Computability and Complexity

Section 1: Motivations & History, Sets & Proofs, Functions & Equinumerous sets

Miguel Couceiro
miguel.couceiro@loria.fr
https://members.loria.fr/mcouceiro/

NLP Master's Program

Based on lecture notes of Romain Péchoux

Motivations

Discrete Mathematics plays an important role in CS:

- information theory : data compression, cryptography
- Probability theory: random number generator
- Graph theory: network modeling
- Logic: reasoning and proofs
- Complexity theory: lower and upper bounds

This course is about what computation actually is (from a mathematical point of view). For this, it introduces:

- (un)computability and (un)decidability
- computational complexity.

Turing machine

- A *model of computation* (*computational model*) is a machinery that performs computations.
- The central concept in this course is

Turing machine (TM)

an abstract (but quite simple) model of computation introduced by Alan Turing in the 30's (before computers!)

- The TM model was inspired by the human *reasoning* and conceived to reflect human *computations*.

Church's thesis

- **TM**s seem too technical (low level), but Church's Thesis:

  "Anything that is computable can be computed by a TM."

  where "computable" means "computed by human means".

- The **TM** model is a universal model of computation

Despite the many "realistic" models of computation proposed:

They have no more *computational power* than TMs.

Why is this material important?

TMs are robust models of computation that provide a mathematical basis for CS.

The concept of a TM splits the mathematical universe into:

- "things" that can be computed, and
- "things" that cannot.

We will see that there are many (simply) well-defined mathematical problems that cannot be computed by any reasonable means.

But also important for other reasons

These concepts have ramifications into other domains: logic, philosophy, cognitive science and artificial intelligence.

The links with logic are deep and intimate:

- Logicians such as Gödel, Church, Turing, and Kleene first introduced and explored the concept of computability.
- In turn, they fed back into logic and revealed its limitations (see Gödel's celebrated Incompleteness Theorems).

Impact on Philosophy

The discovery of non computable (uncomputable) problems affected occidental philosophical culture deeply.

Example: Hilbert's 10th problem on the algorithmic solvability of Diophantine equations (integer sol.s of polynomial equations)

It also raises many other philosophical issues:

- Church's thesis is not a mathematical truth (i.e., something that can be proved)
- It is also not an empirical generalization!

Impact on Cognitive Science and Artificial Intelligence

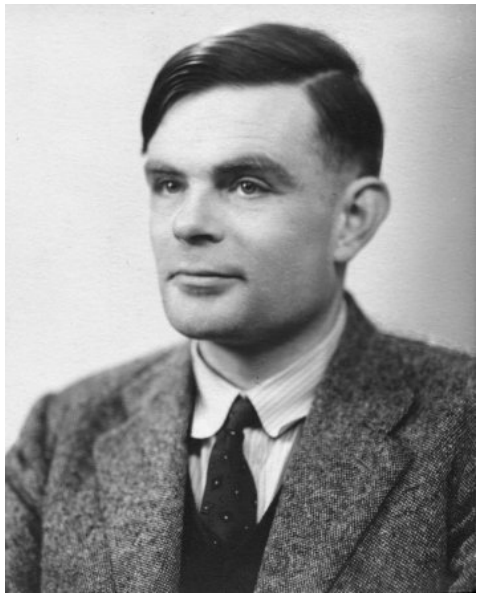
TMs were inspired by the cognitive process of computation

TMs gave rise to devices with internal states that provided the ideas that helped psychology to break free of behaviorism in a scientific way, thus giving rise to modern cognitive science.

It also suggested that intelligence could be not only modeled, but actually created by programming.

This led to the birth of artificial intelligence.

Alan Turing (1912-1954)



Alan Turing (born 23 June 1912, died 7 June 1954), British mathematician, cryptographer, a key figure in the birth of theoretical and practical cs, and a pioneer of Artificial Intelligence and Cognitive Science (with special reference to Natural Language). He also did important early work on the formation of patterns and mathematical biology.

Computability and Incompatibility

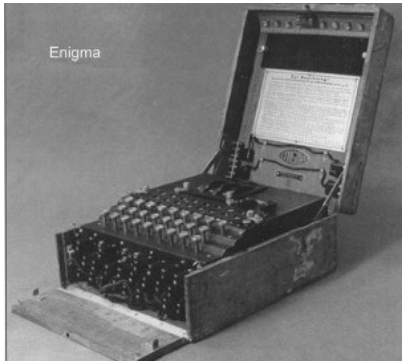
- He introduced TM in his 1936 paper:

  "On Computable Numbers, with an Application to the Entscheidungsproblem".

- and showed convincingly that such machines would be capable of solving any conceivable mathematical problem that could be dealt with algorithmically.
- In 1937 and 1938 he was in Princeton, he completed a PhD under the direction of A. Church (on TM with oracles).

