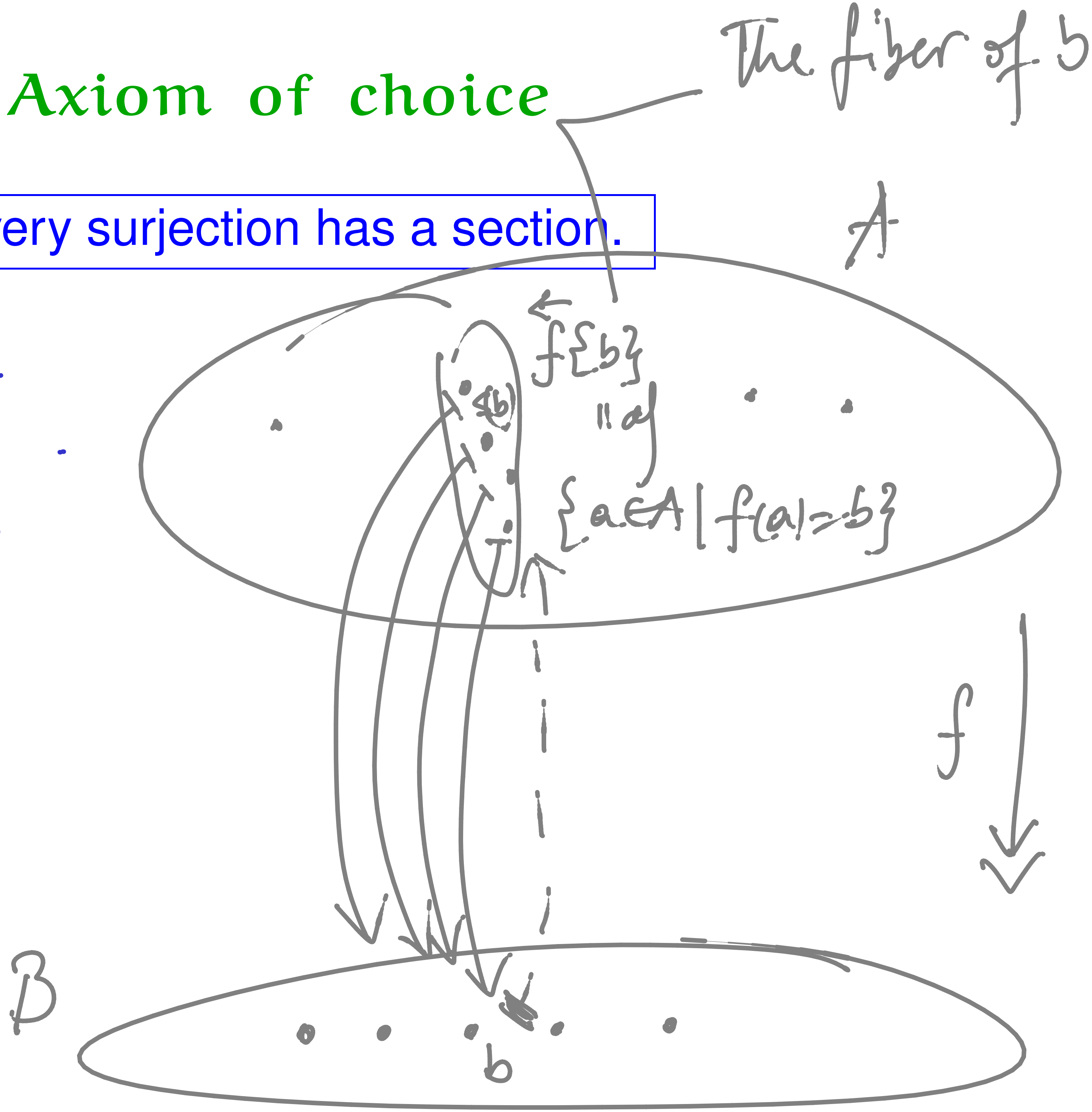
Axiom of choice

Every surjection has a section.

$$\forall \; A \overset{f}{\twoheadrightarrow} B \; . \; \exists \; B \overset{s}{\to} A \; .$$

$$f \circ s = id_B$$



Functional Inverse Images

Given $f : A \to B$, $S \subseteq B$

$$\overleftarrow{f}(S) = \{ a \in A \mid f(a) \in S \} = \bigcup_{b \in S} \overleftarrow{f}\{b\}$$

$$\overleftarrow{f} : \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$$

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

$\forall b, b' \in B$.

