SETS

RELATIONS, MAPPINGS, SIZE

What are sets

- A $\boxed{\textit{set}}$ is ***a collection into a whole of some well-recognized objects,*** dubbed the set's $\boxed{\textit{elements.}}$
- We write $a \in S$ for "a *is an element of* S"

What are sets

- A $\boxed{\textit{set}}$ is ***a collection into a whole of some well-recognized objects,*** dubbed the set's $\boxed{\textit{elements.}}$
- We write $a \in S$ for "a *is an element of* S"
- The concept of *set* is "defined" here in terms of "collection" and "whole", i.e. synonyms of "set"!
- **Shouldn't concepts be defined using previously defined ones?**

What are sets

- A $\boxed{\textit{set}}$ is ***a collection into a whole of some well-recognized objects,*** dubbed the set's $\boxed{\textit{elements.}}$
- We write $a \in S$ for "a *is an element of* S"
- The concept of *set* is "defined" here in terms of "collection" and "whole", i.e. synonyms of "set"!
- **Shouldn't concepts be defined using previously defined ones?**
- Regressing this way cannot go on indefinitely: we must stop with concepts that are left ***undefined***.
- We only explain those informally,
  hoping to establish some
  shared imagery, intuitions and understanding.
  "Set" is just such a concept.

Exhibiting sets

- Sets are determined by their elements.
  That is, if sets A and B have the same elements,
  then they are one and the same set,
  even if they are described in very different ways.
- This is the $\boxed{\textit{Principle of Extensionality}}$.

Exhibiting sets

- Sets are determined by their elements.
  That is, if sets A and B have the same elements,
  then they are one and the same set,
  even if they are described in very different ways.
- This is the ***Principle of Extensionality***.
- It implies that finite sets can be defined
  by exhibiting their elements: $\{a_1, \ldots, a_k\}$.
  So $\{0, 1\}$, $\{1, 0\}$ and $\{0, 0, 1\}$ are all the same set.

Names and notations for special sets

- Some sets are commonly assumed as given, and assigned notations.
  - For an alphabet Σ, the set Σ^* of Σ-strings.

Names and notations for special sets

- Some sets are commonly assumed as given, and assigned notations.
  - For an alphabet Σ, the set Σ^* of Σ-strings.
  - The set $\{0.1\}$ of ***booleans***, denoted $\mathcal{B}ool$.

Names and notations for special sets

- Some sets are commonly assumed as given, and assigned notations.
  - For an alphabet Σ, the set Σ^* of Σ-strings.
  - The set $\{0.1\}$ of ***booleans***, denoted $\mathcal{B}ool$.
  - ***nat*** or $\mathbb{N}$: The set of natural numbers $0, 1, 2, 3\ldots$.
  - ***int*** or $\mathbb{Z}$: The integers
  - $\mathbb{Q}$: the rational numbers (Q for "quotients")
  - $\mathbb{R}$: the real numbers (the "real number line")

Names and notations for special sets

- Some sets are commonly assumed as given, and assigned notations.
  - For an alphabet Σ, the set Σ^* of Σ-strings.
  - The set $\{0.1\}$ of ***booleans***, denoted $\mathcal{B}ool$.
  - ***nat*** or $\mathbb{N}$: The set of natural numbers $0, 1, 2, 3 \ldots$.
  - ***int*** or $\mathbb{Z}$: The integers
  - $\mathbb{Q}$: the rational numbers (Q for "quotients")
  - $\mathbb{R}$: the real numbers (the "real number line")
  - The ***empty set,*** denoted $\emptyset$, which has no elements.

Names and notations for special sets

- Some sets are commonly assumed as given, and assigned notations.
  - For an alphabet Σ, the set Σ^* of Σ-strings.
  - The set $\{0.1\}$ of ***booleans***, denoted $\mathcal{B}ool$.
  - ***nat*** or $\mathbb{N}$: The set of natural numbers $0, 1, 2, 3 \ldots$.
  - ***int*** or $\mathbb{Z}$: The integers
  - $\mathbb{Q}$: the rational numbers (Q for "quotients")
  - $\mathbb{R}$: the real numbers (the "real number line")
  - The ***empty set,*** denoted $\emptyset$, which has no elements.
- A set with exactly one element, however complex, is a ***singleton.***
  Examples: $\{0\}$, $\{\emptyset\}$, $\{\{\emptyset\}\}$ and $\{\mathbb{N}\}$

Abstraction notation

- Another approach to defining sets is to delineate them
  by certain properties, as in
  "the set of registered voters".

- Such definitions are captured by the notational convention
  $\{x \mid$ a property of $x\}$.

- Between braces: (1) a declared variable, say x ,
  (2) a vertical bar (pronounced "such that")
  (3) a property of x .

Abstraction notation

- Another approach to defining sets is to delineate them by certain properties, as in ***"the set of registered voters"***.
- Such definitions are captured by the notational convention $\{x \mid$ a property of $x\}$.
- Between braces: (1) a declared variable, say x,
  (2) a vertical bar (pronounced "such that")
  (3) a property of x.
- Example: $\{z \mid z = 2^x$ for some $x \in \mathbb{N}\}$.
  More concisely: $\{2^x \mid x \in \mathbb{N}\}$.

Abstraction notation

- Another approach to defining sets is to delineate them
  by certain properties, as in
  "the set of registered voters".

- Such definitions are captured by the notational convention
  $\{x \mid$ a property of $x\}$.

- Between braces: (1) a declared variable, say x,
  (2) a vertical bar (pronounced "such that")
  (3) a property of x.

- Example: $\{z \mid z = 2^x$ for some $x \in \mathbb{N}\}$.
  More concisely: $\{2^x \mid x \in \mathbb{N}\}$.

- A set's elements can themselves be complex entities!
  Examples: $\{\emptyset\}$, $\{\mathbb{N}\}$, $\{\emptyset, \{\emptyset\}\}$.

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) \;=\; \{x \mid p < x < q\} \qquad \text{(\textbf{\textit{open interval}})}$$

$$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\} \qquad \text{(\textbf{\textit{closed interval}})}$$

$$[p..q) \;=\; \{x \mid p \leqslant x < q\} \qquad \text{(\textbf{\textit{left-closed interval}})}$$

$$[p..) \;=\; \{x \mid p \leqslant x\} \qquad \text{(\textbf{\textit{right-infinite interval}})}$$

The latter is often written $[p..\infty)$.

