

$$[n] = \{0, 1, \dots, n-1\}$$

Characteristic (or indicator) functions

$$\mathcal{P}(A) \cong (A \Rightarrow [2])$$

$$\chi: \mathcal{P}(A) \rightarrow (A \Rightarrow [2])$$

defined as, for $S \subseteq A$,

$$\chi_S(a) = \begin{cases} 1 & a \in S \\ 0 & a \notin S \end{cases}$$

$$\forall a \in A.$$

$$\varphi: (A \Rightarrow [2]) \rightarrow \mathcal{P}(A)$$

defined by, for $f: A \rightarrow [2]$,

$$\varphi(f) = \{x \in A \mid f(x) = 1\}$$


exercise

establish
the bijective
correspondence.

Finite cardinality

Definition 136 A set A is said to be finite whenever $A \cong [n]$ for some $n \in \mathbb{N}$, in which case we write $\#A = n$.

Theorem 137 For all $m, n \in \mathbb{N}$,

1. $\mathcal{P}([n]) \cong [2^n]$  $\mathcal{P}(\{0, \dots, n-1\})$
 $\cong \{0, 1, \dots, 2^n - 1\}$
2. $[m] \times [n] \cong [m \cdot n]$
3. $[m] \uplus [n] \cong [m + n]$
4. $([m] \Rightarrow [n]) \cong [(n + 1)^m]$
5. $([m] \Rightarrow [n]) \cong [n^m]$
6. $\text{Bij}([n], [n]) \cong [n!]$

Infinity axiom

There is an infinite set, containing \emptyset and closed under successor.

Bijections

Proposition 138 For a function $f : A \rightarrow B$, the following are equivalent.

1. f is bijective.

