Uncountable Cardinality

Theorem: The sets

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

are not countable.

<u>**NB**</u>: Suppose $\mathbb{N} \overset{e}{\twoheadrightarrow} \mathcal{P}(\mathbb{N})$

Then

$$\begin{tikzcd}
\mathbb{N} \arrow[r, two heads, "e'"] \arrow[dr, "e"'] & (\mathbb{N} \Rightarrow [2]) \arrow[d, phantom, "\cong" rotate=90] \\
& \mathcal{P}(\mathbb{N})
\end{tikzcd}$$

$$\mathbb{N} \xrightarrow{e} (\mathbb{N} \Rightarrow [2]) \ni s$$

Then $\exists k \in \mathbb{N}.\ e(k) = s$

$$e(k)(k) = s(k) = \overline{e(k)(k)} \quad ↯$$

$$\begin{array}{lllllll}
 & s(0) & s(1) & \cdots & s(n) & \cdots & n \in \mathbb{N} \\
e(0) & e(0)(0) & e(0)(1) & \cdots & e(0)(n) & \cdots & \\
e(1) & e(1)(0) & e(1)(1) & \cdots & e(1)(n) & \cdots & \\
\vdots & & & & & & \\
e(n) & e(n)(0) & e(n)(1) & \cdots & e(n)(n) & \cdots & \\
\vdots & & & & & \ddots &
\end{array}$$

Let $s : \mathbb{N} \to [2]$

$$s(n) \overset{def}{=} \overline{e(n)(n)}$$

Also there is no $\mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$

Exercise: Show it by diagonalisation

Corollary: The sets

$$[0,1] \subseteq \mathbb{R}$$

are not countable.

$$\begin{aligned} (\mathbb{N} \Rightarrow [2]) &\overset{\subseteq}{\twoheadrightarrow} [0,1] \\ s &\longmapsto \sum_{\substack{i \\ s(i)=1}} \frac{1}{2^{i+1}} \end{aligned}$$

Unbounded cardinality

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

PROOF:

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

$$S^{e} = \{ a \in A \mid a \notin e(a) \}$$

$$\exists \alpha \in A.\ e(\alpha) = S$$

$$\alpha \in e(\alpha) \Leftrightarrow \alpha \in S \Leftrightarrow \alpha \notin e(\alpha) \ \lightning$$

$\boxtimes$

Corollary: For all sets A, there is no surjection from A to $(A \Rightarrow [2])$

Because

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

Definition 157 *A* fixed-point *of a function* $f : X \to X$ *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* $X \to X$ *has a fixed-point; and hence* X *is a singleton.*

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

Let $f : X \to X$ and define

$s : A \to X$, $s(a) = f(e(a)(a))$

$\exists \alpha.\ e(\alpha) = s$

$e(\alpha)(\alpha) = s(\alpha) = f(e(\alpha)(\alpha))$.

$\boxtimes$

If every function on X has a fixed-point then X is a singleton.

$x_1 \in X$, $x_2 \in X$

$x_1 \neq x_2$

Define

$$X \to X : \begin{cases} x_1 \mapsto x_2 \\ x \neq x_1 \mapsto x_1 \end{cases}$$

Corollary 159 *The sets*

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

are not enumerable.

