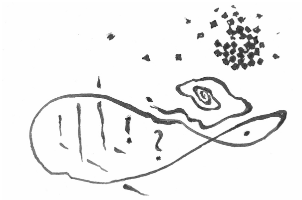
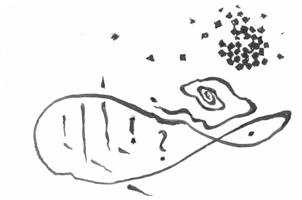
Algorithmic Adventures

From Knowledge to Magic



Book by Juraj Hromkovič, ETH Zurich
Slides by Tom Verhoeff, TU Eindhoven

Quotation



Little progress would be made in the world
if we were always afraid of possible negative consequences.

Georg Christoph Lichtenberg

Potential and Actual Infinity

The sequence of natural (counting) numbers never ends:

$$0,\ 1,\ 2,\ 3,\ \ldots$$

There is no largest natural number: after i comes $i+1$

The sequence is **unbounded**, giving rise to **potential infinity**:

at each moment we have encountered only a finite set

We never need to see **actual infinity**, the whole infinite set together:

$$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \ldots\}$$

$\mathbb{N}$ is an infinite object, about which we reason symbolically

How many elements does $\mathbb{N}$ have? ∞?

Integer numbers

The set $\mathbb{Z}$ of integer numbers (integers):

$$\mathbb{Z} = \{\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}$$

How many elements does $\mathbb{Z}$ have? ∞?

Are there more integers than natural numbers?

The set $\mathbb{Z}^+$ of positive integers:

$$\mathbb{Z}^+ = \{1,\ 2,\ 3,\ \ldots\}$$

How many elements does $\mathbb{Z}^+$ have? ∞?

Are there more natural numbers than positive integers?

Rational numbers

The set $\mathbb{Q}^+$ of positive rational numbers (integer fractions):

$$\mathbb{Q}^+ = \left\{ \frac{m}{n} \,\middle|\, m, n \in \mathbb{Z}^+ \right\}$$

There is no smallest positive fraction: $\frac{1}{i} > \frac{1}{i+1} > \ldots > 0$

The positive fractions extend the positive integers: $\mathbb{Z}^+ \subset \mathbb{Q}^+$

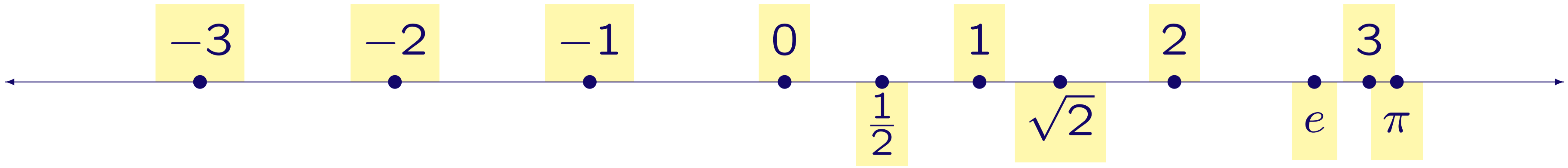
Between every pair of fractions q_1, q_2 lies another fraction: $(q_1 + q_2)/2$

Between natural numbers n and $n + 1$ lie infinitely many fractions

How many elements does $\mathbb{Q}^+$ have? ∞?

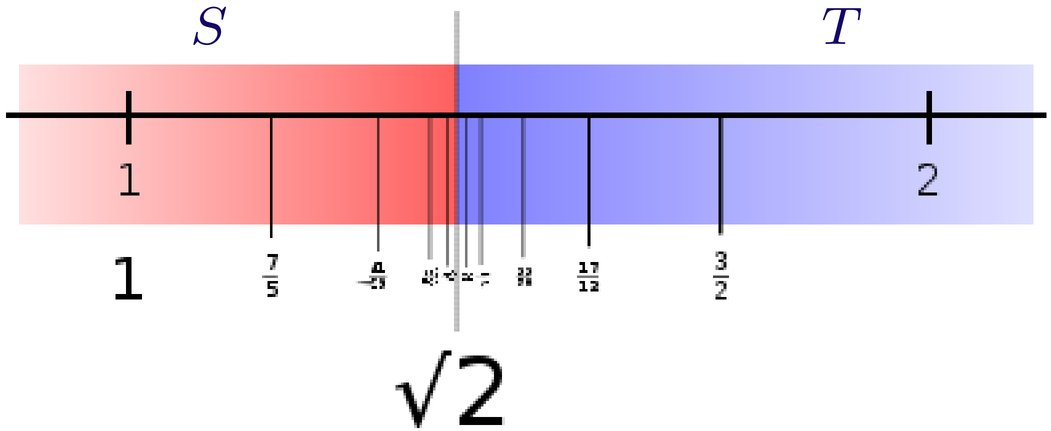
Are there more positive fractions than natural numbers?