2. $\forall b \in B. \exists! a \in A. f(a) = b.$

3. $(\forall b \in B. \exists a \in A. f(a) = b)$

\wedge

$(\forall a_1, a_2 \in A. f(a_1) = f(a_2) \implies a_1 = a_2)$

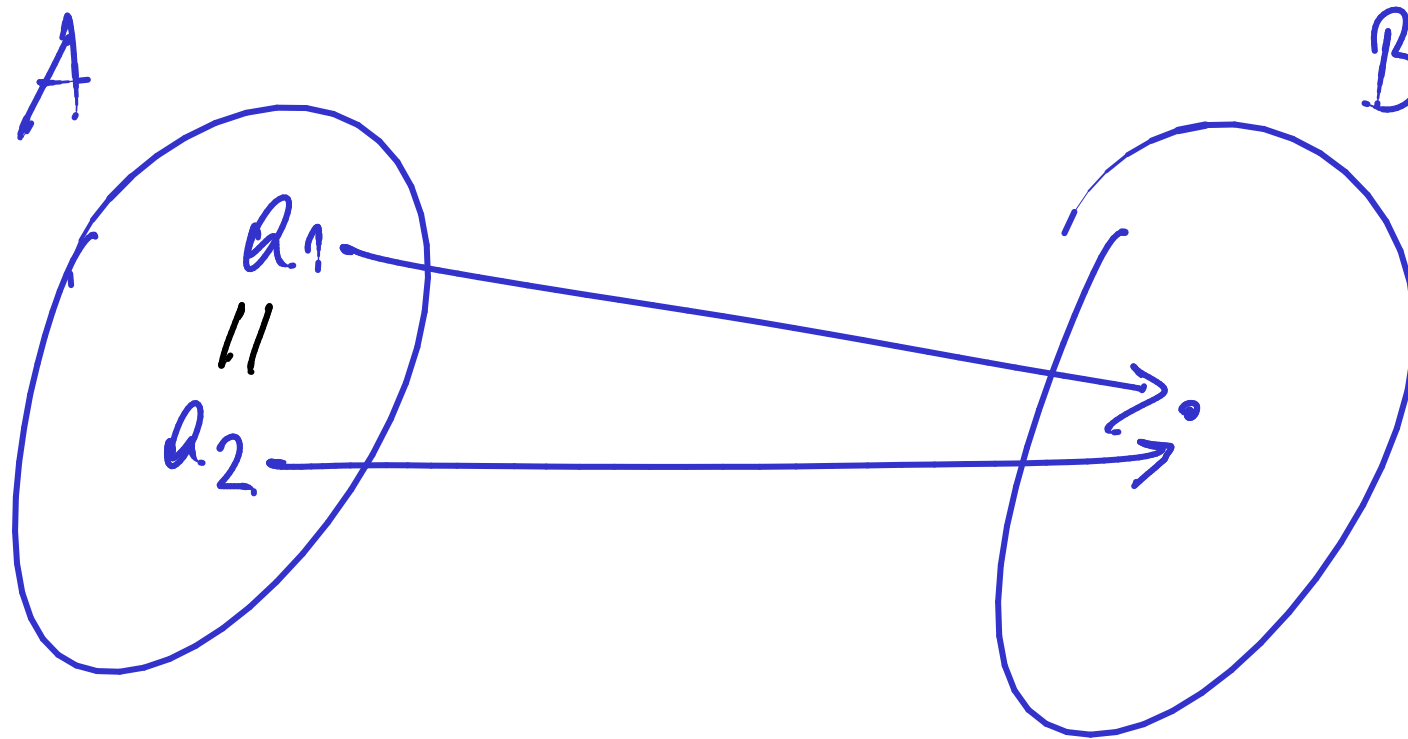
SURJECTIVITY

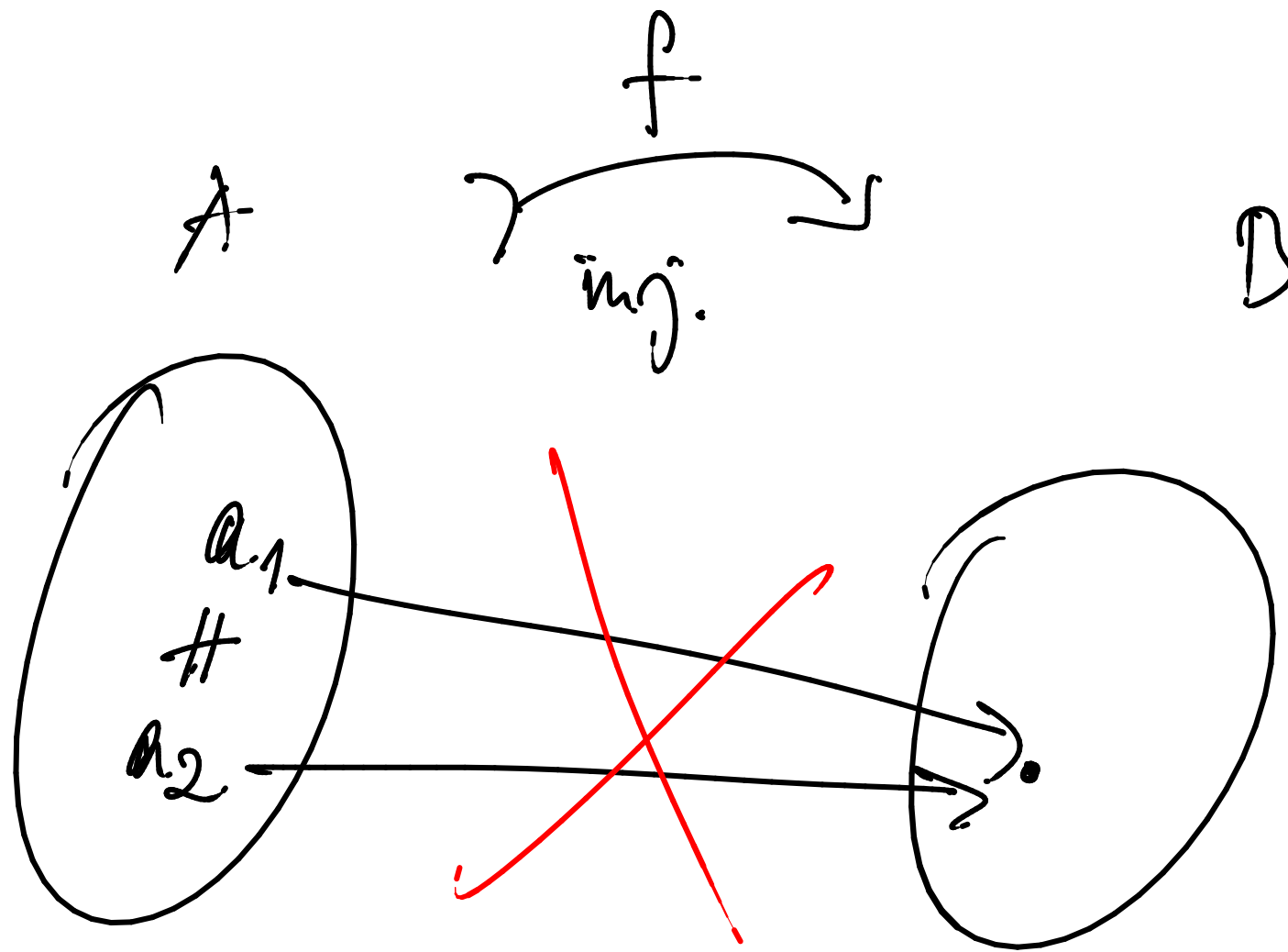
INJECTIVITY.