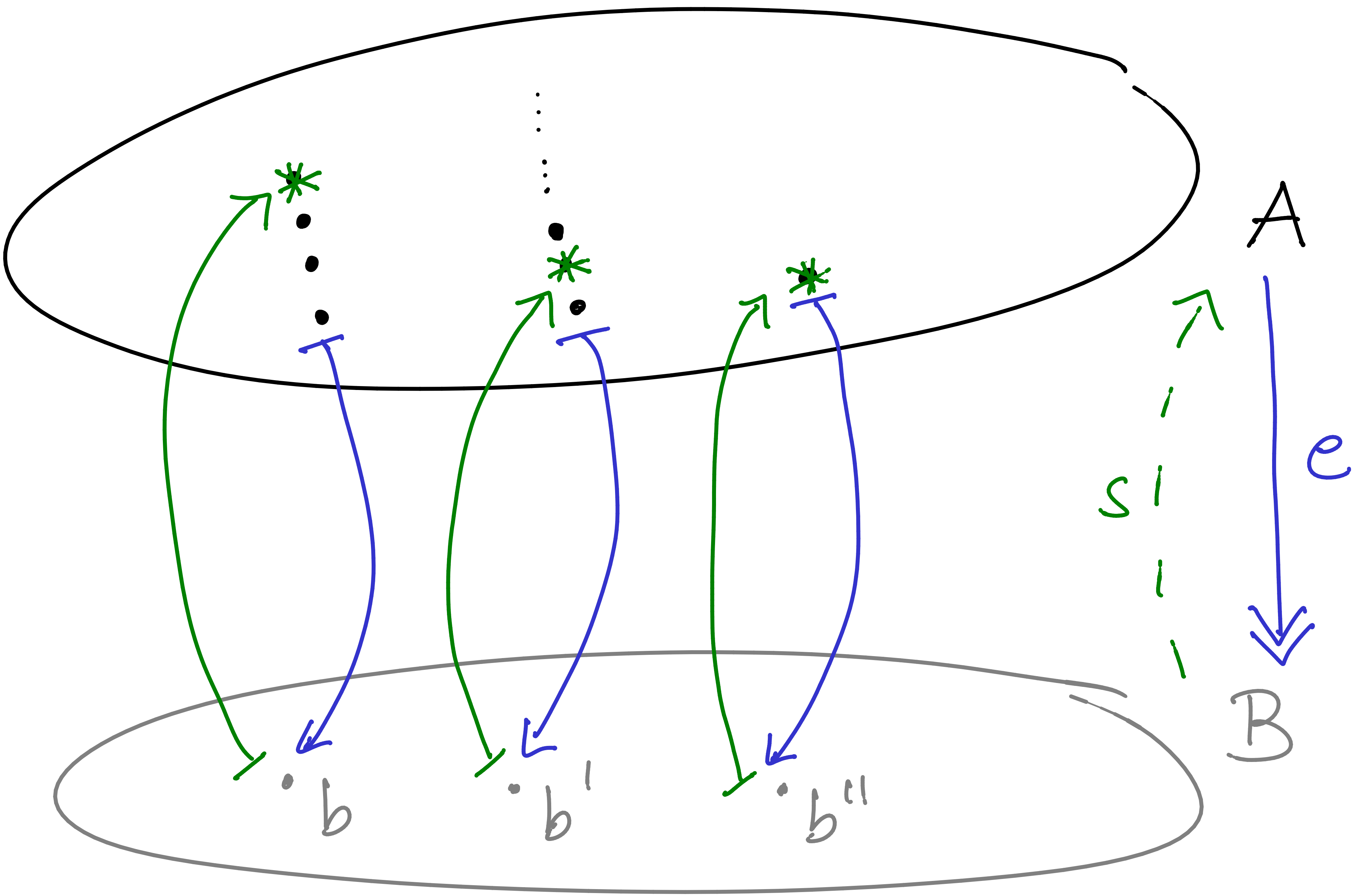
Corollary 160 *There are* non-computable *infinite sequences of bits.*

Axiom of choice

$\boxed{\text{Every surjection has a section.}}$

$$\begin{tikzcd} A \arrow[d, two heads, "e"] \\ B \arrow[u, bend left, dashed, "\exists s"] \end{tikzcd}$$

$e \circ s = id_B$


A
B
e
s
b
b'
b''

NB: Every section-retraction pair

$$\begin{tikzcd} A \arrow[r, "r"] & B \arrow[l, bend left, "s"] \end{tikzcd} \qquad r \circ s = id_B$$