The Number Line and Dedekind Cuts



A *Dedekind cut* of $\mathbb{Q}^+$ is a pair of nonempty subsets $S, T \subset \mathbb{Q}^+$ with

- $S \cup T = \mathbb{Q}^+$, i.e., they partition Q^+ into two parts
- $S < T$, i.e., $s < t$ for all $s \in S$ and $t \in T$, i.e., S lies left of T
- S has no largest element (N.B. T may but need not have a smallest element)



Real numbers

The set $\mathbb{R}^+$ of positive real numbers (Dedekind cuts):

$$\mathbb{R}^+ = \left\{ (S,T) \;\middle|\; S,T \text{ is a Dedekind cut of } \mathbb{Q}^+ \right\}$$

Every real number r has an infinite **radix-R expansion** ($2 \leq R \in \mathbb{N}$):

$$r = n.d_1 d_2 d_3 \ldots = n + \textstyle\sum_{i=1}^{\infty} d_i R^{-i}, \text{ with } n \in \mathbb{N},\ d_i \in \mathbb{N},\ d_i < R$$

$\sqrt{2} = 1.41421\ldots$ (decimal, $R = 10$) $= 1.01101\ldots$ (binary, $R = 2$)

The positive real numbers extend the positive fractions: $\mathbb{Q}^+ \subset \mathbb{R}^+$

Square root two is a real number, not a fraction: $\sqrt{2} \in \mathbb{R}^+ \setminus \mathbb{Q}^+$

How many elements does $\mathbb{R}^+$ have? ∞?

Are there more positive real numbers than positive fractions?

Comparing the Sizes of (Infinite) Sets According to Cantor

The **size** of set S is denoted by $|S|$

A **matching** of sets S and T is a set of pairs $(s,t) \in S \times T$ such that

- $s \in S$ and $t \in T$
- each element of S is the first element of a exactly one pair
- each element of T is the second element of a exactly one pair

We write $S \overset{1-1}{\longleftrightarrow} T$ when there exists a matching between S and T

Cantor (mathematician, 1845–1918) defined:

$$|S| = |T| \quad \text{if and only if} \quad S \overset{1-1}{\longleftrightarrow} T$$

Comparing $\mathbb{N}$ and $\mathbb{Z}^+$

$$\begin{array}{rcccccccccccl} \mathbb{N} & = & \{ & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & \ldots \;\} \\ & & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{Z}^+ & = & \{ & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & \ldots \;\} \end{array}$$

A matching between $\mathbb{N}$ and $\mathbb{Z}^+$:

$$\{\, (i, i+1) \mid i \in \mathbb{N} \,\}$$

Hence

$$|\mathbb{N}| = \left|\mathbb{Z}^+\right|$$

Note that $\mathbb{Z}^+$ is a proper subset of $\mathbb{N}$: $\mathbb{Z}^+ \subset \mathbb{N}$

A proper part of an infinite set can have the same size as the whole set

Definition S is infinite when it has a proper subset $T \subset S$ with $|T| = |S|$

Comparing $\mathbb{N}$ to some other subsets

$$
\begin{array}{rcllllllllll}
\mathbb{N} & = & \{ & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & \ldots \} \\
& & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{N}_{\text{even}} & = & \{ & 0, & 2, & 4, & 6, & 8, & 10, & 12, & 14, & 16, & \ldots \} \\
& & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{N}_{\text{square}} & = & \{ & 0, & 1, & 4, & 9, & 16, & 25, & 36, & 49, & 64, & \ldots \} \\
& & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{N}_{\text{prime}} & = & \{ & 2, & 3, & 5, & 7, & 11, & 13, & 17, & 19, & 23, & \ldots \} \\
& & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{N}_{\text{powers of 10}} & = & \{ & 1, & 10, & 10^2, & 10^3, & 10^4, & 10^5, & 10^6, & 10^7, & 10^8, & \ldots \}
\end{array}
$$

All these infinite subsets have the same size as $\mathbb{N}$

$|S| = |\mathbb{N}| \;\Leftrightarrow\;$ the elements of S can be **enumerated** (numbered)

Comparing $\mathbb{N}$ to $\mathbb{Z}$

$$
\begin{array}{ccccccccccccc}
\mathbb{N} & = & \{ & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & \ldots \} \\
 & & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{Z} & = & \{ & 0, & -1, & 1, & -2, & 2, & -3, & 3, & -4, & 4, & \ldots \}
\end{array}
$$

An enumeration need not be order preserving!