World War II and Cryptography

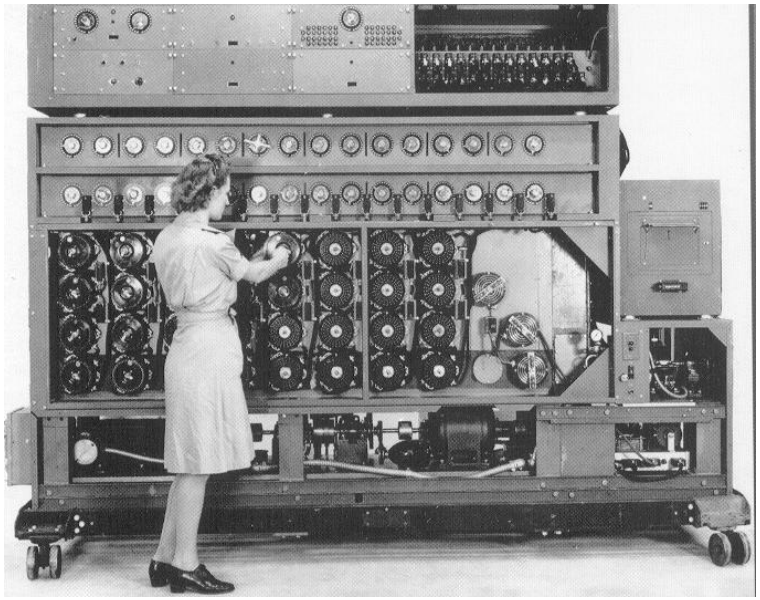
- During WWII, Turing was the key figure in the British attempts at Benchley Park to break the U-boats Enigma machine codes:



- Enigma was capable of encoding/decoding transmissions. Eventually an Enigma machine was captured - but how could it be understood? It had up to 1022 states!

Turing's response: the Bombe

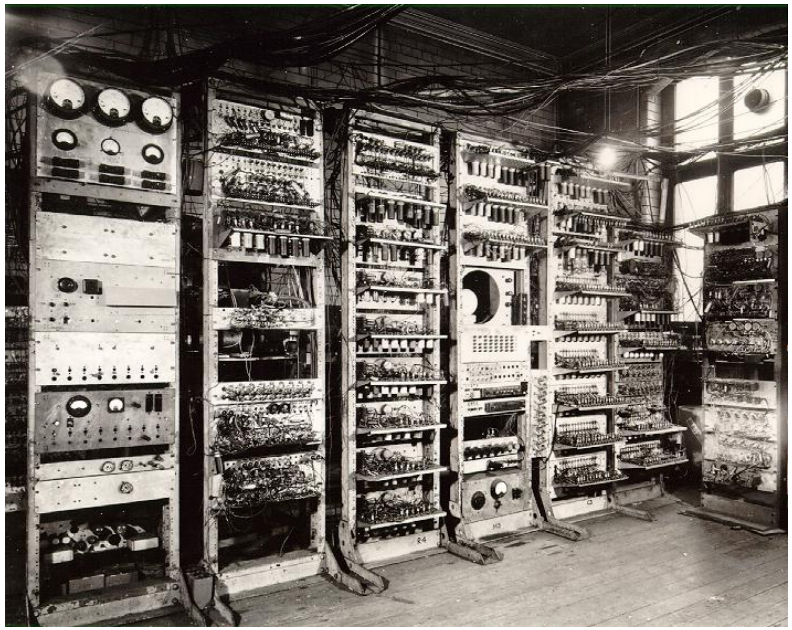
- His answer was the creation of the Bombe. It was, in effect, an early computer, though not a universal computer, that could rapidly test many possible settings of the Enigma machine by using logical deduction:



- Turing had the first Bombe running by March 1940. By the end of the war, 200 were in operation.

Manchester Mark 1 - 1949

In 1948 he moved to Manchester University where he participated in the development of the Manchester Mark 1:



The Manchester Mark 1 was one of the world's first fully general computers (that is, it was a physical embodiment of TM concept).

The Turing test

- The test was pioneering concept in the philosophy of AI and Cognitive Science; it was introduced in his classic 1950 paper "Computing Machinery and Intelligence".
- In essence, he replaced the question "Can a machine think?" by a concrete experiment:

  If a program can chat with a person (in the modern sense of using MSN, or Yahoo or Skype . . .) over an extended session, and at the end of the session the person cannot decide if he was chatting with a computer or a machine, then we must conclude we have a machine that thinks.
- Turing concluded: *"I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted."*

Legacy

- Turing died in 1954 (by suicide).
- He has been widely recognized and honored since his death. The cs equivalent of the the Nobel Prize is called the Turing Prize.
- He was in Time Magazine's list of 100 most influential people of the 20th century.

And now, back to the course . . .

What will you get out of this course?

- An understanding of the most fundamental concepts of theoretical computer science, namely that there are both computable and uncomputable functions.
- A deeper insight into what computation actually is and how it can be modeled.
- A deeper insight into computational complexity:
  - the difference between simple and complex computations
  - the concept of non-determinism

Preliminary planning of lectures

Preliminary planning:

- Section 1: Motivation & History, Sets & Proofs, Functions & Equinumerous sets
- Section 2: Turing machines & Church's thesis.
- Section 3: Uncomputability and undecidability.
- Section 4: Computational complexity

Evaluation:

- Homework assignments (33%)
- Final exam (67%)

Origins of Set Theory

- Set theory has its origins of Georg Cantor (1845-1918) a German mathematician who was interested in generalizing results in Fourier analysis.
- His investigations led him to give a detailed account of the structure of infinity (he discovered the transfinite numbers).
- Moreover, his work showed that the concept of a “set” is fundamental to mathematics.
- Currently, set theory is regarded as the standard basis of mathematics.
- Every mathematical object of interest (e.g. the numbers) can be linked to a set.
- Here we will take a rather naïve approach to set theory

Sets and membership

- A set is a collection of 'objects' (e.g., numbers, anything concrete or abstract, other sets, etc.)
- The objects in a set are called its elements or its members.
- If x is a member of a set X, then we write $x \in X$.
- Otherwise, if x is not a member of X, then we write $x \notin X$.