is such that

- the retraction $r : A \to B$ is a surjection

and

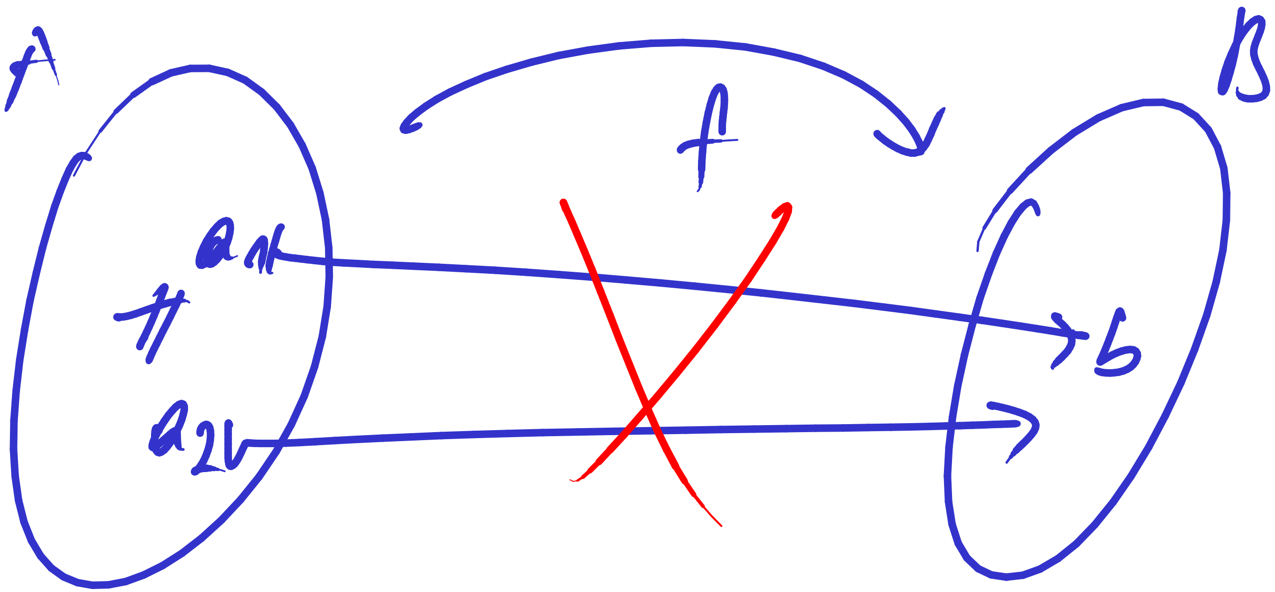
- the section $s : B \to A$ is an injection

$$s(a_1) = s(a_1) \Rightarrow \underset{\displaystyle a_1}{\underset{\parallel}{r(s(a_1))}} = \underset{\displaystyle a_2}{\underset{\parallel}{r(s(a_2))}}$$

Injections

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

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



Proposition: Every section is an injection.

Proposition: Let X be a set.

(i) The unique function from the empty set to X is an injection; and

(ii) it is a section iff X is empty.

$$\begin{tikzcd} \emptyset \arrow[r, "\exists! u"] & A \arrow[l, bend left, dashed, "r?"] \end{tikzcd}$$

<u>NB</u>: There are no functions from a non-empty set to the empty set.

Theorem 146 *The identity function is an injection, and the composition of injections yields an injection.*

The set of injections from A to B is denoted

$$\mathrm{Inj}(A, B)$$

and we thus have

$$\begin{tikzcd}
 & \mathrm{Sur}(A,B) \arrow[dr, phantom, sloped, "\subseteq"] & \\
\mathrm{Bij}(A,B) \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \mathrm{Fun}(A,B) \subseteq \mathrm{PFun}(A,B) \subseteq \mathrm{Rel}(A,B) \\
 & \mathrm{Inj}(A,B) \arrow[ur, phantom, sloped, "\subseteq"] &
\end{tikzcd}$$

with

$$\mathrm{Bij}(A, B) = \mathrm{Sur}(A, B) \cap \mathrm{Inj}(A, B) \quad .$$

Proposition 147 *For all finite sets* A *and* B,

$$\#\mathrm{Inj}(A,B) = \begin{cases} \binom{\#B}{\#A}\cdot(\#A)! & \text{, if } \#A \le \#B \\ 0 & \text{, otherwise} \end{cases}$$