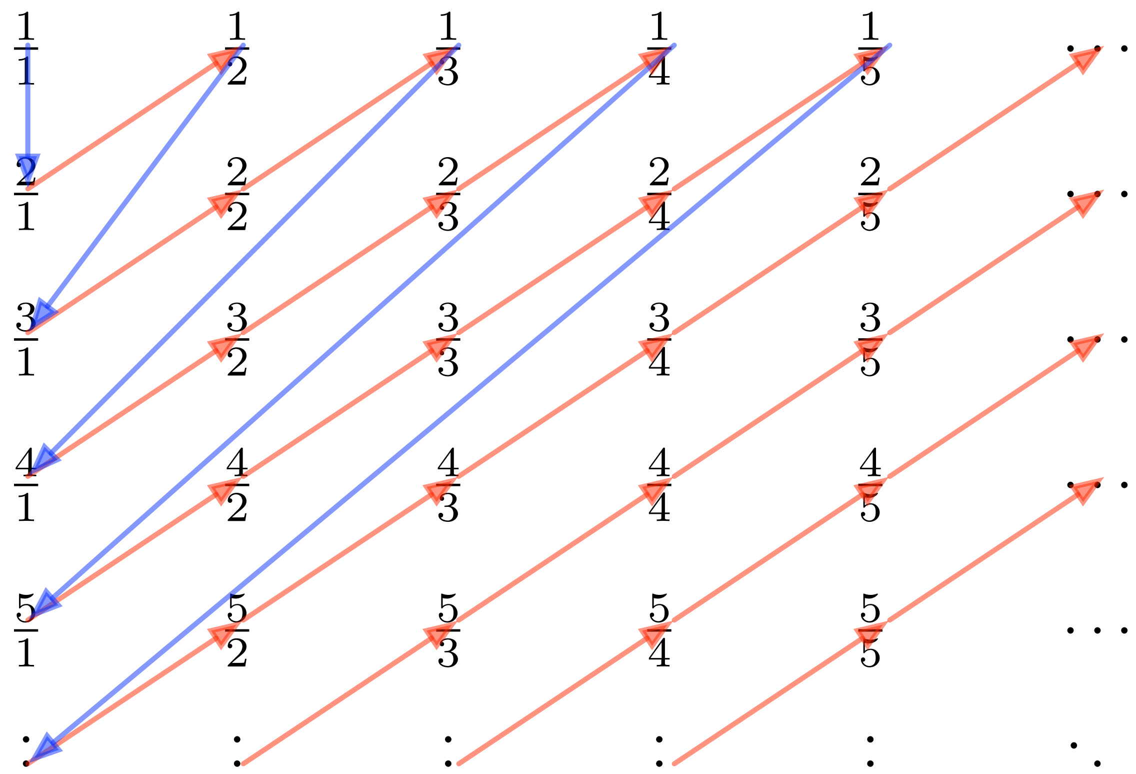
Comparing $\mathbb{N}$ to $\mathbb{Q}^+$

$$
\begin{array}{cccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \cdots \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \cdots \\
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

Can the elements of $\mathbb{Q}^+$ be enumerated?

N.B. Table contains duplicates!

Enumeration of $\mathbb{Q}^+$ by Diagonals (Cantor)



$$
\begin{array}{ccccccccccccc}
\mathbb{N} & = & \{ & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & \ldots \; \} \\
 & & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{Q}^+ & = & \{ & \frac{1}{1}, & \frac{2}{1}, & \frac{1}{2}, & \frac{3}{1}, & \frac{1}{3}, & \frac{4}{1}, & \frac{3}{2}, & \frac{2}{3}, & \frac{1}{4}, & \ldots \; \}
\end{array}
$$

Encoding Pairs of Natural Numbers ($\mathbb{N} \times \mathbb{N}$) in $\mathbb{N}$

An enumerable union of enumerable sets is enumerable

Map $(a, b) \in \mathbb{N} \times \mathbb{N}$ to what unique natural number in $\mathbb{N}$?

A mapping of the form $F(a, b) = Ka + b$ does not work,
because $F(a+1, b) = K(a+1) + b = Ka + b + K = F(a, b+K)$

Diagonalization works: define $F(a, b) = (a+b)(a+b+1)/2 + b$

$F(a, b)$	$b = 0$	$b = 1$	$b = 2$	$b = 3$
$a = 0$	0	2	5	9
$a = 1$	1	4	8	
$a = 2$	3	7		
$a = 3$	6			

Based on *triangular numbers* $(b = 0)$: $a(a+1)/2 = \sum_{i=1}^{a} i$

Encoding k-Tuples of Natural Numbers ($\mathbb{N}^k$) in $\mathbb{N}$

Let $F_2 = F : \mathbb{N}^2 = \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$F_3 : \mathbb{N}^3 = \mathbb{N} \times \mathbb{N} \times \mathbb{N} = \{ (a, b, c) \mid a, b, c \in \mathbb{N} \} \to \mathbb{N}$