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) \;=\; \{x \mid p < x < q\} \qquad \text{(\textbf{\textit{open interval}})}$$
$$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\} \qquad \text{(\textbf{\textit{closed interval}})}$$
$$[p..q) \;=\; \{x \mid p \leqslant x < q\} \qquad \text{(\textbf{\textit{left-closed interval}})}$$
$$[p..) \;=\; \{x \mid p \leqslant x\} \qquad \text{(\textbf{\textit{right-infinite interval}})}$$

The latter is often written $[p..\infty)$.

- Examples for integers: $[1..3] =$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) \;=\; \{x \mid p < x < q\}$$ (***open interval***)

$$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\}$$ (***closed interval***)

$$[p..q) \;=\; \{x \mid p \leqslant x < q\}$$ (***left-closed interval***)

$$[p..) \;=\; \{x \mid p \leqslant x\}$$ (***right-infinite interval***)

The latter is often written $[p..\infty)$.

- Examples for integers: $[1..3] = \{1, 2, 3\}$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$(p..q) \;=\; \{x \mid p < x < q\}$ (***open interval***)

$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\}$ (***closed interval***)

$[p..q) \;=\; \{x \mid p \leqslant x < q\}$ (***left-closed interval***)

$[p..) \;=\; \{x \mid p \leqslant x\}$ (***right-infinite interval***)

The latter is often written $[p..\infty)$.

- Examples for integers: $(1..3) \;=$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) = \{x \mid p < x < q\}$$ (***open interval***)

$$[p..q] = \{x \mid p \leqslant x \leqslant q\}$$ (***closed interval***)

$$[p..q) = \{x \mid p \leqslant x < q\}$$ (***left-closed interval***)

$$[p..) = \{x \mid p \leqslant x\}$$ (***right-infinite interval***)

The latter is often written $[p..\infty)$.

- Examples for integers: $(1..3) = \{2\}$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

  $(p..q) \;=\; \{x \mid p < x < q\}$ (***open interval***) The latter is

  $[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\}$ (***closed interval***)

  $[p..q) \;=\; \{x \mid p \leqslant x < q\}$ (***left-closed interval***)

  $[p..) \;=\; \{x \mid p \leqslant x\}$ (***right-infinite interval***)

  often written $[p..\infty)$.

- Examples for integers: $[1..3) \;=$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$
\begin{aligned}
(p..q) &= \{x \mid p < x < q\} && (\textbf{\textit{open interval}}) \\
[p..q] &= \{x \mid p \leqslant x \leqslant q\} && (\textbf{\textit{closed interval}}) \\
[p..q) &= \{x \mid p \leqslant x < q\} && (\textbf{\textit{left-closed interval}}) \\
[p..) &= \{x \mid p \leqslant x\} && (\textbf{\textit{right-infinite interval}})
\end{aligned}
$$

The latter is often written $[p..\infty)$.

- Examples for integers: $[1..3) = \{1, 2\}$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) = \{x \mid p < x < q\}$$ (***open interval***) The latter is

$$[p..q] = \{x \mid p \leqslant x \leqslant q\}$$ (***closed interval***)

$$[p..q) = \{x \mid p \leqslant x < q\}$$ (***left-closed interval***)

$$[p..) = \{x \mid p \leqslant x\}$$ (***right-infinite interval***)

often written $[p..\infty)$.

- Examples for integers: $(1..3] =$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$
\begin{array}{llll}
(p..q) & = & \{x \mid p < x < q\} & (\textit{\textbf{open interval}}) \\
[p..q] & = & \{x \mid p \leqslant x \leqslant q\} & (\textit{\textbf{closed interval}}) \\
[p..q) & = & \{x \mid p \leqslant x < q\} & (\textit{\textbf{left-closed interval}}) \\
[p..) & = & \{x \mid p \leqslant x\} & (\textit{\textbf{right-infinite interval}})
\end{array}
$$

The latter is often written $[p..\infty)$.

- Examples for integers: $(1..3] = \{2, 3\}$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$(p..q) \ = \ \{x \mid p < x < q\}$ (***open interval***) The latter is

$[p..q] \ = \ \{x \mid p \leqslant x \leqslant q\}$ (***closed interval***)

$[p..q) \ = \ \{x \mid p \leqslant x < q\}$ (***left-closed interval***)

$[p..) \ = \ \{x \mid p \leqslant x\}$ (***right-infinite interval***)

often written $[p..\infty)$.

- Examples for integers: $[1..1] =$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$(p..q) \;=\; \{x \mid p < x < q\}$ (***open interval***) The latter is

$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\}$ (***closed interval***)

$[p..q) \;=\; \{x \mid p \leqslant x < q\}$ (***left-closed interval***)

$[p..) \;=\; \{x \mid p \leqslant x\}$ (***right-infinite interval***)

often written $[p..\infty)$.

- Examples for integers: $[1..1] = \{1\}$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) \;=\; \{x \mid p < x < q\} \qquad (\textbf{\textit{open interval}})$$

The latter is

$$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\} \qquad (\textbf{\textit{closed interval}})$$

$$[p..q) \;=\; \{x \mid p \leqslant x < q\} \qquad (\textbf{\textit{left-closed interval}})$$

$$[p..) \;=\; \{x \mid p \leqslant x\} \qquad (\textbf{\textit{right-infinite interval}})$$

often written $[p..\infty)$.

- Examples for integers: $(1..1) \;=$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$
\begin{array}{lcll}
(p..q) & = & \{x \mid p < x < q\} & \text{(\textbf{\textit{open interval}})} \\
[p..q] & = & \{x \mid p \leqslant x \leqslant q\} & \text{(\textbf{\textit{closed interval}})} \\
[p..q) & = & \{x \mid p \leqslant x < q\} & \text{(\textbf{\textit{left-closed interval}})} \\
[p..) & = & \{x \mid p \leqslant x\} & \text{(\textbf{\textit{right-infinite interval}})}
\end{array}
$$

The latter is often written $[p..\infty)$.

- Examples for integers: $(1..1) = \emptyset$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) \;=\; \{x \mid p < x < q\} \qquad (\textit{\textbf{open interval}})$$

$$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\} \qquad (\textit{\textbf{closed interval}})$$

$$[p..q) \;=\; \{x \mid p \leqslant x < q\} \qquad (\textit{\textbf{left-closed interval}})$$

$$[p..) \;=\; \{x \mid p \leqslant x\} \qquad (\textit{\textbf{right-infinite interval}})$$

The latter is often written $[p..\infty)$.

