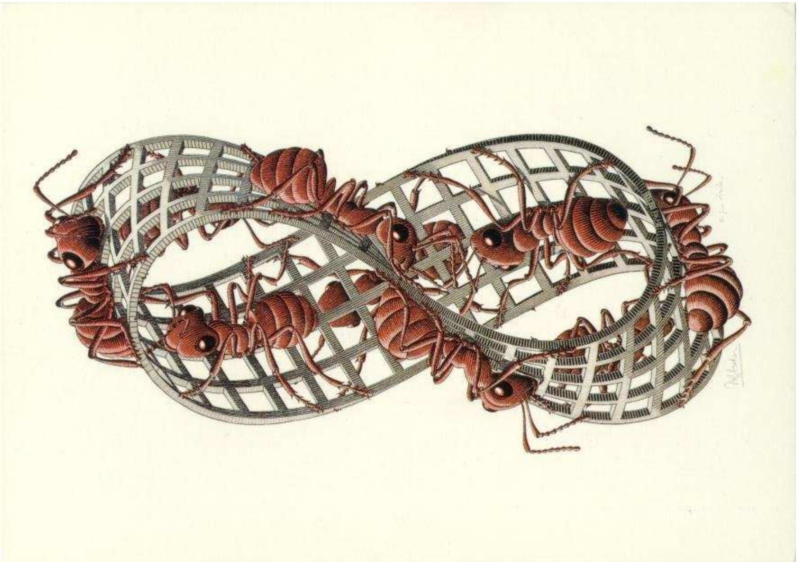
The Construction of



Venanzio Capretta

Foundation Group, ICIS, University of Nijmegen, NL

Theory Days, Põlva, 26 January 2008

Greek philosophy and mathematics

Fascination and fear of infinity.

Anaximander

Apeiron: infinite or limitless, the origin of all things.

Zeno's paradoxes: Achilles and the Tortoise, Arrow Paradox.

Aristotle: "The infinite is potential, never actual."

Zeno's paradoxes: infinite divisibility of a finite interval.

19th century: formal theory of real numbers, problem solved.

A Zeno-like paradox:
A bag and numbered balls. We put balls in the bag and take them out by stages.

11:00: put balls 1, 2, ..., 10 in the bag, take out ball 1;

11:30: put balls 11, 12, ..., 20 in the bag, take out ball 2;

11:45: put balls 21, 22, ..., 30 in the bag, take out ball 3;

... and so on.

How many balls will be in the bag at 12:00?

First answer: At 12:00 there are infinitely many balls in the bag, because we add nine balls at each stage and there are infinitely many stages.

Second answer: At 12:00 the bag is empty, because ball number n was taken out at $1/n$ hours before 12:00 and never put back in the bag.

Sieve of Eratosthenes

Fist example of "computing" with an infinite object. An algorithm to compute the sequence of prime numbers.

1. Write down the sequence of natural numbers starting with 2;
2. The first element p in the sequence is the next prime;
3. Delete the multiples of p from the sequence;
4. Go back to 2.

Run of the algorithm:

1. 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ...
2. 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ...
3. 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ...
4. 2 3 5 7 9 11 13 15 ...
2. 2 3 5 7 9 11 13 15 ...
3. 2 3 5 7 9 11 13 15 ...
4. 2 3 5 7 11 13 ...
2. 2 3 5 7 11 13 ...

Observations:

We are computing with infinite lists.
The algorithm doesn't terminate,
but still defines a correct output.

Cantor

Mathematical theory of infinite sets.
Discovery of different sizes of infinity.
Let to axiomatic set theory.

Cantor proof:
Let X be a set, then $\mathcal{P}X$, the set of subsets of X, has a higher cardinality than X.

Let $\phi : X \to \mathcal{P}X$.
Prove that ϕ “misses” at least one element (it is not surjective).
$U = \{x \in X \mid x \notin \phi(x)\}$. It cannot be $U = \phi(u)$ for $u \in X$.
Suppose $U = \phi(u)$ and ask: $u \in U$ or $u \notin U$?

20th century

Development of Axiomatic Set Theory: ZFC.
Criticism from intuitionists and predicativists.

Skolem's paradox

ZFC has a countable model:
The Löwenheim-Skolem theorem states that a theory always has a countable model, constructed using the syntax.