We can specify a set by its members in between $\{$ and $\}$:

- For example, $\{1, 2\}$ is the set that contains 1 and 2.
- However, this only works for finite (small) sets.

Sets and membership

- A set is a collection of 'objects' (e.g., numbers, anything concrete or abstract, other sets, etc.)
- The objects in a set are called its elements or its members.
- If x is a member of a set X, then we write $x \in X$.
- Otherwise, if x is not a member of X, then we write $x \notin X$.

We can specify a set by its members in between $\{$ and $\}$:

- For example, $\{1, 2\}$ is the set that contains 1 and 2.
- However, this only works for finite (small) sets.

Useful Examples

Consider the set $\{1, 3\}$. This is a two-element set:

- $1 \in \{1, 3\}$ and $3 \in \{1, 3\}$.
- but $2 \notin \{1, 3\}$.

Consider now the set $\{1, \{1, 3\}\}$. **NB:** it has two elements!

- $1 \in \{1, 3\}$ and $\{1, 3\} \in \{1, \{1, 3\}\}$.
- $3 \notin \{1, \{1, 3\}\}$.

Sets and equality

When are two sets equal?
When they contain exactly the same elements.

In other words: two sets are different **iff** one of them contains an element that is not a member of the other.

Notation: $X = Y$ if they are equal. Otherwise, $X \neq Y$.

NB: Sets are *extensional*, i.e., they are completely determined by their members.

Examples and the empty set

Examples:

- $\{1, 2\} = \{1, 2\}$ (contain exactly the same elements).
- $\{1\} \neq \{1, 2\}$ (the second contains 2 and the first does not).
- $\{1, 2\} = \{2, 1\}$?
- $\{1\} = \{1, 1\}$?

Empty set: the set that contains no object (denoted $\emptyset$)

- Represents the natural number 0 and allows the construction of all others.
- The empty set is unique, i.e., there is only one! Why?

Examples and the empty set

Examples:

- $\{1, 2\} = \{1, 2\}$ (contain exactly the same elements).
- $\{1\} \neq \{1, 2\}$ (the second contains 2 and the first does not).
- $\{1, 2\} = \{2, 1\}$?
- $\{1\} = \{1, 1\}$?

Empty set: the set that contains no object (denoted $\emptyset$)

- Represents the natural number 0 and allows the construction of all others.
- The empty set is unique, i.e., there is only one! Why?

Subset

A set X is a subset of a set Y if $x \in X$ implies $x \in Y$.

Notation: $X \subseteq Y$ if X is a subset of Y. Otherwise, $X \nsubseteq Y$.
That is, there is a member of X that does not belong to Y.

Examples:

- $\{1,3\} \subseteq \{1,2,3\}$. But $\{1,4\} \nsubseteq \{1,2,3\}$
- $\{1,\{1,3\}\} \subseteq \{1,\{1,3\},\emptyset,3\}$.

NB1: For any set X, $\emptyset \subseteq X$. Why?

NB2: $\in$ and $\subseteq$ are different concepts:

- $\{1,3\} \in \{1,\{1,3\}\}$ **but** $\{1,3\} \nsubseteq \{1,\{1,3\}\}$.
- $\{1,3\} \subseteq \{1,2,3\}$ **but** $\{1,3\} \notin \{1,2,3\}$.
- $\{1,3\} \in \{1,3,\{1,3\}\}$ **and** $\{1,3\} \subseteq \{1,3,\{1,3\}\}$.

Properties of $\subseteq$

$\subseteq$ is a partial order: For any sets X, Y, Z,

- Reflexivity: $X \subseteq X$
- Transitivity: $X \subseteq Y$ and $Y \subseteq Z$ implies $X \subseteq Z$.
- Antisymmetry: $X \subseteq Y$ and $Y \subseteq X$ implies $X = Y$.

NB: $X = Y$ iff $X \subseteq Y$ and $Y \subseteq X$.

In general: we prove $=$ by showing both of the latter.

Proper subset: $X \subsetneq Y$ if $X \subseteq Y$ but $X \neq Y$

Intersection, union, difference and the algebra of sets

Let X and Y be sets:

- Intersection: $X \cap Y = \{x : x \in X \text{ and } x \in Y\}$.
  If $X \cap Y = \emptyset$, then X and Y are said to be disjoint.
- Union: $X \cup Y = \{x : x \in X \text{ or } x \in Y\}$.
- Difference: $X \setminus Y = \{x : x \in X \text{ but } x \notin Y\}$.