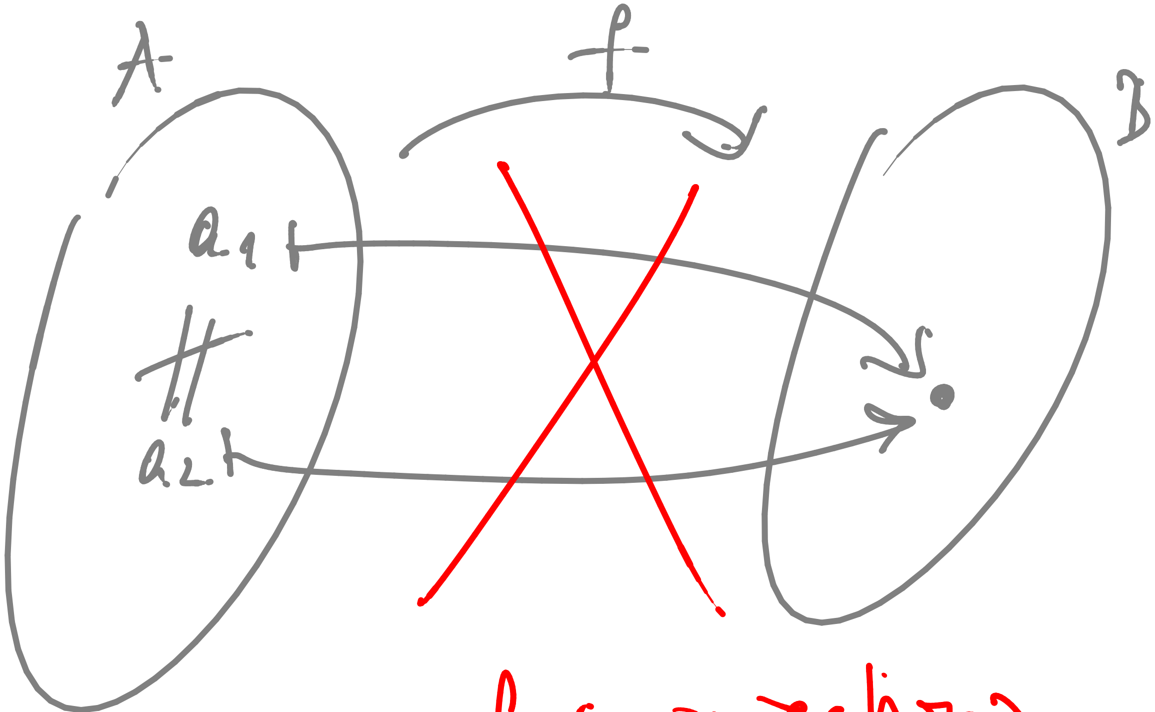
$$s(b) = s(b')$$
$$\Downarrow$$
$$b = f(s(b)) = f(s(b')) = b'$$

$\rightsquigarrow$ sections are injections.

Injections

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

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



for injections.

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

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

with

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

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

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

PROOF IDEA: $A = \{a_1, \ldots, a_n\}$ $(\#A = n)$

$B = \{b_1, \ldots, b_m\}$ $(\#B = m)$

(1) $\underset{n}{\underset{\shortparallel}{\#A}} > \underset{m}{\underset{\shortparallel}{\#B}}$

$a_1 \longmapsto b_{i_1}$

$a_2 \longmapsto b_{i_2}$ injectivity $\Rightarrow i_j \neq i_k \;\forall j \neq k$

$\vdots$

$a_m \longmapsto b_{i_m}$

$\vdots$

$a_n \longmapsto ?$

(2) $\underset{n}{\#A} \leq \underset{m}{\#B}$

$$\begin{aligned} a_1 &\longmapsto b_{i_1} \\ a_2 &\longmapsto b_{i_2} \\ &\vdots \\ a_n &\longmapsto b_{i_n} \end{aligned}$$

injectivity $\Rightarrow \forall j \neq k.$ $b_{i_j} \neq b_{i_k}$

choose n elements of B $\binom{m}{n}$

say $\{b_{i_1}, \dots, b_{i_n}\}$

and describe an injection by permuting them.

$\binom{m}{n} \cdot n!$

$$\begin{array}{ccccc} a_1 & a_2 & a_3 & \cdots & a_n \\ \downarrow & \downarrow & \downarrow & & \downarrow \\ m \cdot & (m-1) \cdot & (m-2) & \cdots & (m-n+1) \end{array} = \binom{m}{n} \cdot n!$$