- Examples for integers: $[-1..1) =$

Conventions for numeric intervals

- To denote intervals of integers or real numbers we indicate end-point's inclusion with a bracket, and exclusion with a parenthesis.

$$(p..q) \;=\; \{x \mid p < x < q\} \qquad (\textbf{\textit{open interval}})$$

The latter is

$$[p..q] \;=\; \{x \mid p \leqslant x \leqslant q\} \qquad (\textbf{\textit{closed interval}})$$

$$[p..q) \;=\; \{x \mid p \leqslant x < q\} \qquad (\textbf{\textit{left-closed interval}})$$

$$[p..) \;=\; \{x \mid p \leqslant x\} \qquad (\textbf{\textit{right-infinite interval}})$$

often written $[p..\infty)$.

- Examples for integers: $[-1..1) = \{-1, 0\}$

Relations between sets

- We say that A is a subset of B
  and write $A \subseteq B$ if every element of A is an element of B,
    that is $x \in A$ implies $x \in B$.

Relations between sets

- We say that A is a subset of B
  and write $A \subseteq B$ if every element of A is an element of B,
  that is $x \in A$ implies $x \in B$.

- Examples:
  - $\mathbb{N} \subseteq \mathbb{Z}$.
  - For any set A: $A \subseteq A$ and $\emptyset \subseteq A$.
  - The set of elephants is a subset of the set of mammals.

Relations between sets

- We say that A is a subset of B
  and write $A \subseteq B$ if every element of A is an element of B,
  that is $x \in A$ implies $x \in B$.

- Examples:
  - $\mathbb{N} \subseteq \mathbb{Z}$.
  - For any set A: $A \subseteq A$ and $\emptyset \subseteq A$.
  - The set of elephants is a subset of the set of mammals.

- If $A \subseteq B$ and $B \subseteq A$
  then A and B have the same elements.
  By Extensionality this implies $A = B$.

True or false?

$0 \in \{0, 1\}$	$\mathbb{N} \subseteq \{\mathbb{N}\}$
$\{0\} \subseteq \{0, 1\}$	$\mathbb{N} \in \{\mathbb{N}\}$
$\{0\} \in \{0, 1\}$	$\emptyset \subseteq \{\emptyset\}$
$\{0, 1, 1\} \subseteq \{1, 0\}$	$\{\emptyset\} \subseteq \emptyset$
$\{0, 1\} \subseteq \mathbb{N}$	$\emptyset \in \emptyset$
$\{0, 1\} \subseteq \{\mathbb{N}\}$	$\emptyset \in \{\emptyset\}$

The perils of abstraction

- In the template $\{x \mid \cdots x \cdots\}$,
  does x stand for "anything"?

- If that were so, we'd be able to define

$$R =_{\text{df}} \{x \mid x \notin x\}$$

  That is, for all x

$$x \in R \quad \textbf{IFF} \quad x \notin x$$

- In particular, if we take x to be R then

$$R \in R \quad \textbf{IFF} \quad R \notin R$$

  A contradiction!

- This is known as $\boxed{\textit{Russell's Paradox.}}$

The Separation Principle

- There is a circularity at the root of the definition of R:

  "all sets" includes the set R itself,

  which is defined in terms of "all sets."

- Work-around: Zermelo's **_Separation Principle:_**

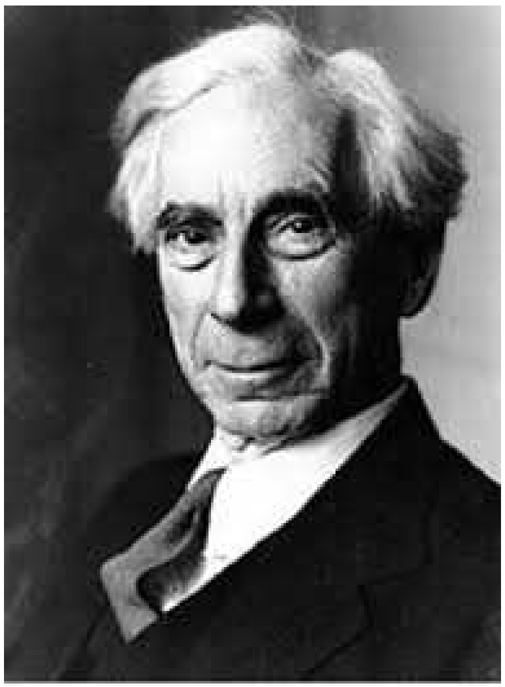
  For a *given* set S we may define $\{x \in S \mid \cdots x \cdots\}$.

  We "separate" out the elements of S along the given property.

- This blocks Russell's paradox:

  S would have to be "all sets", which is not admissible as a set.

Bertrand Russell and Ernst Zermelo



Russell (1872-1970)

Zermelo (1871-1953)

The Diagonal Method

- Russell's Paradox epitomizes a powerful line of reasoning.

  To illustrate, let's call a book ***modest*** if its text does not mention its title.

  Question: Can we compile a catalog of all modest books?

- Suppose such a catalog existed, with title $\boldsymbol{M}$ say.

  A book is listed in $\boldsymbol{M}$ iff it does not mention itself.

  In particular, $\boldsymbol{M}$ is listed in $\boldsymbol{M}$ iff $\boldsymbol{M}$ is not listed in $\boldsymbol{M}$.

- Consequence: ***There can be no catalog of all modest books!***

- **Where does the contradiction come from?**

Contradictions via two-faced objects

- The catalog argument refers to each book in two ways:

  as a title, and as contents.

- Russell's Paradox refers to each set in two ways:

  as a set of other objects, and as a possible element of other sets.

- This duality is the core of the ***Self-reference Method***

  AKA the ***Diagonal Method.***

  (A matrix's diagonal is where row $\#i$ meets column $\#i$.)

- This duality is ingrained in computing:

  a program is both a string and an algorithm.

Operations on sets

- $$\begin{aligned} A \cap B &= \{x \mid x \in A \text{ and } x \in B\} \\ A \cup B &= \{x \mid x \in A \text{ or } x \in B\} \\ A - B &= \{x \mid x \in A \text{ and } x \notin B\} \end{aligned}$$

Operations on sets

- $$\begin{aligned} A \cap B &= \{x \mid x \in A \text{ and } x \in B\} \\ A \cup B &= \{x \mid x \in A \text{ or } x \in B\} \\ A - B &= \{x \mid x \in A \text{ and } x \notin B\} \end{aligned}$$
- When all sets considered are subsets of some set U ,

  we refer to $U - A$ as the **complement** of A,

  and write $\bar{A}$ for it.