Algebra of sets: $\cap, \cup, \setminus$ induce a rich algebraic structure

- Empty set rules: $X \cap \emptyset = \emptyset$, $X \cup \emptyset = X$, $X \cap (Y \setminus X) = \emptyset$
- Commutativity: $X \cap Y = Y \cap X$ and $X \cup Y = Y \cup X$
- Associativity: $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ and $X \cup (Y \cup Z) = (X \cup Y) \cup Z$
- Distributivity: $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ and $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- De Morgan rules: $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$ and $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$

NB: Such algebras are called Boolean Algebras

Intersection, union, difference and the algebra of sets

Let X and Y be sets:

- Intersection: $X \cap Y = \{x : x \in X \text{ and } x \in Y\}$.
  If $X \cap Y = \emptyset$, then X and Y are said to be disjoint.
- Union: $X \cup Y = \{x : x \in X \text{ or } x \in Y\}$.
- Difference: $X \setminus Y = \{x : x \in X \text{ but } x \notin Y\}$.

Algebra of sets: $\cap, \cup, \setminus$ induce a rich algebraic structure

- Empty set rules: $X \cap \emptyset = \emptyset$, $X \cup \emptyset = X$, $X \cap (Y \setminus X) = \emptyset$
- Commutativity: $X \cap Y = Y \cap X$ and $X \cup Y = Y \cup X$
- Associativity: $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ and
  $X \cup (Y \cup Z) = (X \cup Y) \cup Z$
- Distributivity: $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ and
  $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- De Morgan rules: $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$ and
  $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$

NB: Such algebras are called Boolean Algebras

Set of natural numbers

The set of natural numbers $0, 1, 2, 3, \ldots$ is denoted by $\mathbb{N}$ (or ω)

$\mathbb{N}$ is a fund. infinite set used to define other sets of numbers

In set theory, the set $\mathbb{N}$ is constructed using $\emptyset$:

- $0 \equiv \emptyset$,
- $1 \equiv \{\emptyset\}$ (that is $\{0\}$),
- $2 \equiv \{\emptyset, \{\emptyset\}\}$ (that is $\{0, 1\}$),
- $\ldots$
- $n + 1 \equiv \{0, 1, ..., n\} = n \cup \{n\}$ (see ref.s in the end).

Other sets of numbers

- The set $\mathbb{Z}$ of integers $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
  Clearly, $\mathbb{Z}$ is infinite and $\mathbb{N} \subsetneq \mathbb{Z}$.
- The set $\mathbb{Z}^+ = \mathbb{N}\backslash\{0\}$ of positive integers $1, 2, 3, \ldots$.
- The set $\mathbb{Z}^-$ of negative integers $-1, -2, -3, \ldots$
  Clearly $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$.
- The set $\mathbb{Q}$ of rational numbers, i.e., of the form n/m where $n \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. This set has the density property: $\forall p < q \in \mathbb{Q}, \exists r \in \mathbb{Q} : p < r < q$ (e.g., $(q + p)/2$).
- However, the Pythagoreans knew +2000 years ago that $\sqrt{2}$ (the length of the hypotenenuse of right triangle with unit sides) cannot be represented as a fraction...

Proof technique: reductio ad absurdum or proof by contradiction or indirect proof. (Exercises)

The real numbers

The set $\mathbb{R}$ of real numbers consists of $\mathbb{Q}$ together with all the non-fractional numbers (e.g., $\sqrt{2}$, π and e) needed to fill gaps.

Every real number r can be seen as the limit of a rational sequence and can be represented by an infinite decimal number. For example:

- $29.345345345\ldots$
- $0.3333333\ldots$
- $0.000008765287\ldots$

The real numbers are one of the richest and most important mathematical structures.

One of Cantor's greatest achievements was to give one of the first rigorous accounts of what $\mathbb{R}$ actually was.

Power Sets

The power set $\mathcal{P}(X)$ of a set X is the set of all subsets of X.

NB1: both X and $\emptyset$ belong to $\mathcal{P}(X)$.

NB2: $X \in \mathcal{P}(Y)$ **iff** $X \subseteq Y$.

Examples:

- $\emptyset$ has 0 elements. **NB:** $\mathcal{P}(\emptyset)$ has $1 = 2^0$ elements.
- $\mathcal{P}(\{3,5\}) = \{\{3,5\},\{3\},\{5\},\emptyset\}$. **NB:** $4 = 2^2$ elements.
- $\mathcal{P}(\{1,3,5\}) =$
  $\{\{1,3,5\},\{1,3\},\{1,5\},\{3,5\},\{1\},\{3\},\{5\},\emptyset\}$.
  NB: $8 = 2^3$ elements.

How large are power sets?

Theorem: If X has n elements, then $\mathcal{P}(X)$ has 2^n elements.

Proof: Mathematical induction.
Prove that a property P holds for every $n \in \mathbb{N}$ in two steps:

- Base case: Show that $P(0)$ holds
- Inductive step: Show that if $P(k)$ holds, $\forall k \leq n$, **then** $P(n+1)$ also holds

(See exercises!)

Question: How can we compare sizes of infinite sets?

Answer: through mappings (functions) of certain types...

