The 'arithmetic' of sets

Calculus of bijections

- $A \cong A$, $A \cong B \implies B \cong A$, $(A \cong B \wedge B \cong C) \implies A \cong C$
- If $A \cong X$ and $B \cong Y$ then

$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad , \quad A \times B \cong X \times Y \quad , \quad A \uplus B \cong X \uplus Y \quad ,$$

$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad , \quad (A \rightharpoonup B) \cong (X \rightharpoonup Y) \quad ,$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad , \quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$

- $A \cong [1] \times A$, $(A \times B) \times C \cong A \times (B \times C)$, $A \times B \cong B \times A$

monoid laws

- $[0] \uplus A \cong A$, $(A \uplus B) \uplus C \cong A \uplus (B \uplus C)$, $A \uplus B \cong B \uplus A$

distributive laws

- $[0] \times A \cong [0]$, $(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$

$(bc)^a = b^a \cdot c^a$

- $(A \Rightarrow [1]) \cong [1]$, $(A \Rightarrow (B \times C)) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $([0] \Rightarrow A) \cong [1]$, $((A \uplus B) \Rightarrow C) \cong (A \Rightarrow C) \times (B \Rightarrow C)$

$c^{a+b} = c^a \cdot c^b$

- $([1] \Rightarrow A) \cong A$, $((A \times B) \Rightarrow C) \cong (A \Rightarrow (B \Rightarrow C))$

$c^{ab} = (c^b)^a$

- $(A \rightharpoonup B) \cong (A \Rightarrow (B \uplus [1]))$
- $\mathcal{P}(A) \cong (A \Rightarrow [2])$

Characteristic (or indicator) functions

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

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

$$S \subseteq A \longmapsto \lambda a \in A.\, \text{if } a \in S \text{ then } 1 \text{ else } 0$$

$$\{a \in A \mid f(a) = 1\} \longleftarrow\!\shortmid\ f$$

a 'test' function

Finite cardinality

$\{0, 1, \ldots, n-1\}$
$\|$ def

Definition 133 *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 134 *For all* $m, n \in \mathbb{N}$,

1. $\mathcal{P}\big([n]\big) \cong [2^n]$

2. $[m] \times [n] \cong [m \cdot n]$

3. $[m] \uplus [n] \cong [m + n]$

4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$

5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$

6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

Infinity axiom

$\boxed{\text{There is an infinite set, containing } \emptyset \text{ and closed under successor.}}$

Bijections

Proposition 135 *For a function* $f : A \to B$*, the following are equivalent.*

1. f *is bijective.*
2. $\forall\, b \in B.\, \exists!\, a \in A.\, f(a) = b.$ EXISTENCE ~ INJECTION
3. $$\begin{array}{l} \big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \\ \wedge \\ \big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \end{array}$$

UNIQUENESS ~ SURJECTION

Surjections

Definition 136 *A function* $f : A \to B$ *is said to be* <u>surjective</u>, *or a* <u>surjection</u>, *and indicated* $f : A \twoheadrightarrow B$ *whenever*

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

NB: For such f,

$$\{ f(a) \in B \mid a \in A \} = B$$

$$\|^{\text{def}} \; \{ b \in B \mid \exists\, a \in A.\ b = f(a) \}$$

Theorem 137 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

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

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Sur}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) .$$

Enumerability

Definition 139

1. *A set A is said to be* enumerable *whenever there exists a surjection $\mathbb{N} \twoheadrightarrow A$, referred to as an* enumeration.