$\cup$ *is the dual of* $\cap$

- We have $\overline{A \cap B} = \bar{A} \cup \bar{B}$:

$$x \notin A \cap B \text{ \textbf{\textit{iff}} } x \notin A \text{ or } x \notin B$$

"not both true" is the same as "at least one is false"

$\cup$ *is the dual of* $\cap$

- We have $\overline{A \cap B} = \bar{A} \cup \bar{B}$:

$$x \notin A \cap B \ \textbf{\textit{iff}}\ x \notin A \text{ or } x \notin B$$

"not both true" is the same as "at least one is false"

- Complementing both sides we get:
$A \cap B = \overline{\bar{A} \cup \bar{B}}$

$\cup$ *is the dual of* $\cap$

- We have $\overline{A \cap B} = \bar{A} \cup \bar{B}$:

$$x \notin A \cap B \ \textit{\textbf{iff}} \ x \notin A \ \text{or} \ x \notin B$$

“not both true” is the same as “at least one is false”

- Complementing both sides we get:

  $A \cap B = \overline{\bar{A} \cup \bar{B}}$

- Similarly, we have $\overline{A \cup B} = \bar{A} \cap \bar{B}$:

$$x \notin A \cup B \ \textit{\textbf{iff}} \ x \notin A \ \text{and} \ x \notin B$$

“neither true” is the same as “both false”

$\cup$ *is the dual of* $\cap$

- We have $\overline{A \cap B} = \bar{A} \cup \bar{B}$:

$$x \notin A \cap B \ \textbf{\textit{iff}}\ x \notin A \text{ or } x \notin B$$

  "not both true" is the same as "at least one is false"

- Complementing both sides we get:
  $A \cap B = \overline{\bar{A} \cup \bar{B}}$

- Similarly, we have $\overline{A \cup B} = \bar{A} \cap \bar{B}$:

$$x \notin A \cup B \ \textbf{\textit{iff}}\ x \notin A \text{ and } x \notin B$$

  "neither true" is the same as "both false"

- Complementing both sides we get:
  $A \cup B = \overline{\bar{A} \cap \bar{B}}$

The power-set operation

- If A is a set, then the $\boxed{\textit{power-set}}$ of A is

$$\mathcal{P}(A) =_{\mathrm{df}} \{B \mid B \subseteq A\}$$

The power-set operation

- If A is a set, then the **power-set** of A is

$$\mathcal{P}(A) =_{\mathrm{df}} \{B \mid B \subseteq A\}$$

- Examples:
  - $A = \{0, 1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$

The power-set operation

- If A is a set, then the $\boxed{\textit{power-set}}$ of A is

$$\mathcal{P}(A) =_{\mathrm{df}} \{B \mid B \subseteq A\}$$

- Examples:
  - $A = \{0,1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$
  - $$\begin{aligned}\mathcal{P}(\{a,b,c\}) \quad = \quad & \{\ \emptyset, \\ & \{a\}, \{b\}, \{c\}, \\ & \{a,b\}, \{a,c\}, \{b,c\}, \\ & \{a,b,c\} \quad \}\end{aligned}$$

The power-set operation

- If A is a set, then the $\boxed{\textbf{power-set}}$ of A is
$$\mathcal{P}(A) =_{\mathrm{df}} \{B \mid B \subseteq A\}$$
- Examples:
  - $A = \{0, 1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
  - $$\begin{aligned}\mathcal{P}(\{a, b, c\}) \quad = \quad & \{\ \emptyset, \\ & \{a\}, \{b\}, \{c\}, \\ & \{a, b\}, \{a, c\}, \{b, c\}, \\ & \{a, b, c\} \quad \}\end{aligned}$$
- *What is* $\mathcal{P}(\emptyset)$?

The power-set operation

- If A is a set, then the $\boxed{\textit{power-set}}$ of A is
- Examples:

$$\mathcal{P}(A) =_{\mathrm{df}} \{B \mid B \subseteq A\}$$

  - $A = \{0, 1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
  - $$\begin{aligned} \mathcal{P}(\{a, b, c\}) \quad = \quad & \{\ \emptyset, \\ & \{a\}, \{b\}, \{c\}, \\ & \{a, b\}, \{a, c\}, \{b, c\}, \\ & \{a, b, c\} \quad \} \end{aligned}$$

- *What is* $\mathcal{P}(\emptyset)$? $\mathcal{P}(\emptyset) = \{\emptyset\}$

The power-set operation

- If A is a set, then the $\boxed{\textit{power-set}}$ of A is

$$\mathcal{P}(A) =_{\mathrm{df}} \{B \mid B \subseteq A\}$$

- Examples:
  - $A = \{0, 1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
  - $$\begin{aligned} \mathcal{P}(\{a, b, c\}) \quad = \quad \{\ & \emptyset, \\ & \{a\}, \{b\}, \{c\}, \\ & \{a, b\}, \{a, c\}, \{b, c\}, \\ & \{a, b, c\} \quad \} \end{aligned}$$
  - *What is* $\mathcal{P}(\emptyset)$? $\mathcal{P}(\emptyset) = \{\emptyset\}$
  - *What is* $\mathcal{P}(\{1\})$*?*

The power-set operation

- If A is a set, then the $\boxed{\textit{power-set}}$ of A is

$$\mathcal{P}(A) =_{\text{df}} \{B \mid B \subseteq A\}$$

- Examples:
  - $A = \{0, 1\}$, $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
  - $$\begin{aligned} \mathcal{P}(\{a, b, c\}) \quad = \quad & \{\ \emptyset, \\ & \{a\}, \{b\}, \{c\}, \\ & \{a, b\}, \{a, c\}, \{b, c\}, \\ & \{a, b, c\} \quad \} \end{aligned}$$

- *What is* $\mathcal{P}(\emptyset)$? $\mathcal{P}(\emptyset) = \{\emptyset\}$

- *What is* $\mathcal{P}(\{1\})$*?* $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$

Size of the power-set

- If a finite A has n elements,

  then $\mathcal{P}(A)$ has 2^n elements:

Size of the power-set

- If a finite A has n elements,

  then $\mathcal{P}(A)$ has 2^n elements:

  - A subset $B \subseteq A$, is fixed by choosing, for each $x \in A$,

    whether or not $x \in B$.

  - Each choice doubles the number of previous choices.

Disjoint sets

- Sets A, B are $\boxed{\textit{disjoint}}$ if $A \cap B = \emptyset$,

  i.e. they have no element in common.

Disjoint sets

- Sets A, B are $\boxed{\textit{disjoint}}$ if $A \cap B = \emptyset$,

  i.e. they have no element in common.

- Example:

  The Canadian citizenry is disjoint from the Japanese citizenry

  (Japan disallows dual citizenship...)

Disjoint sets

- Sets A, B are $\boxed{\textit{disjoint}}$ if $A \cap B = \emptyset$,

  i.e. they have no element in common.