How large are power sets?

Theorem: If X has n elements, then $\mathcal{P}(X)$ has 2^n elements.

Proof: Mathematical induction.
Prove that a property P holds for every $n \in \mathbb{N}$ in two steps:

- Base case: Show that $P(0)$ holds
- Inductive step: Show that if $P(k)$ holds, $\forall k \leq n$, **then** $P(n+1)$ also holds

(See exercises!)

Question: How can we compare sizes of infinite sets?

Answer: through mappings (functions) of certain types...

Functions as binary relations

A relation between X and Y is $R \subseteq X \times Y$ of ordered pairs

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}$$

NB: $\langle x, y \rangle = \langle u, v \rangle$ **iff** $x = u$ and $y = v$.

A function f with domain X and range Y is a special kind of binary relation between X and Y: for each $x \in X$, there is a unique $y \in Y$ s.t. $\langle x, y \rangle \in f$ (usually written as $f(x) = y$).

The image of f is $\mathrm{Im}(f) = \{y \in Y : y = f(x) \text{ for some } x \in X\}$.

(Counter-)Examples:

- The binary relation $\{\langle x, y \rangle \in \mathbb{R} \times \mathbb{R} : \ y = x^2\}$ is a function.
- However, $\{\langle x, y \rangle \in \mathbb{R}^+ \times \mathbb{R} : \ y^2 = x\}$ is not a function.
- The identity $id_X = \{\langle x, x \rangle : \ x \in X\}$ on a set X is a function.

Functions as binary relations

A relation between X and Y is $R \subseteq X \times Y$ of ordered pairs

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}$$

NB: $\langle x, y \rangle = \langle u, v \rangle$ **iff** $x = u$ and $y = v$.

A function f with domain X and range Y is a special kind of binary relation between X and Y: for each $x \in X$, there is a unique $y \in Y$ s.t. $\langle x, y \rangle \in f$ (usually written as $f(x) = y$).

The image of f is $\mathrm{Im}(f) = \{y \in Y : y = f(x) \text{ for some } x \in X\}$.

(Counter-)Examples:

- The binary relation $\{\langle x, y \rangle \in \mathbb{R} \times \mathbb{R} : \ y = x^2\}$ is a function.
- However, $\{\langle x, y \rangle \in \mathbb{R}^+ \times \mathbb{R} : \ y^2 = x\}$ is not a function.
- The identity $id_X = \{\langle x, x \rangle : \ x \in X\}$ on a set X is a function.

Functions as binary relations

A relation between X and Y is $R \subseteq X \times Y$ of ordered pairs

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}$$

NB: $\langle x, y \rangle = \langle u, v \rangle$ **iff** $x = u$ and $y = v$.

A function f with domain X and range Y is a special kind of binary relation between X and Y: for each $x \in X$, there is a unique $y \in Y$ s.t. $\langle x, y \rangle \in f$ (usually written as $f(x) = y$).

The image of f is $\mathrm{Im}(f) = \{y \in Y : y = f(x) \text{ for some } x \in X\}$.

(Counter-)Examples:

- The binary relation $\{\langle x, y \rangle \in \mathbb{R} \times \mathbb{R} : \ y = x^2\}$ is a function.
- However, $\{\langle x, y \rangle \in \mathbb{R}^+ \times \mathbb{R} : \ y^2 = x\}$ is not a function.
- The identity $id_X = \{\langle x, x \rangle : \ x \in X\}$ on a set X is a function.

Function composition

Let A, B, C be sets, and $g \subseteq A \times B$ and $f \subseteq B \times C$ be functions.

The composition of f with g is the function $f \circ g \subseteq A \times C$ defined by $f \circ g(a) = f(g(a))$.

NB: The concept of function can be generalized through $n+1$-ary relations $R \subseteq A_1 \times \cdots \times A_n \times A_{n+1}$ in a natural way: for each $\mathbf{x} \in A_1 \times \cdots \times A_n$ there is a unique $y \in A_{n+1}$...

Examples: arithmetical operations, aggregation functions, etc.

Injective functions

- A function f is injective if and only if distinct elements of the domain map to distinct elements of the range.
- That is, a function is injective if and only if for all x, y in its domain such that $f(x) = f(y)$, we have that $x = y$.
- Injective functions are often called *one-to-one functions*.

(Counter-)Examples:

- Let $A = \{a, b, c\}$, $f = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle\}$, and $g = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, b\rangle\}$. Then f is injective but not g.
- The real functions defined by $f(x) = x + 1$ and $g(x) = x^3$ are injective, whereas $h(x) = x^2$ is not.

Surjective functions

- A function $f \subseteq X \times Y$ is surjective if $\mathrm{Im}(f) = Y$
- Surjective functions are often called *onto functions*.

(Counter-)Examples:

- Let $A = \{a, b, c\}$, $f = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle\}$, and $g = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, b\rangle\}$. Then f is surjective but not g.
- The real function defined by $f(x) = x^3$ is surjective.
- The real function defined by $f(x) = x^2$ is not surjective.

