statements:

- 'hello'
- $x+7=2$
- $a+b=c$

open sentences or **propositional functions** or predicates

we use variables ..p, q, r....
to stand for statements, we call
these propositional variables

we use functional notation P(x)
Q(y), R(a, b, c), etc... to denote
propositional fcns.

(2.2) operations: and, or, not

and (conjunction): $p \wedge q$

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

True only in the case both operands are true, false in every other case.

Ex. p = 'it is raining today'

q = 'today is Wednesday'

or (disjunction, inclusive or): $p \vee q$

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

false only in case both operands are false, true in every other case

exor (exclusive or): $p \oplus q$

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

true only if both operands are different, false otherwise.

Ex. 'your money or your life'

<u>not (negation)</u> : $\sim p$ (also $\neg p$)

p	$\sim p$
F	T
T	F

reverse truth value of operand.

(2.3) operation : Conditional

<u>conditional (implication)</u> : $p \Rightarrow q$ (also $p \rightarrow q$)

p	q	$p \Rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

False only in case hypothesis is true and conclusion is false, true otherwise.

p left operand : <u>hypothesis</u>

q right " : <u>conclusion</u>

Read $p \Rightarrow q$ as:

'if p, then q'

'p implies q'

'p only if q'

'p is sufficient for q'

also:

'q, if p'

'q, whenever p'

'q is necessary for p'