But inside ZFC we can prove that there are uncountable sets, for example $\mathbb{R}$. Is $\mathbb{R}$ in the model countable or uncountable?

It is uncountable from inside but countable from the outside.

Notion of cardinality not absolute, but depends on the theory.

In Computer Science: we count cardinality using computable functions. They are much fewer than all functions in set theory. There can be non-recursively countable data types.

Non-Well-Founded Sets

Chain of membership relations:

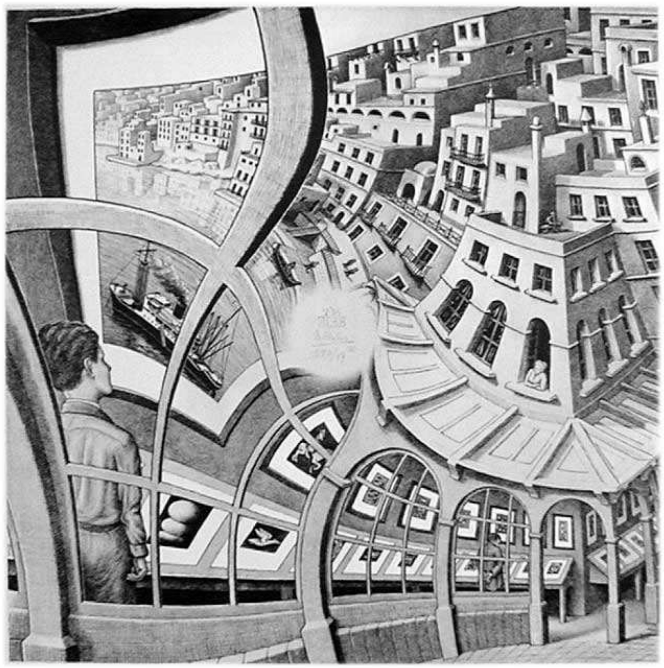
$$\cdots \in x_4 \in x_3 \in x_2 \in x_1 \in x_0.$$

In standard set theory such a chain cannot descend for ever: Foundation Axiom.

Peter Aczel developed a set theory in which it is possible to descend forever.
Anti-Foundation Axiom: Every pointed graph defines a set.

$$\begin{tikzcd} a \arrow[r] \arrow[d, bend right] & b \arrow[d] \\ c \arrow[r] \arrow[u, bend right] & d \arrow[loop right] \end{tikzcd}$$

$$\begin{aligned} a &= \{b, c\} = \{\{d\}, \{a, d\}\} = \{\{\{d\}\}, \{\{b, c\}, \{d\}\}\} \\ b &= \{d\} \\ c &= \{a, d\} \\ d &= \{d\} \end{aligned}$$



M. C. Escher, *Print Gallery* (1956)

Co-Inductive Data Types

Types whose elements may contain infinite structures.

Inductive Type:

$$\mathsf{List}(A) = \mathsf{nil} : \mathsf{List}(A) \mid \mathsf{cons} : A \to \mathsf{List}(A) \to \mathsf{List}(A)$$

Elements are well-founded: no infinite descending chain of cons:

$$\mathsf{cons}\, a_0\, (\mathsf{cons}\, a_1\, (\mathsf{cons}\, a_2\, (\cdots (\mathsf{cons}\, a_n\, \mathsf{nil}) \cdots))) = [a_0, a_1, a_2, \ldots, a_n]$$

CoInductive Type:

$$\mathsf{Stream}(A) = \mathsf{scons} : A \to \mathsf{Stream}(A) \to \mathsf{Stream}(A)$$

We can have non-well-founded elements: infinite descending chains of scons:

$$\mathsf{scons}\, a_0\, (\mathsf{scons}\, a_1\, (\mathsf{scons}\, a_2\, (\cdots\cdots))) = [a_0, a_1, a_2, \ldots]$$

Circular definitions:

$$\begin{array}{l} \mathsf{from} : \mathbb{N} \to \mathsf{Stream}(\mathbb{N}) \\ \mathsf{from}\, n = \mathsf{scons}\, n\, (\mathsf{from}\, (n+1)) \end{array}$$

$$\mathsf{nat} : \mathsf{Stream}(\mathbb{N}) = \mathsf{from}\, 0 = [0, 1, 2, \ldots]$$

The definition of from uses from to define itself.

It is acceptable because it is guarded by scons.