- Example:

  The Canadian citizenry is disjoint from the Japanese citizenry

  (Japan disallows dual citizenship...)

- More generally, a ***collection*** C of sets is $\boxed{\textit{disjoint}}$ if

  $A \cap B = \emptyset$ for every distinct $A, B \in C$.

  (The phrase ***pairwise-disjoint*** means the same thing.)

Disjoint sets

- Sets A, B are $\boxed{\textit{disjoint}}$ if $A \cap B = \emptyset$,

  i.e. they have no element in common.

- Example:

  The Canadian citizenry is disjoint from the Japanese citizenry

  (Japan disallows dual citizenship...)

- More generally, a ***collection*** C of sets is $\boxed{\textit{disjoint}}$ if

  $A \cap B = \emptyset$ for every distinct $A, B \in C$.

  (The phrase ***pairwise-disjoint*** means the same thing.)

- Example: The collection of open intervals $(0..1)$, $(1..2)$, $(2..3)$, $(3..4)$, $\cdots$

Partitions

- A collection C of non-empty subsets of S is a $\boxed{\textit{partition of } S}$ if every $x \in S$ is in exactly one $A \in C$.

Partitions

- A collection C of non-empty subsets of S is a $\boxed{\textit{partition of } S}$ if every $x \in S$ is in exactly one $A \in C$.

- Examples:
  - $\{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}\}$ can be partitioned into $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ and $\{\mathtt{d}\}$.

  How many partitions into 2 sets? into 3 sets? into 4?

Partitions

- A collection C of non-empty subsets of S is a ***partition of S***
  if every $x \in S$ is in exactly one $A \in C$.

- Examples:
  - $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}\}$ can be partitioned into $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ and $\{\mathbf{d}\}$.

    How many partitions into 2 sets? into 3 sets? into 4?

  - $\{\mathbf{a}...\mathbf{z}\}$ can be partitioned into the vowels and the consonants.

Partitions

- A collection C of non-empty subsets of S is a $\boxed{\textit{partition of } S}$
  if every $x \in S$ is in exactly one $A \in C$.

- Examples:
  - $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}\}$ can be partitioned into $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ and $\{\mathbf{d}\}$.

    How many partitions into 2 sets? into 3 sets? into 4?
  - $\{\mathbf{a}...\mathbf{z}\}$ can be partitioned into the vowels and the consonants.
  - $\mathbb{N}$ can be partitioned into the prime numbers, composite numbers, and $\{0, 1\}$.

    Another partition: Singletons $\{0\}$, $\{1\}$, $\{2\}$ ... .

Partitions

- A collection C of non-empty subsets of S is a $\boxed{\textit{partition of } S}$

  if every $x \in S$ is in exactly one $A \in C$.

- Examples:

  - $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}\}$ can be partitioned into $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ and $\{\mathbf{d}\}$.

    How many partitions into 2 sets? into 3 sets? into 4?

  - $\{\mathbf{a} ... \mathbf{z}\}$ can be partitioned into the vowels and the consonants.

  - $\mathbb{N}$ can be partitioned into the prime numbers, composite numbers, and $\{0, 1\}$.

    Another partition: Singletons $\{0\}$, $\{1\}$, $\{2\}$ ... .

- Non-example:

  - English words fall into eight parts of speech,

    but this is not a partition: some words are both noun and verb.

- **Which are partitions:**
  - Classify humanity by birth-year:

    people born in 2023, 2022, ...

- **Which are partitions:**
  - Classify humanity by birth-year:

    people born in 2023, 2022, ...
  - Classify $\mathbb{R}$ into two:

    finite decimal expansions & infinite decimal expansions

- **Which are partitions:**
  - Classify humanity by birth-year:

    people born in 2023, 2022, ...
  - Classify $\mathbb{R}$ into two:

    finite decimal expansions & infinite decimal expansions
  - Classify $\mathbb{R}$ into the half-closed intervals

    $[n..n+1)$, (n an integer).

RELATIONS

Ordered pairs

- Given any two objects a, b

  we can form the $\boxed{\textit{ordered-pair}}$ $\langle a, b \rangle$.

  a and b need not have anything in common, and may be identical.

Ordered pairs

- Given any two objects a, b

  we can form the $\boxed{\textit{ordered-pair}}$ $\langle a, b \rangle$.

  a and b need not have anything in common, and may be identical.

- Unlike the set $\{a, b\}$, order and repetition in $\langle a, b \rangle$ ***do*** matter:

  $\langle a, b \rangle = \langle c, d \rangle$ iff $a = c$ and $b = d$.

Ordered pairs

- Given any two objects a, b

  we can form the $\boxed{\textit{ordered-pair}}$ $\langle a, b\rangle$.

  a and b need not have anything in common, and may be identical.

- Unlike the set $\{a, b\}$, order and repetition in $\langle a, b\rangle$ ***do*** matter:

  $\langle a, b\rangle = \langle c, d\rangle$ iff $a = c$ and $b = d$.

- More generally, for each $k \geqslant 1$ we can form

  the $\boxed{\textit{ordered } k\textit{-tuples}}$ $\langle a_1, \ldots, a_k\rangle$ of the objects $a_1, \ldots, a_k$.

Ordered pairs

- Given any two objects a, b

  we can form the $\boxed{\textit{ordered-pair}}$ $\langle a, b\rangle$.

  a and b need not have anything in common, and may be identical.

- Unlike the set $\{a, b\}$, order and repetition in $\langle a, b\rangle$ ***do*** matter:

  $\langle a, b\rangle = \langle c, d\rangle$ iff $a = c$ and $b = d$.

- More generally, for each $k \geqslant 1$ we can form

  the $\boxed{\textit{ordered } k \textit{-tuples}}$ $\langle a_1, \ldots, a_k\rangle$ of the objects $a_1, \ldots, a_k$.

- As we did for sets, we take the formation of ordered-pairs

  and ordered tuples to be a basic, intuitively clear, operation.

Set-product

- Pairing of objects leads us to $\boxed{\textit{set-product}}$ of two sets A, B :

$$A \times B \quad =_{\mathrm{df}} \quad \{\langle a, b\rangle \mid a \in A,\ b \in B\}$$

Set-product

- Pairing of objects leads us to $\boxed{\textit{set-product}}$ of two sets A, B :

$$A \times B \;=_{\mathrm{df}}\; \{\langle a, b\rangle \mid a \in A,\ b \in B\}$$

- If A has p elements and B has q elements,

  then $A \times B$ has $p \cdot q$ elements.

- Examples.