PROOF IDEA:

$$\begin{array}{cccc}
a_1 & a_2 & a_3 \;\cdots & a_m \\
\downarrow & \downarrow & \downarrow & \downarrow \\
b_1 & b_1 & b_1 & \vdots \\
b_2 & b_2 & \times & \\
b_{i_1} & \times & \times & \\
\vdots & \vdots & \vdots & \\
b_n & b_n & b_n &
\end{array}$$

$$n \times (n-1) \times (n-2) \times \cdots \times (n-m+1)$$

$$\frac{n!}{(n-m)!} \text{ injections}$$

$\boxtimes$

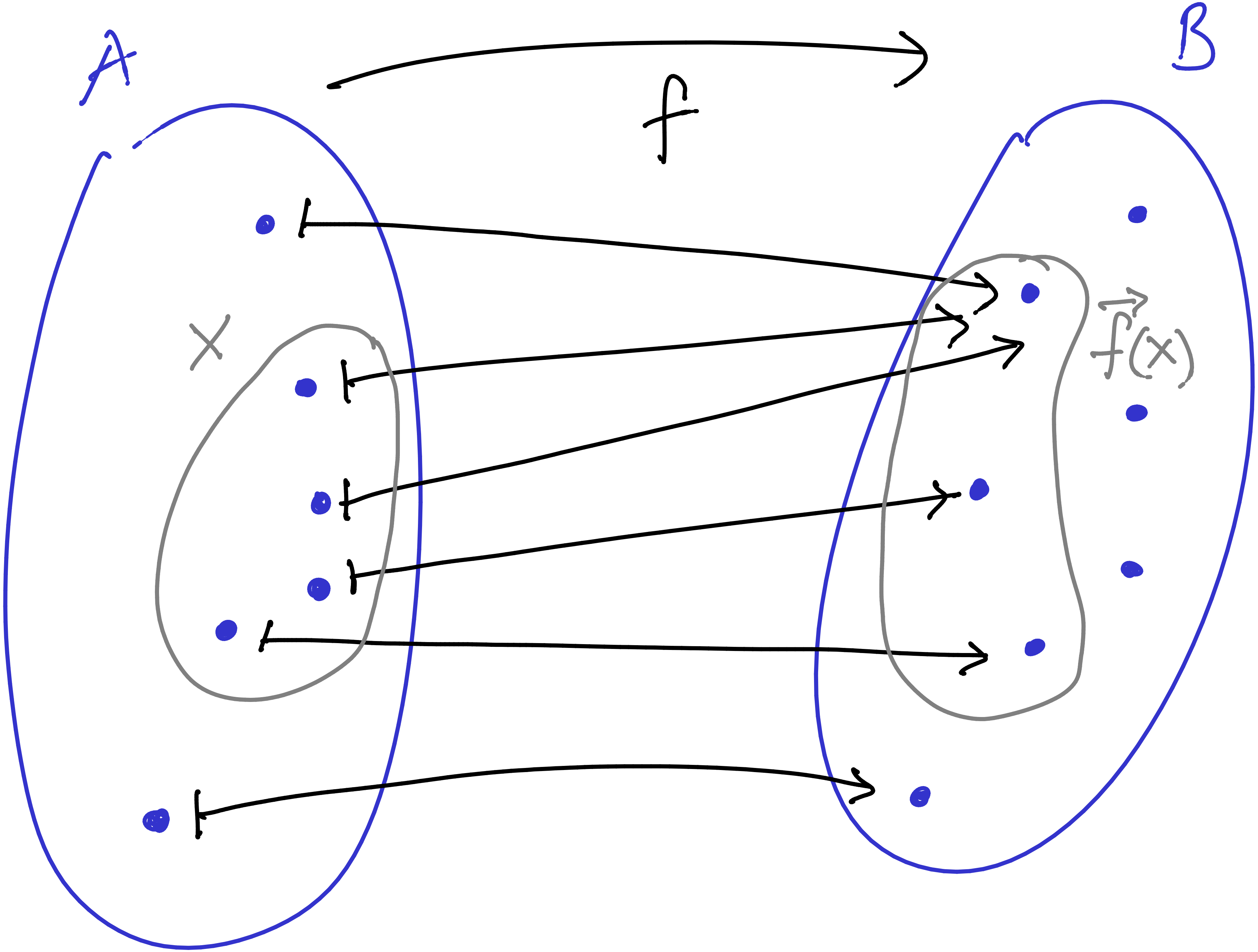
Direct and Inverse Images

Functional Images

Definition Let $f : A \to B$ be a function. The <u>direct image</u> of $X \subseteq A$ under f is the set $\vec{f}(X) \subseteq B$, defined as

$$\vec{f}(X) = \{ b \in B \mid \exists x \in X.\ f(x) = b \}$$

$$= \{ f(x) \in B \mid x \in X \}$$


A
B
f
X
$\vec{f}(X)$

Proposition For all functions $f : A \to B$, the mapping

$$A \ni a \longmapsto f(a)$$

determines a function

$$f' : A \longrightarrow \vec{f}(A)$$

that is surjective.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "f'"'] & B \\ & \vec{f}(A) \arrow[u, phantom, sloped, "\subseteq"] \end{tikzcd}$$

Moreover, whenever $f : A \to B$ is injective, $f' : A \to \vec{f}(A)$ is bijective.