2. *A* countable *set is one that is either empty or enumerable.*

Idea: $e : \mathbb{N} \twoheadrightarrow A$ enumerates A as

$$e(0), e(1), \ldots, e(n), \ldots \quad (n \in \mathbb{N})$$

since

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

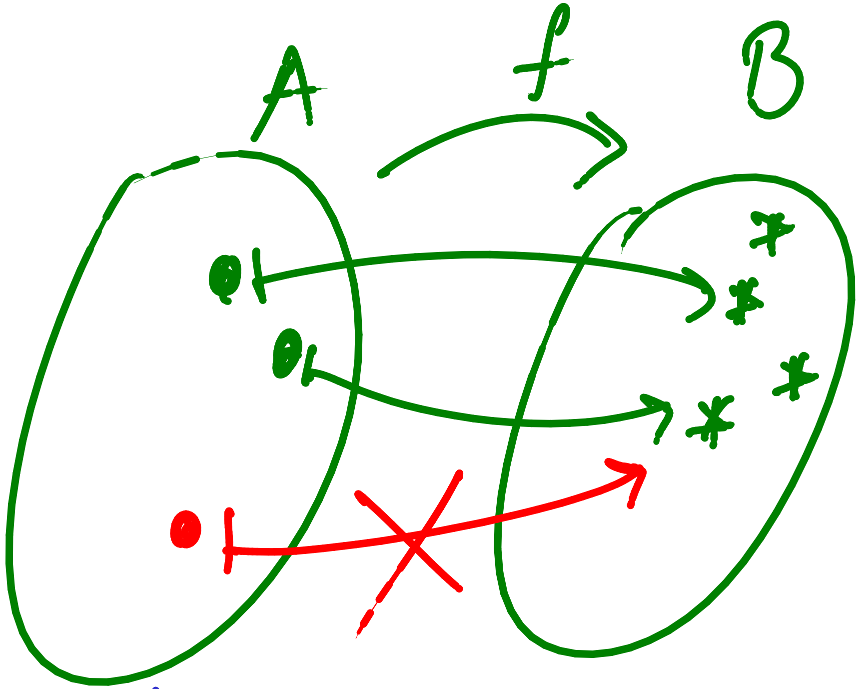
Injections

Definition 142 *A function* $f : A \to B$ *is said to be* injective*, or an* injection*, and indicated* $f : A \rightarrowtail B$ *whenever*

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

Idea: f produces a 'copy' of A inside B :

$$\{ f(a) \mid a \in A \} \cong A$$



$$a \neq a' \Rightarrow f(a) \neq f(a')$$

Theorem 143 *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

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

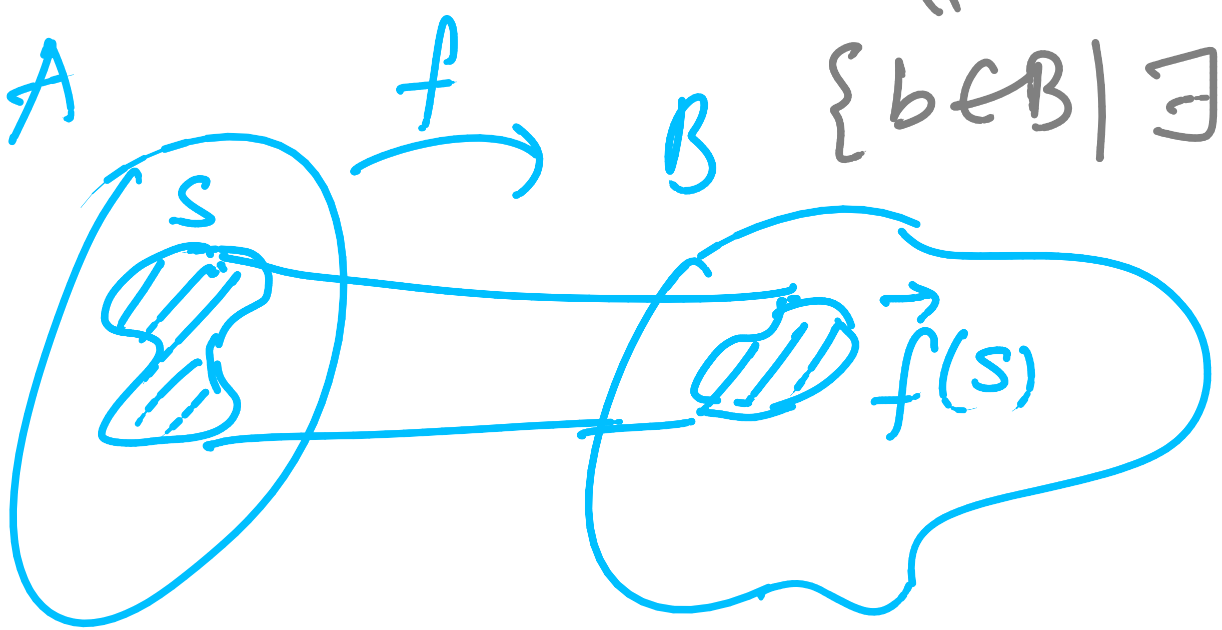
- DIRECT IMAGE of functions.