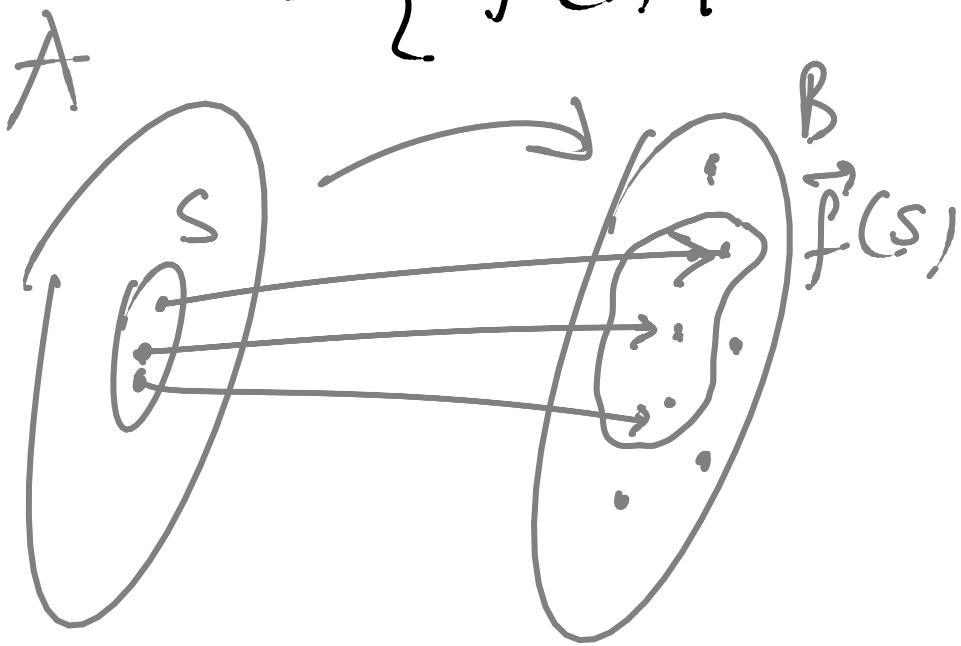
possible choices of b's $\in B$

Functional Direct Images

Given $f : A \to B$, $S \subseteq A$

$$\vec{f}(S) = \{ b \in B \mid \exists a \in A .\ a \in S \land f(a) = b \}$$

$$= \{ f(a) \mid a \in S \}$$



Replacement axiom

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

functional mapping

$i \longmapsto a_i$

I set

?

$\{a_i \mid i \in I\}$ set

Example: Consider I a set and a mapping that to every $i \in I$ associates a set A_i. Then $\{A_i \mid i \in I\}$ a set and so is $\bigcup\{A_i \mid i \in I\}$.

Set-indexed constructions

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

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

Examples:

$i \mapsto \{i\} \times A_i$

1. Indexed disjoint unions:

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

$A^0 = [1]$

2. Finite sequences on a set A:

$A^{n+1} = A \times A^n$

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

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

PROOF: Say I enumerable $\mathbb{N} \overset{e}{\twoheadrightarrow} I$

$\forall i \in I.\ A_i$ enumerable $\mathbb{N} \overset{\varepsilon_i}{\twoheadrightarrow} A_i$

Claim: $\biguplus_{i \in I} A_i$ enumerable.

RTP

$$\begin{array}{l} \mathbb{N} \twoheadrightarrow \biguplus_{i \in I} A_i \overset{\text{def}}{=} \bigcup_{i \in I} \{i\} \times A_i \\ \cong \\ \mathbb{N} \times \mathbb{N} \twoheadrightarrow \\ (x, y) \mapsto (e(x), \varepsilon_{e(x)}(y)) \end{array}$$

Exercise: is a surjection.

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

Unbounded cardinality

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

$\Downarrow$ $\mathcal{P}(\mathbb{N})$ is not enumerable!

PROOF: There is no surjection

$$\mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$$

Assume such a surjection, say e, exists.

$$\forall S \subseteq \mathbb{N}.\ \exists \hat{s} \in \mathbb{N}.\ e(\hat{s}) = S$$

e		0	1	2	3	$\cdots$	n	$\cdots$	
0	$\mapsto$	t	f	f	f	$\cdots$	f	$\cdots$	$e(0)=\{0\}$
1	$\mapsto$	t	f	t	f	$\cdots$			$e(1)=\text{even}$
2	$\mapsto$								
3	$\mapsto$								
$\vdots$									
n	$\mapsto$								
$\vdots$									

Consider the subset of $\mathbb{N}$ given by

	0	1	2	3	$\cdots$ n $\cdots$
$R=$	f	t			$\stackrel{\text{def}}{\vert}$

$f \Downarrow e(0)\neq R$ $\quad$ $t \Downarrow e(1)\neq R$

t: $e(n)=f$ $\quad$ f: $e(n)=t$

$\Downarrow$

$e(n)\neq R$

Then $\forall n$ $e(n)\neq R$

Therefore e is not an enumeration

$\therefore \boxtimes$

$$A \overset{e}{\twoheadrightarrow} \mathcal{P}(A)$$

$$R \overset{\text{def}}{=} \{ a \in A \mid a \notin e(a) \}$$

$$a \in R \Leftrightarrow a \notin e(a)$$

$$\exists r \in A .\ e(r) = R$$

$$r \in R \Leftrightarrow r \notin e(r) = R \quad \boxed{\times}$$

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.*

Foundation axiom

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

Thereby, providing a

Principle of $\in$*-Induction* .