Injective functions preserve cardinality

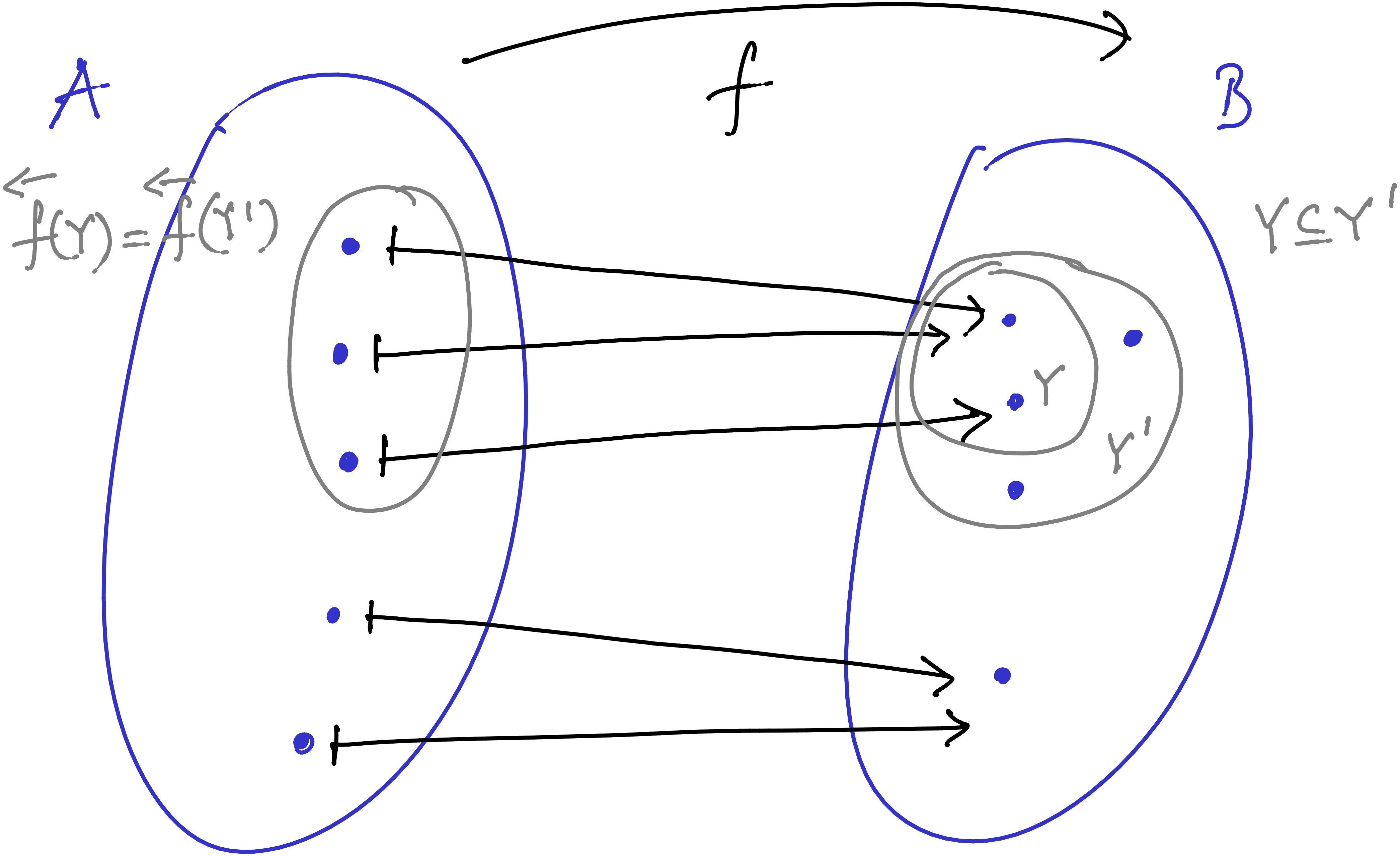
Corollary For an injective function

$f : A \rightarrowtail B$,

$$\forall X \subseteq A. \quad X \cong \vec{f}(X) .$$

Definition: Let $f : A \to B$ be a function. The <u>inverse image</u> of $Y \subseteq B$ is the set $\overleftarrow{f}(Y) \subseteq A$ defined as