Set-product

- Pairing of objects leads us to $\boxed{\textit{set-product}}$ of two sets A, B :

$$A \times B \;=_{\mathrm{df}}\; \{\langle a, b\rangle \mid a \in A,\ b \in B\}$$

- If A has p elements and B has q elements,

  then $A \times B$ has $p \cdot q$ elements.

- Examples.
  - $\{a, b\} \times \{0, 1, 2\} = \{\langle a, 0\rangle,\ \langle a, 1\rangle,\ \langle a, 2\rangle,\ \langle b, 0\rangle,\ \langle b, 1\rangle,\ \langle b, 2\rangle\}$

Set-product

- Pairing of objects leads us to $\boxed{\textit{set-product}}$ of two sets A, B:

$$A \times B \quad =_{\text{df}} \quad \{\langle a, b\rangle \mid a \in A,\ b \in B\}$$

- If A has p elements and B has q elements,

  then $A \times B$ has $p \cdot q$ elements.

- Examples.
  - $\{a, b\} \times \{0, 1, 2\} = \{\langle a, 0\rangle,\ \langle a, 1\rangle,\ \langle a, 2\rangle,\ \langle b, 0\rangle,\ \langle b, 1\rangle,\ \langle b, 2\rangle\}$
  - $\mathbb{R} \times \mathbb{R}$ is the real-number ***plane***.
  - $\mathbb{Z} \times \mathbb{Z}$ is the integer grid.

Set-product

- Pairing of objects leads us to $\boxed{\textit{set-product}}$ of two sets A, B :

$$A \times B \quad =_{\text{df}} \quad \{\langle a, b\rangle \mid a \in A,\ b \in B\}$$

- If A has p elements and B has q elements,

  then $A \times B$ has $p \cdot q$ elements.

- Examples.
  - $\{a, b\} \times \{0, 1, 2\} = \{\langle a, 0\rangle,\ \langle a, 1\rangle,\ \langle a, 2\rangle,\ \langle b, 0\rangle,\ \langle b, 1\rangle,\ \langle b, 2\rangle\}$
  - $\mathbb{R} \times \mathbb{R}$ is the real-number ***plane***.
  - $\mathbb{Z} \times \mathbb{Z}$ is the integer grid.
  - $\langle$ US town-names$\rangle$ $\times$ $\langle$ US state-names$\rangle$.

  Some elements: $\langle$*Bloomington*, *Indiana*$\rangle$, $\langle$*Cambridge*, *Ohio*$\rangle$, $\langle$*Portland*, *Maine*$\rangle$

Binary relations

- Given sets A, B any set $R \subseteq A \times B$ is a $\boxed{\textit{binary-relation from } A \textit{ to } B.}$

Binary relations

- Given sets A, B any set $R \subseteq A \times B$ is a $\boxed{\textit{binary-relation from } A \textit{ to } B\,.}$
- When $\langle a, b \rangle \in R$ we also write (in infix)

  $a\,R\,b$ or — if clearer — $a\,(R)\,b$.

- A relation from a set A to itself is a $\boxed{\textit{relation over } A.}$

Binary relations

- Given sets A, B any set $R \subseteq A \times B$ is a $\boxed{\textbf{\textit{binary-relation from }} A \textbf{\textit{ to }} B\,\textbf{.}}$
- When $\langle a, b\rangle \in R$ we also write (in infix)

  $a\,R\,b$ or — if clearer — $a\,(R)\,b$.
- A relation from a set A to itself is a $\boxed{\textbf{\textit{relation over }} A\textbf{.}}$
- With few exceptions we use the usual ***infix notation:*** For $\langle a, b\rangle \in R$ we write $a\,R\,b$.

Examples

- Size order over the real numbers: $\{\langle x, y\rangle \mid x, y \in \mathbb{R},\ x < y\}$.

Examples

- Size order over the real numbers: $\{\langle x, y\rangle \mid x, y \in \mathbb{R},\ x < y\}$.
- Divisibility over the integers:

  $p \mid q$ when p divides q. Eg: $3 \mid 21$.

Examples

- Size order over the real numbers: $\{\langle x, y\rangle \mid x, y \in \mathbb{R},\ x < y\}$.
- Divisibility over the integers:

  $p \mid q$ when p divides q. Eg: $3 \mid 21$.
- Relatively prime:

  $\{\langle p, q\rangle \mid p, q$ have no common divisor $\}$. Eg: 8 and 15

Examples

- Size order over the real numbers: $\{\langle x, y\rangle \mid x, y \in \mathbb{R},\ x < y\}$.
- Divisibility over the integers:

  $p \mid q$ when p divides q. Eg: $3 \mid 21$.
- Relatively prime:

  $\{\langle p, q\rangle \mid p, q$ have no common divisor $\}$. Eg: 8 and 15
- Kinship relations: *parent-of*, *granddaughter-of*, *sibling-of*.

Examples

- Size order over the real numbers: $\{\langle x, y\rangle \mid x, y \in \mathbb{R},\ x < y\}$.
- Divisibility over the integers:

  $p \mid q$ when p divides q. Eg: $3 \mid 21$.
- Relatively prime:

  $\{\langle p, q\rangle \mid p, q$ have no common divisor $\}$. Eg: 8 and 15
- Kinship relations: *parent-of*, *granddaughter-of*, *sibling-of*.
- Reporting relation in an organization.

Examples

- Size order over the real numbers: $\{\langle x, y\rangle \mid x, y \in \mathbb{R},\ x < y\}$.
- Divisibility over the integers:

  $p \mid q$ when p divides q. Eg: $3 \mid 21$.
- Relatively prime:

  $\{\langle p, q\rangle \mid p, q$ have no common divisor $\}$. Eg: 8 and 15
- Kinship relations: *parent-of*, *granddaughter-of*, *sibling-of*.
- Reporting relation in an organization.
- Dependency relation between components of software modules.

⋆ *Renatus Cartesius*

- René Descartes, 1596-1650
- `https://en.wikipedia.org/wiki/Ren%C3%A9_Descartes`
- The unity of Mathematics!

Visual representation by di-graphs

- Any binary relation $R \subseteq A \times A$

  can be represented as a directed-graph without multiple edges:

  The vertices are the elements of A

  and there is an edge $x \leftrightarrow y$ iff $x(R)y$.

MASQUERADING AS EQUALITY

Reflexive relations

- One useful type of relations consists of those who share the essential properties of equality.
- $R \subseteq A \times A$ is $\boxed{\textbf{\textit{reflexive on } } A}$ if xRx for all $x \in A$.
- Note that this property of R, standing alone.

Examples

- Identity over a set A.