This guarantees productivity: the unfolding of the definition will keep producing new parts of the structure forever.

Sieve of Eratosthenes:

$$\mathsf{filter} : \mathbb{N} \to \mathsf{Stream}(\mathbb{N}) \to \mathsf{Stream}(\mathbb{N})$$
$$\mathsf{filter}\, x\, (\mathsf{scons}\, y\, s) = \mathsf{filter}\, x\, s \quad \text{if } y \text{ is divisible by } x$$
$$\mathsf{filter}\, x\, (\mathsf{scons}\, y\, s) = \mathsf{scons}\, y\, (\mathsf{filter}\, x\, s) \quad \text{otherwise}$$

$$\mathsf{sieve} : \mathsf{Stream}(\mathbb{N}) \to \mathsf{Stream}(\mathbb{N})$$
$$\mathsf{sieve}\, (\mathsf{scons}\, x\, s) = \mathsf{scons}\, x\, (\mathsf{sieve}\, (\mathsf{filter}\, x\, s))$$

$$\mathsf{primes} : \mathsf{Stream}(\mathbb{N}) = \mathsf{sieve}\, (\mathsf{from}\, 2)$$

Problem: filter is not guarded.

But primes is productive.

Ongoing work: finer analysis of computational infinite objects.
Work with Tarmo Uustalu and Varmo Vene

Other example (productive but not guarded):

$$\mathsf{down\_runs} : \mathsf{Stream} \to \mathsf{Stream}$$
$$\mathsf{down\_runs}\, s = \mathsf{drf}\, \langle 1, s \rangle$$

$$\mathsf{drf} : \mathbb{N} \times \mathsf{Stream} \to \mathsf{Stream}$$
$$\mathsf{drf}\, \langle n, (\mathsf{scons}\, x_1\, (\mathsf{scons}\, x_2\, s)) \rangle = \begin{cases} \mathsf{drf}\, \langle (n+1), (\mathsf{scons}\, x_2\, s) \rangle & \text{if } x_1 > x_2 \\ \mathsf{scons}\, n\, (\mathsf{drf}\, \langle 1, (\mathsf{scons}\, x_2\, s) \rangle) & \text{if } x_1 \leq x_2 \end{cases}$$

down_runs counts the length of "descending subsequences":

$$\begin{aligned} & \mathsf{down\_runs}\, [4, 2, 1, 3, 2, 9, 6, 5, 3, 6, 3, 2, 7, \ldots] \\ & = \mathsf{drf}\, \langle 1, [4, 2, 1, 3, 2, 9, 6, 5, 3, 6, 3, 2, 7, \ldots] \rangle \\ & = \mathsf{drf}\, \langle 2, [2, 1, 3, 2, 9, 6, 5, 3, 6, 3, 2, 7, \ldots] \rangle \\ & = \mathsf{drf}\, \langle 3, [1, 3, 2, 9, 6, 5, 3, 6, 3, 2, 7, \ldots] \rangle \\ & = \mathsf{scons}\, 3\, (\mathsf{drf}\, \langle 1, [3, 2, 9, 6, 5, 3, 6, 3, 2, 7, \ldots] \rangle) \\ & \quad \vdots \\ & = [3, 2, 4, 3, \ldots] \end{aligned}$$

CoInductive Types to represent computations

Work with Ana Bove

Trace of a computation:

If the computation doesn't terminate, the trace is infinite.

$$\begin{array}{l}\textsf{hail}\,1 = 0 \\ \textsf{hail}\,n = 1 + \textsf{hail}\,(n/2) \quad \text{if } n \text{ is even} \\ \textsf{hail}\,n = 1 + \textsf{hail}\,(3n+1) \quad \text{if } n \text{ is odd}\end{array}$$

Open Problem: Is hail a total function? Collatz conjecture

Trace of the computation of (hail 27):

$$[27, 82, 41, 124, 62, 31, 94, 47, 142, 71, \ldots]$$

Conclusions

Infinite objects can be represented computationally;

Computations on infinite objects:
infinite but productive;

Computations are infinite objects:

Epistemic logic: representation of Common Knowledge;

Much work to do
Understand the properties of computations on infinite objects.

A research group at the University of Leiden
Led by Hendrik Lenstra
studied Escher's work *Print Gallery*

They managed to fill in the gap in the middle.

Here is the result ...
http://escherdroste.math.leidenuniv.nl/