Injections

Definition 145 A function $f : A \rightarrow B$ is said to be injective, or an injection, and indicated $f : A \rightarrowtail B$ whenever

$$\forall a_1, a_2 \in A. (f(a_1) = f(a_2)) \implies a_1 = a_2 .$$





Intuitively an injection $f: A \rightarrow B$ gives a "copy" of A in B.

$$\{\cdot\}: A \rightarrow \mathcal{P}(A)$$

$$\{ \cdot \} \text{ def } \{\cdot\}(a) \stackrel{\text{def}}{=} \{a\} \quad \forall a \in A$$

is injective.

$\#A \leq \#B$ iff def There is an injection from A to B .

E.g. $\#A \leq \#\mathcal{P}(A)$

Given $f: A \rightarrow B$, is it possible to obtain every output $b \in B$ from an input of A via f ?
Surjections are exactly those functions f for which this is **Surjections** the case.

Definition 139 A function $f: A \rightarrow B$ is said to be surjective, or a surjection, and indicated $f: A \twoheadrightarrow B$ whenever

$$\forall b \in B. \exists a \in A. f(a) = b .$$

Enumerability

Definition 142

1. A set A is said to be enumerable whenever there exists a surjection $\mathbb{N} \rightarrow A$, referred to as an enumeration.
2. A countable set is one that is either empty or enumerable.

Given

$$e: \mathbb{N} \rightarrow A$$

$$\{e(0), e(1), e(2), \dots, e(n), \dots\} = A$$

$$\| \{e(n) \in A \mid n \in \mathbb{N}\} \|$$

$$\| \{a \in A \mid \exists n \in \mathbb{N}. a = e(n)\} \|$$

Proposition 143 Every non-empty subset of an enumerable set is enumerable.

PROOF: A enumerable, $e: \mathbb{N} \rightarrow A$
 S non-empty subset of A , $s \in S \subseteq A$.

R.T.P.: S enumerable. $\equiv e': \mathbb{N} \rightarrow S$?

$$e'(n) = \text{def} \begin{cases} e(n), & e(n) \in S \\ s, & \text{otherwise} \end{cases} \quad n \in \mathbb{N}$$



enumerable A, B

$$e_A: \mathbb{N} \rightarrow A$$

$$e_B: \mathbb{N} \rightarrow B$$

$$\rightsquigarrow ? e: \mathbb{N} \rightarrow A \times B$$

$$e'(n, m) \stackrel{\text{def}}{=} (e_A n, e_B m)$$

Countability

$$\mathbb{N} \cong \mathbb{N} \times \mathbb{N} \xrightarrow{e'} A \times B$$

def

$$\xrightarrow{e}$$

Proposition 144

1. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable sets.