Bijective functions (bijections)

- A function is bijective if it is both injective and surjective.
- Bijections are "invertible": if $f \subseteq X \times Y$ is bijective, then there is $g \subseteq Y \times X$ s.t. $g \circ f = id_X$ and $f \circ g = id_Y$.
- g is bijective and unique: the inverse of f and denoted f^{-1}

Examples:

- Let $A = \{a, b, c\}$, $f = \{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle\}$. We have seen that f is bijective. What is f^{-1}?
- The real function $g(x) = x + 1$ is bijective. What is g^{-1} ?
- For any set X, id_X is a bijection. What is $(id_X)^{-1}$?

Equinumerous sets

- Two sets are equinumerous (i.e., have the same number of elements) if there is a bijection between them.
- Equivalently, X and Y are equinumerous if there is an injection $f \subseteq X \times Y$ and an injection $g \subseteq Y \times X$

NB: We do not need to count! The idea of "having the same number of elements" does not depend on the notion of number.

Comparing infinite sets

- The most fundamental infinite set in set theory is $\mathbb{N}$, the set of natural numbers.
- A set X is countably infinite if there is a bijection $f \subseteq X \times \mathbb{N}$.

Example: The set $E = \{0, 2, 4, 6, 8, \ldots\}$ is countably infinite.

- Here's an obvious bijection between E and $\mathbb{N}$: $f(e) = e/2$.
- It is easy to check that f is both injective and surjective.
- Thus while it is true that $E \subsetneq \mathbb{N}$, it is also true that E and $\mathbb{N}$ have the same number of elements: E is countably infinite!

The set of integers is countably infinite

- The set of integers $\mathbb{Z}$, that is $\{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$, is also countably infinite
- Here are the first few values of a suitable bijection f: $f(0) = 0$, $f(1) = 1$, $f(-1) = 2$, $f(2) = 3$, $f(-2) = 4$, $f(3) = 5$, $f(-3) = 6$, $f(4) = 7$, $f(-4) = 8$, $\ldots$
- Precisely: $f(z) = -2z$, if $z \leq 0$, and $f(z) = 2z - 1$ if $z > 0$.
- Thus while it is true that $\mathbb{N} \subsetneq \mathbb{Z}$, it is also true that $\mathbb{Z}$ and $\mathbb{N}$ have the same number of elements. $\mathbb{Z}$ is countably infinite.

Two surprising examples

- Two much richer looking sets are can be placed in one two one correspondence with the natural numbers.
- First: $\mathbb{N} \times \mathbb{N}$ is countably infinite. That is, moving from the one dimensional infinity $\mathbb{N}$ to the two dimensional infinity $\mathbb{N} \times \mathbb{N}$ does not result in a larger set.
- Second: $\mathbb{Q}$ is also countably infinite. That is, moving from the discretely ordered set $\mathbb{N}$ to the densely ordered set $\mathbb{Q}$ does not result in a larger set.
- These results date back to 1874; they are due to Georg Cantor. Let's take a closer look . . .

$\mathbb{N} \times \mathbb{N}$ is countably infinite

$$
\begin{array}{cccc}
\vdots & \vdots & \vdots & \dots \\
\langle 0,2 \rangle & \langle 1,2 \rangle & \langle 2,2 \rangle & \dots \\
\langle 0,1 \rangle & \langle 1,1 \rangle & \langle 2,1 \rangle & \dots \\
\langle 0,0 \rangle & \langle 1,0 \rangle & \langle 2,0 \rangle & \dots
\end{array}
$$

$\mathbb{N} \times \mathbb{N}$ is countably infinite

$$\begin{array}{cccc} \vdots & \vdots & \vdots & \dots \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 2,2\rangle & \dots \\ \langle 0,1\rangle & \langle 1,1\rangle & \langle 2,1\rangle & \dots \\ \langle 0,0\rangle & \langle 1,0\rangle & \langle 2,0\rangle & \dots \end{array}$$

Let's count these ordered pairs: 0

$\mathbb{N} \times \mathbb{N}$ is countably infinite

$$\begin{array}{cccc} \vdots & \vdots & \vdots & \dots \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 2,2\rangle & \dots \\ \langle 0,1\rangle & \langle 1,1\rangle & \langle 2,1\rangle & \dots \\ \langle 0,0\rangle & \langle 1,0\rangle & \langle 2,0\rangle & \dots \end{array}$$

Let's count these ordered pairs: 1

$\mathbb{N} \times \mathbb{N}$ is countably infinite

$$\begin{array}{cccc} \vdots & \vdots & \vdots & \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 2,2\rangle & \dots \\ \langle 0,1\rangle & \langle 1,1\rangle & \langle 2,1\rangle & \dots \\ \langle 0,0\rangle & \langle 1,0\rangle & \langle 2,0\rangle & \dots \end{array}$$

Let's count these ordered pairs: 2

$\mathbb{N} \times \mathbb{N}$ is countably infinite

$$\begin{array}{cccc} \vdots & \vdots & \vdots & \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 2,2\rangle & \dots \\ \langle 0,1\rangle & \langle 1,1\rangle & \langle 2,1\rangle & \dots \\ \langle 0,0\rangle & \langle 1,0\rangle & \langle 2,0\rangle & \dots \end{array}$$

Let's count these ordered pairs: 3

$\mathbb{N} \times \mathbb{N}$ is countably infinite

$$\begin{array}{cccc} \vdots & \vdots & \vdots & \dots \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 2,2\rangle & \dots \\ \langle 0,1\rangle & \langle 1,1\rangle & \langle 2,1\rangle & \dots \\ \langle 0,0\rangle & \langle 1,0\rangle & \langle 2,0\rangle & \dots \end{array}$$

Let's count these ordered pairs: And so on...