$$\overleftarrow{f}(Y) = \{ a \in A \mid f(a) \in Y \}.$$



A
f
B
$\overleftarrow{f}(Y) = \overleftarrow{f}(Y')$
$Y \subseteq Y'$
Y
Y'

Proposition: For $f: A \to B$, the mapping

$$B \supseteq Y \longmapsto \overleftarrow{f}(Y) \subseteq A$$

determines a function

$$\mathcal{P}(B) \longrightarrow \mathcal{P}(A)$$

that preserves the Boolean algebra structure of powersets.

E.g.

$$
\begin{aligned}
\overleftarrow{f}(Y^c) &= \{ a \in A \mid f(a) \in Y^c \} \\
&= \{ a \in A \mid f(a) \notin Y \} \\
&= \{ a \in A \mid f(a) \in Y \}^c \\
&= \left(\overleftarrow{f}(Y) \right)^c
\end{aligned}
$$

Replacement axiom

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

From a mapping

$$i \longmapsto f(i)$$

The replacement axiom allows the construction of a set

$$\{ f(i) \mid i \in I \}$$

for i ranging over an indexing set I.

Set-indexed constructions

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

$$\bigcup_{i \in I} A_i \; = \; \bigcup \left\{ A_i \mid i \in I \right\} \; = \; \left\{ a \mid \exists\, i \in I.\, a \in A_i \right\} \quad .$$

Examples:

1. Indexed disjoint unions:

$$\biguplus_{i \in I} A_i \; = \; \bigcup_{i \in I} \{i\} \times A_i$$

2. Finite sequences on a set A:

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

3. Finite partial functions from a set A to a set B:

$$(A \rightharpoonup_{\text{fin}} B) \;=\; \biguplus_{S \in \mathcal{P}_{\text{fin}}(A)} (S \Rightarrow B)$$

where

$$\mathcal{P}_{\text{fin}}(A) = \{\, S \subseteq A \mid S \text{ is finite} \,\}$$

4. Non-empty indexed intersections: for $I \neq \emptyset$,

$$\bigcap_{i \in I} A_i \;=\; \{\, x \in \bigcup_{i \in I} A_i \mid \forall\, i \in I .\, x \in A_i \,\}$$

5. Indexed products:

$$\prod_{i \in I} A_i \;=\; \left\{\, \alpha \in (I \Rightarrow \bigcup_{i \in I} A_i) \;\middle|\; \forall\, i \in I .\, \alpha(i) \in A_i \,\right\}$$

Proposition 153 *An enumerable indexed disjoint union of enumerable sets is enumerable.*

PROOF:

$$e : \mathbb{N} \twoheadrightarrow I$$

$$e_i : \mathbb{N} \twoheadrightarrow A_i \qquad i \in I$$

$$\begin{tikzcd}
\mathbb{N} \arrow[rr, two heads] \arrow[dr, two heads] & & \biguplus_{i \in I} A_i \\
& \mathbb{N} \times \mathbb{N} \arrow[ur, two heads] &
\end{tikzcd}$$

$$(m, n) \mapsto (e(m), e_{e(m)}(n))$$

Corollary 155 *If* X *and* A *are countable sets then so are* A^*, $\mathcal{P}_{\text{fin}}(A)$, *and* $(X \rightharpoonup_{\text{fin}} A)$.

There are non-computable infinite sequences of bits.

$\underbrace{Prog}_{\text{countable.}} \subseteq \Sigma^*$ countable Σ finite

Foundation axiom

$\boxed{\text{The membership relation is well-founded.}}$

Thereby, providing a

Principle of $\in$*-Induction* .