2. The product and disjoint union of countable sets is countable.

3. Every finite set is countable.

4. Every subset of a countable set is countable.

Unbounded cardinality

Theorem 156 (Cantor's diagonalisation argument) For every set A , no surjection from A to $\mathcal{P}(A)$ exists.

PROOF:

E.g. $A = \mathcal{N}$

~~$\mathcal{N} \rightarrow$~~ $\mathcal{P}(\mathcal{N}) \cong (\mathcal{N} \Rightarrow \{2\})$

infinite
sequences of
0, 1's

⇓ there is no bijection
from A to $\mathcal{P}(A)$

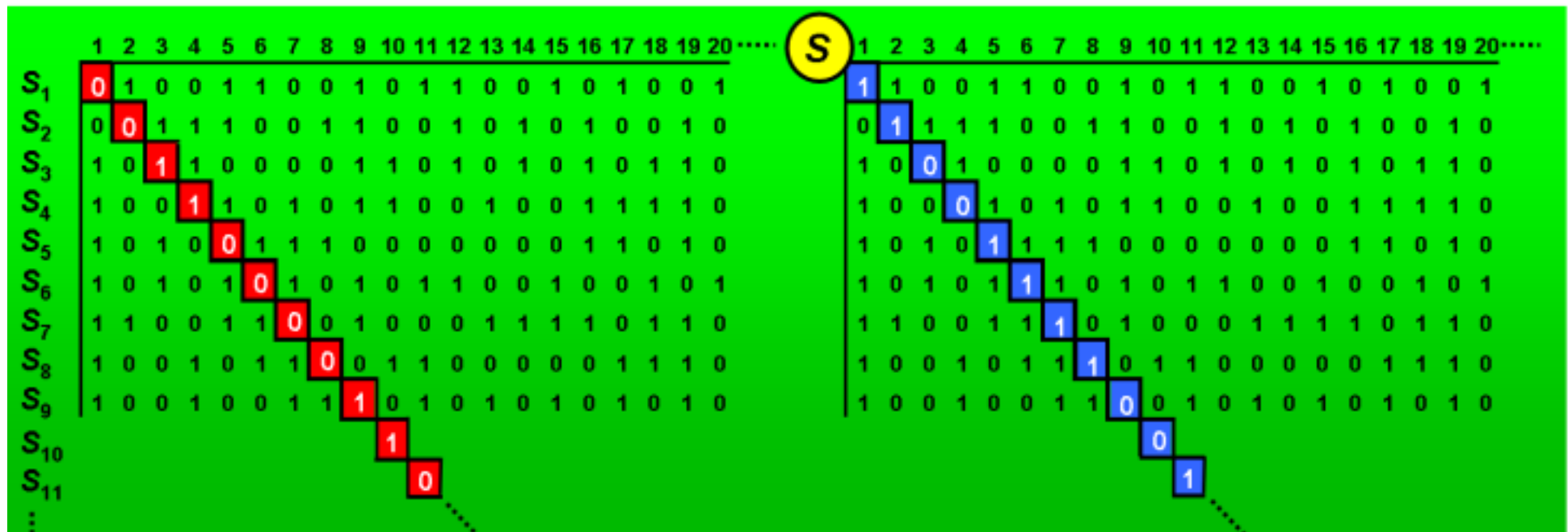
($A \neq \mathcal{P}(A)$)

So A and $\mathcal{P}(A)$ have
different cardinalities.

$\# A < \# \mathcal{P}(A) < \# \mathcal{P}\mathcal{P}A < \# \mathcal{P}\mathcal{P}\mathcal{P}A < \dots$

THEOREM OF THE DAY

Cantor's Uncountability Theorem *There are uncountably many infinite 0-1 sequences.*



Proof: Suppose you *could* count the sequences. Label them in order: S_1, S_2, S_3, \dots , and denote by $S_i(j)$ the j -th entry of sequence S_i . Now define a new sequence, S , whose i -th entry is $S_i(i) + 1 \pmod{2}$. So S is $S_1(1) + 1, S_2(2) + 1, S_3(3) + 1, S_4(4) + 1, \dots$, with all entries remaindered modulo 2. S is certainly an infinite sequence of 0s and 1s. So it must appear in our list: it is, say, S_k , so its k -th entry is $S_k(k)$. But this is, by definition, $S_k(k) + 1 \pmod{2} \neq S_k(k)$. So we have contradicted the possibility of forming our enumeration. QED.