It is not particularly hard to write down an expression that captures this idea:

$$j(m,n) = [(m+n)^2 + 3m + n]/2$$

And it is not difficult to show that j is a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

Lots of interesting sets are countably infinite

- In particular, the set of rational numbers $\mathbb{Q}$ is countably infinite.
- This can be seen by a similar argument to the one we just saw for $\mathbb{N} \times \mathbb{N}$. Why is this?
- This makes us wonder: are all infinite sets countable?
- The answer is "no": Georg Cantor proved the celebrated result that there can not be a bijection between $\mathbb{R}$ and $\mathbb{N}$.
- That is, $\mathbb{R}$ is not countably infinite... it is bigger!
- His proof was a reductio ad absurdum, i.e., he assumed that such a bijection existed, and showed that this assumption led to a contradiction.
- He obtained the contradiction by a very elegant argument that has come to be known as the diagonal argument.

Lots of interesting sets are countably infinite

- In particular, the set of rational numbers $\mathbb{Q}$ is countably infinite.
- This can be seen by a similar argument to the one we just saw for $\mathbb{N} \times \mathbb{N}$. Why is this?
- This makes us wonder: are all infinite sets countable?
- The answer is "no": Georg Cantor proved the celebrated result that there can not be a bijection between $\mathbb{R}$ and $\mathbb{N}$.
- That is, $\mathbb{R}$ is not countably infinite... it is bigger!
- His proof was a reductio ad absurdum, i.e., he assumed that such a bijection existed, and showed that this assumption led to a contradiction.
- He obtained the contradiction by a very elegant argument that has come to be known as the diagonal argument.

Power sets are big!

We will illustrate a diagonal argument for showing that:
there is no set X in bijection with its power set $\mathcal{P}(X)$
(actually, this can be used to show Cantor's result!).

Some preliminary observations:

- First: recall that the result is true for finite sets since, if a finite set X has n elements, then $\mathcal{P}(X)$ has 2^n elements! So for finite sets, no bijection can exist.
- Second: for any X, there is an injective function from X to $\mathcal{P}(X)$ (just take $y \mapsto \{y\}$).
- Hence: $\mathcal{P}(X)$ cannot be smaller than X!
- However: these remarks don't show that it is impossible (at least for infinite sets) to find a bijection between X to $\mathcal{P}(X)$.
- To show this, we need diagonalization...

What we will do...

Let X be any set, and **suppose** $g\colon X \to \mathcal{P}(X)$ is a bijection.

We will use diagonalization to define $D_g \subseteq X$, the diagonal set of g, that is is not in the image of g.

NB: This would show that g is not surjective!

But can we do this? After all, we know little about X and g.

What we will do...

Let X be any set, and **suppose** $g\colon X \to \mathcal{P}(X)$ is a bijection.

We will use diagonalization to define $D_g \subseteq X$, the diagonal set of g, that is is not in the image of g.

NB: This would show that g is not surjective!

But can we do this? After all, we know little about X and g.

Diagonalization!

Given g, define the diagonal D_g of g as:

$$D_g = \{z \in X : z \notin g(z)\}$$

Clearly: $D_g \subseteq X$, i.e., $D_g \in \mathcal{P}(X)$.

But: for each $z \in X : z \in D_g$ iff $z \notin g(z)$

Hence: for each z, $D_g \neq g(z)$, i.e., D_g is not in the image of g!

Consequences

- This argument shows that no function g from X to $\mathcal{P}(X)$ can be surjective.
- This is because, given any such function g, we have that D_g is not in the image of g.
- Hence no function g from X to $\mathcal{P}(X)$ can be a bijection.
- That is, for any set X we have that $\mathcal{P}(X)$ is bigger than X.
- In particular, $\mathcal{P}(\mathbb{N})$ is bigger than $\mathbb{N}$. $\mathcal{P}(\mathbb{N})$ is certainly not countably infinite - it is bigger.
- And $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ is bigger than $\mathcal{P}(\mathbb{N})$.
- And $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$ is bigger than $\mathcal{P}(\mathcal{P}(\mathbb{N}))$.
- And so on and so on: the infinities just keep on getting bigger and bigger and the process never stops . . .

Consequences

- This argument shows that no function g from X to $\mathcal{P}(X)$ can be surjective.
- This is because, given any such function g, we have that D_g is not in the image of g.
- Hence no function g from X to $\mathcal{P}(X)$ can be a bijection.
- That is, for any set X we have that $\mathcal{P}(X)$ is bigger than X.
- In particular, $\mathcal{P}(\mathbb{N})$ is bigger than $\mathbb{N}$. $\mathcal{P}(\mathbb{N})$ is certainly not countably infinite - it is bigger.
- And $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ is bigger than $\mathcal{P}(\mathbb{N})$.
- And $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$ is bigger than $\mathcal{P}(\mathcal{P}(\mathbb{N}))$.
- And so on and so on: the infinities just keep on getting bigger and bigger and the process never stops . . .