Examples

- Identity over a set A.
- $\leqslant$ between integers

Examples

- Identity over a set A.
- $\leqslant$ between integers
- Congruence between angles (over angles in geometry)

Examples

- Identity over a set A.
- $\leqslant$ between integers
- Congruence between angles (over angles in geometry)
- *is-connected-to* (over vertices of an undirected graph)

Examples

- Identity over a set A.
- $\leqslant$ between integers
- Congruence between angles (over angles in geometry)
- *is-connected-to* (over vertices of an undirected graph)

Non-examples:

- *has-same-address-as* (over people): Not everyone has an address!

Examples

- Identity over a set A.
- $\leqslant$ between integers
- Congruence between angles (over angles in geometry)
- *is-connected-to* (over vertices of an undirected graph)

Non-examples:

- *has-same-address-as* (over people): Not everyone has an address!
- *is-the-same-as-integer* as a relation on the real numbers

Examples

- Identity over a set A.
- $\leqslant$ between integers
- Congruence between angles (over angles in geometry)
- *is-connected-to* (over vertices of an undirected graph)

Non-examples:

- *has-same-address-as* (over people): Not everyone has an address!
- *is-the-same-as-integer* as a relation on the real numbers
- Inequality $<$ between real numbers

Which are reflexive?

- *has-same-prime-factors-as* (over $\mathbb{N}$)

Which are reflexive?

- *has-same-prime-factors-as* (over $\mathbb{N}$)   Yes

Which are reflexive?

- *has-same-prime-factors-as* (over $\mathbb{N}$)
- *equi-distant-to-origin* (over points in the plane)

Which are reflexive?

- *has-same-prime-factors-as* (over $\mathbb{N}$)
- *equi-distant-to-origin* (over points in the plane)   Yes

Which are reflexive?

- *has-same-prime-factors-as* (over $\mathbb{N}$)
- *equi-distant-to-origin* (over points in the plane)
- *has-common-border-with* (between countries)

Which are reflexive?

- *has-same-prime-factors-as* (over $\mathbb{N}$)
- *equi-distant-to-origin* (over points in the plane)
- *has-common-border-with* (between countries)

  No: no country has a common border with itself

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Examples:

- Equality (over any set)

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Examples:

- Equality (over any set)
- *has-same-prime-factors-as* (over $\mathbb{N}$)

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Examples:

- Equality (over any set)
- *has-same-prime-factors-as* (over $\mathbb{N}$)
- *is-connected-to* (over vertices of an undirected graphs)

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textbf{symmetric}}$ if $u \, R \, v$ implies $v \, R \, u$

Examples:

- Equality (over any set)
- *has-same-prime-factors-as* (over $\mathbb{N}$)
- *is-connected-to* (over vertices of an undirected graphs)
- *spouse-of*, *sibling-of*, *class-mate-of* (over people)

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Non-examples:

- Weak inequality $\leqslant$

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Non-examples:

- Weak inequality $\leqslant$
- *is-connected-to* (over vertices of a directed graph)

Symmetric relations

$R \subseteq A \times A$ is $\boxed{\textit{symmetric}}$ if $u\,R\,v$ implies $v\,R\,u$

Non-examples:

- Weak inequality $\leqslant$
- *is-connected-to* (over vertices of a directed graph)
- *parent-of*, *supervisor-of* (over people)

Which are symmetric?

- *loves*

Which are symmetric?

- *loves* Unfortunately not

Which are symmetric?

- *loves*
- *earlier-than*

Which are symmetric?

- *loves*
- *earlier-than* No

Which are symmetric?

- *loves*
- *earlier-than*
- *cousin-of*

Which are symmetric?

- *loves*
- *earlier-than*
- *cousin-of*   Yes

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Examples
  - $<$ over $\mathbb{R}$

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Examples
  - $<$ over $\mathbb{R}$
  - *divides* over $\mathbb{N}$

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Examples
  - $<$ over $\mathbb{R}$
  - *divides* over $\mathbb{N}$
  - *ancestor-of* (over people)

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Examples
  - $<$ over $\mathbb{R}$
  - *divides* over $\mathbb{N}$
  - *ancestor-of* (over people)
  - *connected-to* (over vertices of a di-graph)

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Examples
  - $<$ over $\mathbb{R}$
  - *divides* over $\mathbb{N}$
  - *ancestor-of* (over people)
  - *connected-to* (over vertices of a di-graph)
  - $\subseteq$ (over $\mathcal{P}(\mathbb{N})$)

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Non-examples:
  - *parent-of*, *cousin-of*

Transitive relations

- $R \subseteq A \times A$ is $\boxed{\textit{transitive}}$

  if xRy and yRz together imply xRz.

- Non-examples:
  - *parent-of*, *cousin-of*
  - *within-walking-distance-of*

Which are transitive?

- *substring-of*

Which are transitive?

- *substring-of* Yes

Which are transitive?

- *substring-of*
- *brother-in-law-of*

Which are transitive?

- *substring-of*
- *brother-in-law-of* No

Which are transitive?

- *substring-of*
- *brother-in-law-of*
- *relatively-prime-with*

Which are transitive?

- *substring-of*
- *brother-in-law-of*
- *relatively-prime-with* No: Take $\langle 2, 3\rangle$ and $\langle 3, 2\rangle$)

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

- Examples:
  - *is-connected-to* (over an undirected graph)

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

- Examples:
  - *is-connected-to* (over an undirected graph)
  - *has-same-prime-factors-as* (over $\mathbb{N}$)

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

- Examples:
  - *is-connected-to* (over an undirected graph)
  - *has-same-prime-factors-as* (over $\mathbb{N}$)
  - *equi-distant-to-origin* (between points in the plane)

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

- Non-examples

  - *is-descendant-of*, self included (between people)

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

- Non-examples
  - *is-descendant-of*, self included (between people)
  - Identity on $\mathbb{N}$ as a relation on $\mathbb{R}$

Equivalence relations

- ***Reflexivity, symmetry*** and ***transitivity***

  are the basic properties of equality.

- $R \subseteq A \times A$ is an $\boxed{\textit{equivalence}}$ relation

  if it is reflexive on A, symmetric, and transitive.