The theorem establishes that the real numbers are *uncountable* — that is, they cannot be enumerated in a list indexed by the positive integers (1, 2, 3, ...). To see this informally, consider the infinite sequences of 0s and 1s to be the binary expansions of fractions (e.g. $0.010011\dots = 0/2 + 1/4 + 0/8 + 0/16 + 1/32 + 1/64 + \dots$). More generally, it says that the set of subsets of a countably infinite set is uncountable, and to see *that*, imagine every 0-1 sequence being a different recipe for building a subset: the i -th entry tells you whether to include the i -th element (1) or exclude it (0).

Georg Cantor (1845–1918) discovered this theorem in 1874 but it apparently took another twenty years of thought about what were then new and controversial concepts: ‘sets’, ‘cardinalities’, ‘orders of infinity’, to invent the important proof given here, using the so-called *diagonalisation method*.

Web link: www.math.hawaii.edu/~dale/godel/godel.html. There is an [interesting discussion](http://mathoverflow.net) on mathoverflow.net about the history of diagonalisation: type ‘earliest diagonal’ into their search box.

Further reading: *Mathematics: the Loss of Certainty* by Morris Kline, Oxford University Press, New York, 1980.



Corollary 159 *The sets*

$$\mathcal{P}(\mathbb{N}) \cong (\mathbb{N} \Rightarrow [2]) \cong [0, 1] \cong \mathbb{R}$$

are not enumerable.

Corollary 160 *There are non-computable infinite sequences of bits.*

Assume $A \xrightarrow{e} \mathcal{P}(A)$

Define $S \in \mathcal{P}(A)$

by $S = \{x \in A \mid x \notin e(x)\}$

there exists $a \in A$ s.t. $e(a) = S$

$\forall x \in A. x \in e(a) \Leftrightarrow x \in S$

implies $\forall x \in A. x \in e(a) \Leftrightarrow x \notin e(x)$
 $a \in e(a) \Leftrightarrow a \notin e(a)$ a contradiction \square

Definition 157 A fixed-point of a function $f : X \rightarrow X$ is an element $x \in X$ such that $f(x) = x$.

Theorem 158 (Lawvere's fixed-point argument) For sets A and X , if there exists a surjection $A \twoheadrightarrow (A \Rightarrow X)$ then every function $X \rightarrow X$ has a fixed-point; and hence X is a singleton.

PROOF: $e : A \twoheadrightarrow (A \Rightarrow X)$

$$f : X \rightarrow X$$

Define $A \rightarrow X : a \mapsto f(e a a)$

There is $\alpha \in A$ s.t. $e(\alpha) = \varphi \Rightarrow e(\alpha)(\alpha) = \varphi(\alpha)$

$e \alpha \alpha$ is a fixed point of f . \square $f(e \alpha \alpha)$

Axiom of choice

Every surjection has a section.

Replacement axiom

The direct image of every definable functional property on a set is a set.

$$\begin{array}{ccc} i \in I & \longmapsto & A_i \\ \text{Set} & & \text{sets} \end{array}$$

$$\{A_i \mid i \in I\} \text{ set.}$$

Set-indexed constructions

For every mapping associating a set A_i to each element of a set I , we have the set

$$\bigcup_{i \in I} A_i = \bigcup \{A_i \mid i \in I\} = \{a \mid \exists i \in I. a \in A_i\} .$$

Examples:

1. Indexed disjoint unions:

$$\bigsqcup_{i \in I} A_i = \bigcup_{i \in I} \{i\} \times A_i$$

2. Finite sequences on a set A :

$$A^* = \bigsqcup_{n \in \mathbb{N}} A^n$$

Foundation axiom

The membership relation is well-founded.

Thereby, providing a

Principle of \in -Induction .