Summary of Section 1

- We have mentioned key concepts of theoretical CS such as Turing machines and Church's Thesis.
- These concepts formalize the notions of "computable" and "uncomputable".
- We saw some implications in other domains such as AI.
- We discussed key notions of set theory and the algebra of sets using $\cup$, $\cap$, $\setminus$ and $\mathcal{P}$.
- There are many "standard" mathematical sets, the simplest (and smallest) being $\emptyset$.
- We met a number of standard infinite sets of numbers, namely $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Z}^-$, $\mathbb{Q}$, and $\mathbb{R}$.
- We also introduced two key proof techniques: reductio ab adsurdum and mathematical induction.

Summary of Section 1

- We have mentioned key concepts of theoretical CS such as Turing machines and Church's Thesis.
- These concepts formalize the notions of "computable" and "uncomputable".
- We saw some implications in other domains such as AI.
- We discussed key notions of set theory and the algebra of sets using $\cup$, $\cap$, $\setminus$ and $\mathcal{P}$.
- There are many "standard" mathematical sets, the simplest (and smallest) being $\emptyset$.
- We met a number of standard infinite sets of numbers, namely $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Z}^-$, $\mathbb{Q}$, and $\mathbb{R}$.
- We also introduced two key proof techniques: reductio ab adsurdum and mathematical induction.

Summary of Section 1

- We have mentioned key concepts of theoretical CS such as Turing machines and Church's Thesis.
- These concepts formalize the notions of "computable" and "uncomputable".
- We saw some implications in other domains such as AI.
- We discussed key notions of set theory and the algebra of sets using $\cup$, $\cap$, $\setminus$ and $\mathcal{P}$.
- There are many "standard" mathematical sets, the simplest (and smallest) being $\emptyset$.
- We met a number of standard infinite sets of numbers, namely $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Z}^-$, $\mathbb{Q}$, and $\mathbb{R}$.
- We also introduced two key proof techniques: reductio ab adsurdum and mathematical induction.

Summary of Section 1 (cont.)

- We formalized the concept of function through binary relations, and defined important properties of functions (injective, surjetive, bijective).
- If there is a bijection between two sets, then their elements can be paired off and the two sets have the same size.
- We discussed countably infinite sets (that are in bijection with $\mathbb{N}$) and saw many, including $\mathbb{Q}$ and $\mathbb{N} \times \mathbb{N}$.
- We also saw that $\mathbb{R}$ is not countably infinite, it is bigger, and we illustrated diagonalization has a standard technique for proving the impossiblity of certain bijections.
- In particular, diagonalization was used to show that no set X is in bijection with its power set $\mathcal{P}(X)$.
- This result shows that there is an infinite hierarchy of infinities, created by starting with $\mathbb{N}$ and iterating the process of taking power sets.

Summary of Section 1 (cont.)

- We formalized the concept of function through binary relations, and defined important properties of functions (injective, surjetive, bijective).
- If there is a bijection between two sets, then their elements can be paired off and the two sets have the same size.
- We discussed countably infinite sets (that are in bijection with $\mathbb{N}$) and saw many, including $\mathbb{Q}$ and $\mathbb{N} \times \mathbb{N}$.
- We also saw that $\mathbb{R}$ is not countably infinite, it is bigger, and we illustrated diagonalization has a standard technique for proving the impossiblity of certain bijections.
- In particular, diagonalization was used to show that no set X is in bijection with its power set $\mathcal{P}(X)$.
- This result shows that there is an infinite hierarchy of infinities, created by starting with $\mathbb{N}$ and iterating the process of taking power sets.

Summary of Section 1 (cont.)

- We formalized the concept of function through binary relations, and defined important properties of functions (injective, surjetive, bijective).
- If there is a bijection between two sets, then their elements can be paired off and the two sets have the same size.
- We discussed countably infinite sets (that are in bijection with $\mathbb{N}$) and saw many, including $\mathbb{Q}$ and $\mathbb{N} \times \mathbb{N}$.
- We also saw that $\mathbb{R}$ is not countably infinite, it is bigger, and we illustrated diagonalization has a standard technique for proving the impossiblity of certain bijections.
- In particular, diagonalization was used to show that no set X is in bijection with its power set $\mathcal{P}(X)$.
- This result shows that there is an infinite hierarchy of infinities, created by starting with $\mathbb{N}$ and iterating the process of taking power sets.

References on Turing, Set Theory, Diagonalization, ...

- The Wikipedia article on Alan Turing is quite informative.
- Elements of Set Theory, by Herbert Enderton, Academic Press 1977. A good introduction to Set Theory.
- Naive Set Theory, by Paul Halmos, Springer, 1970.
- In french, Théorie des ensembles by Krivine is a good reference. But not recommended for beginners.
- The Wikipedia articles on reductio ad absurdum and mathematical induction are also relevant.
- See also Diagonalization and Self-Reference, by Raymond Smullyan, Oxford University Press, 1994.