Define $F_3(a, b, c) = F(a, F(b, c))$

Similarly for $\mathbb{N}^{k+1} = \mathbb{N} \times \mathbb{N}^k$

Define $F_{k+1}(a_1, a_2, a_3, \ldots, a_{k+1}) = F(a_1, F_k(a_2, a_3, \ldots, a_{k+1}))$

Hence, Each $\mathbb{N}^k$ is enumerable: $\left|\mathbb{N}^k\right| = |\mathbb{N}|$

N.B. All F_k are invertible

Encoding All Tuples of Natural Numbers ($\mathbb{N}^* = \bigcup \mathbb{N}^k$) in $\mathbb{N}$

The set of all tuples of natural numbers: $\mathbb{N}^* = \bigcup_{k=1}^{\infty} \mathbb{N}^k$ where $\mathbb{N}^1 = \mathbb{N}$

Define $G : \mathbb{N}^* \to \mathbb{N}$ by

$$G(a_1, a_2, a_3, \ldots, a_k) \;=\; F(k, F_k(a_1, a_2, a_3, \ldots, a_k))$$

where $F_1(n) = n$ (N.B. G is invertible)

G is also called a **Gödel numbering** of $\mathbb{N}^*$

Hence, $\mathbb{N}^*$ is enumerable: $|\mathbb{N}^*| \;=\; |\mathbb{N}|$

Are all sets enumerable?

The Power Set Consisting of All Subsets

For a set S, its **power set** $\mathcal{P}(S)$ consists of all subsets of S:

$$\mathcal{P}(S) = \{ T \mid T \subseteq S \}$$

E.g. $\mathcal{P}(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$

Attempt to match S and $\mathcal{P}(S)$:

$x \in S$	$\leftrightarrow$	subset $T_x \subseteq S$: $\bullet = y \in T_x$				
		a	b	c	d	$\cdots$
a	$\leftrightarrow$	$\bullet$	$\circ$	$\circ$	$\circ$	$\cdots$
b	$\leftrightarrow$	$\circ$	$\circ$	$\bullet$	$\circ$	$\cdots$
c	$\leftrightarrow$	$\bullet$	$\bullet$	$\circ$	$\circ$	$\cdots$
d	$\leftrightarrow$	$\circ$	$\circ$	$\bullet$	$\bullet$	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
?	$\leftrightarrow$	$\circ$	$\bullet$	$\bullet$	$\circ$	$\cdots$

D = complement of diagonal

A Set is Smaller Than Its Power Set (Cantor)

Diagonalization method: assume matching $\{ (x, T_x) \mid x \in S, T_x \subseteq S \}$

$$\begin{aligned} D &= \{ x \in S \mid x \notin T_x \} \\ x \in D &\Leftrightarrow x \in S \text{ and } x \notin T_x \\ D \subseteq S &\text{ and } D \neq T_x \end{aligned}$$

Hence, $D \in \mathcal{P}(S)$ is not matched with any $x \in S$

Consequently, S is smaller than $\mathcal{P}(S)$: $|S| < |\mathcal{P}(S)|$, in particular

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$$

The power set of S is isomorphic to the set of mappings $S \to \{ 0, 1 \}$

$$f : S \to \{ 0, 1 \} \text{ corresponds to } \{ x \in S \mid f(x) = 1 \}$$

$\mathcal{P}(\mathbb{N})$ corresponds to the set of all infinite $0, 1$-sequences

The Set of Real Numbers is Not Enumerable

Real numbers in the interval $[0, 1]$ have *binary expansions* of the form

$$0.d_1 d_2 d_3 \ldots \text{ with } d_i \in \{\, 0, 1 \,\}$$

Thus, there is a correspondence between $[0, 1]$ and infinite $0, 1$-sequences

> There are still some technical difficulties here, because
>
> $$0.\cdots 0\overline{1} \;=\; 0.\cdots 1\overline{0}$$
>
> where $\overline{d}$ means an infinite tail of repeating digits d only

Consequently, the real numbers are not enumerable:

$$|\mathbb{N}| < |\mathbb{R}|$$

Cantor also showed that $|[0, 1]| \;=\; |\mathbb{R}| \;=\; \left|\mathbb{R}^k\right|$

Summary

The size of set S is denoted by $|S|$

The sizes of two sets can be compared via *matchings* between them:

$$|S| = |T| \text{ if and only if } S \overset{1-1}{\longleftrightarrow} T$$

Set S is infinite (in size) if and only if it has

a proper part $P \subset S$ that is as large as the whole: $|P| = |S|$

For the sets of natural numbers $\mathbb{N}$, of positive rational numbers $\mathbb{Q}^+$, of positive real numbers $\mathbb{R}^+$, we have

$$|\mathbb{N}| = \left|\mathbb{Q}^+\right| < \left|\mathbb{R}^+\right|$$

Both proofs used a diagonal construction