$$f : A \to B \quad \rightsquigarrow \quad \vec{f} : \mathcal{P}(A) \to \mathcal{P}(B)$$

$$S \subseteq A \longmapsto \vec{f}(S) = \{ f(a) \in B \mid a \in S \} \subseteq B$$

$$\| $$

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

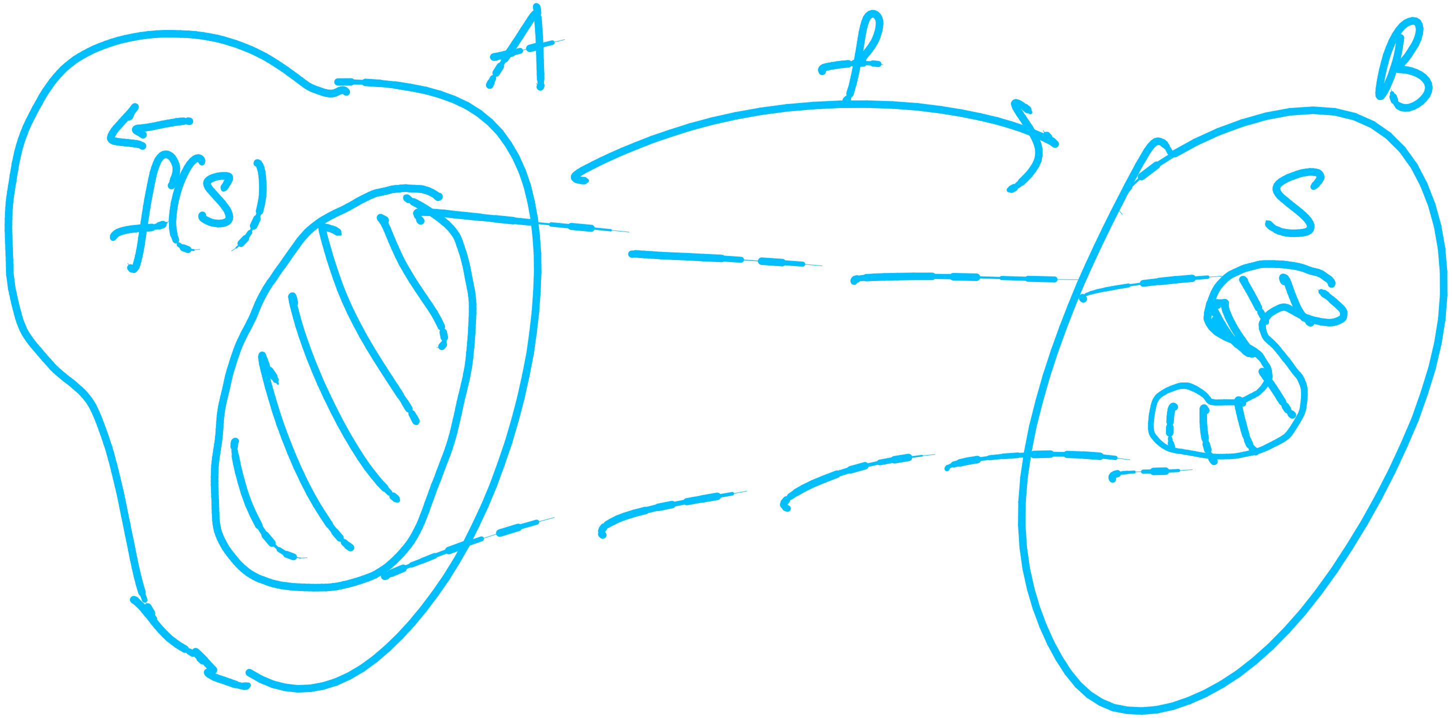


- INVERSE IMAGE for functions

a map of Boolean algebras

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

$$S \subseteq B \longmapsto \overleftarrow{f}(S) = \{ a \in A \mid f(a) \in S \} \subseteq A$$



<u>NB</u> $a \in \overleftarrow{f}(S)$

$\Updownarrow$

$f(a) \in S$

Relational images

Definition 147 *Let* $R : A \rightarrowtriangle B$ *be a relation.*

- *The* direct image *of* $X \subseteq A$ *under* R *is the set* $\overrightarrow{R}(X) \subseteq B$, *defined as*

$$\overrightarrow{R}(X) \;=\; \{\, b \in B \mid \exists x \in X.\, x \mathrel{R} b \,\} \;.$$

Compare with the definition of direct image for functions.

NB *This construction yields a function* $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$.

- *The* inverse image *of* $Y \subseteq B$ *under* R *is the set* $\overleftarrow{R}(Y) \subseteq A$, *defined as*

$$\overleftarrow{R}(Y) = \{ a \in A \mid \forall b \in B.\, a \mathrel{R} b \implies b \in Y \}$$

EXERCISE Show that for a functional relation R this definition coincides with that of the inverse image of a function.

NB *This construction yields a function* $\overleftarrow{R} : \mathcal{P}(B) \to \mathcal{P}(A)$.

Replacement axiom

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

Given an 'indexing' set I and a mapping

$$i \in I \longmapsto A_i$$

we have a <u>set</u>:

$$\{A_i \mid i \in I\} = \{X \mid \exists i \in I . X = A_i\}$$

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:

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:

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

Foundation axiom

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

Thereby, providing a

Principle of $\in$-Induction .