- Non-examples
  - *is-descendant-of*, self included (between people)
  - Identity on $\mathbb{N}$ as a relation on $\mathbb{R}$
  - *is-connected-to* (between people)

Which are equivalences

- *differs-by-less-than-1* (over $\mathbb{R}$)

Which are equivalences

- *differs-by-less-than-1* (over $\mathbb{R}$) Not transitive

Which are equivalences

- *differs-by-less-than-1* (over $\mathbb{R}$)
- *born-on-same-date-as* (between people)

Which are equivalences

- *differs-by-less-than-1* (over $\mathbb{R}$)
- *born-on-same-date-as* (between people)   Yes

Which are equivalences

- *differs-by-less-than-1* (over $\mathbb{R}$)
- *born-on-same-date-as* (between people)
- *sibling-of* (both parents)

Which are equivalences

- *differs-by-less-than-1* (over $\mathbb{R}$)
- *born-on-same-date-as* (between people)
- *sibling-of* (both parents)   Not reflexive

Equivalence approximates equality

- Intuitively, an equivalence unifies objects

  that share some properties of interest.

Equivalence approximates equality

- Intuitively, an equivalence unifies objects

  that share some properties of interest.

- We think of a cluster of equivalent objects as an $\boxed{\textit{equivalence-class.}}$

Equivalence approximates equality

- Intuitively, an equivalence unifies objects

  that share some properties of interest.

- We think of a cluster of equivalent objects as an $\boxed{\textbf{equivalence-class.}}$

- Such class can be identified by one of its members.

  We'll see that it does not matter which one. So we define:

- Given an equivalence $\sim$ over A, and $x \in A$,

  the $\boxed{\sim\text{-class of } x}$ is defined by

$$[x]_\sim \;=_{\text{df}}\; \{y \in S \mid y \sim x\}$$

Examples of equivalence-classes

- Over $\mathbb{N}$, equality modulo 5, that is *has-same-remainder-over-5-as*.

  $[3]_\sim = \{3, 8, 13, 18, \ldots\}$

Examples of equivalence-classes

- Over $\mathbb{N}$, equality modulo 5, that is *has-same-remainder-over-5-as*.

  $[3]_{\sim} = \{3, 8, 13, 18, \ldots\}$

- For points in the plane, *equidistance-to-origin*.

  $[(1, 0)]_{\sim} =$ the unit circle.

Examples of equivalence-classes

- Over $\mathbb{N}$, equality modulo 5, that is *has-same-remainder-over-5-as*.

  $[3]_\sim = \{3, 8, 13, 18, \ldots\}$

- For points in the plane, *equidistance-to-origin*.

  $[(1,0)]_\sim =$ the unit circle.

- Over an undirected graph, *is-connected-to*

  $[u]_\sim =$ the connected component of u

Class-naming is robust

- What if we "name" $[a]_\sim$ by a different a' in it?
- The choice of "name" makes no difference!:

  if $a' \in [a]_\sim$ then $[a']_\sim = [a]_\sim$.

  In fact $\quad a \sim a' \quad$ iff $\quad [a]_\sim = [a']_\sim$

Class-naming is robust

- What if we “name” $[a]_\sim$ by a different a' in it?
- The choice of “name” makes no difference!:

  if $a' \in [a]_\sim$ then $[a']_\sim = [a]_\sim$.

  In fact $a \sim a'$ iff $[a]_\sim = [a']_\sim$
- $\Rightarrow$: Suppose $a \sim a'$, show $[a]_\sim \subseteq [a']_\sim$ ($[a']_\sim \subseteq [a]_\sim$ is similar).

Class-naming is robust

- What if we "name" $[a]_\sim$ by a different a' in it?
- The choice of "name" makes no difference!:

  if $a' \in [a]_\sim$ then $[a']_\sim = [a]_\sim$.

  In fact $a \sim a'$ iff $[a]_\sim = [a']_\sim$
- $\Rightarrow$: Suppose $a \sim a'$, show $[a]_\sim \subseteq [a']_\sim$

$$
\begin{aligned}
x \in [a]_\sim \quad &\Rightarrow \quad x \sim a && \text{(dfn of } [a]_\sim\text{)} \\
&\Rightarrow \quad x \sim a' && \text{(transitivity, since } a \sim a' \\
&\Rightarrow \quad x \in [a']_\sim
\end{aligned}
$$

Class-naming is robust

- What if we "name" $[a]_\sim$ by a different a' in it?

- The choice of "name" makes no difference!:

  if $a' \in [a]_\sim$ then $[a']_\sim = [a]_\sim$.

  In fact $\quad a \sim a' \quad$ iff $\quad [a]_\sim = [a']_\sim$

- $\Rightarrow$: Suppose $a \sim a'$, show $[a]_\sim \subseteq [a']_\sim$

$$\begin{aligned} x \in [a]_\sim \quad &\Rightarrow \quad x \sim a && \text{(dfn of } [a]_\sim) \\ &\Rightarrow \quad x \sim a' && \text{(transitivity, since } a \sim a' \\ &\Rightarrow \quad x \in [a']_\sim \end{aligned}$$

- $\Leftarrow$: Suppose $[a]_\sim \subseteq [a']_\sim$ show $a \sim a'$

Class-naming is robust

- What if we "name" $[a]_\sim$ by a different a' in it?

- The choice of "name" makes no difference!:

  if $a' \in [a]_\sim$ then $[a']_\sim = [a]_\sim$.

  In fact $\quad a \sim a' \quad$ iff $\quad [a]_\sim = [a']_\sim$

- $\Rightarrow$: Suppose $a \sim a'$, show $[a]_\sim \subseteq [a']_\sim$

$$\begin{array}{llll} x \in [a]_\sim & \Rightarrow & x \sim a & \text{(dfn of } [a]_\sim\text{)} \\ & \Rightarrow & x \sim a' & \text{(transitivity, since } a \sim a' \\ & \Rightarrow & x \in [a']_\sim & \end{array}$$

- $\Leftarrow$: Suppose $[a]_\sim \subseteq [a']_\sim$ show $a \sim a'$

$$\begin{array}{llll} a \sim a & & & \text{(reflexivity)} \\ & \Rightarrow & a \in [a]_\sim & \text{(dfn of } [a]_\sim\text{)} \\ & \Rightarrow & a \in [a']_\sim & \text{(since } [a]_\sim = [a']_\sim\text{)} \\ & \Rightarrow & a \sim a' & \text{(dfn of } [a']_\sim\text{)} \end{array}$$

Order relations

- Order relations are everywhere, starting with the order between integers.
- But they can be different in a variety of ways.

Order relations

- Order relations are everywhere, starting with the order between integers.
- But they can be different in a variety of ways.
  - Integers have a successor, real numbers do not.

Order relations

- Order relations are everywhere, starting with the order between integers.
- But they can be different in a variety of ways.
  - Integers have a successor, real numbers do not.
  - $\mathbb{N}$ has a smallest element, $\mathbb{Z}$ does not.

Order relations

- Order relations are everywhere, starting with the order between integers.
- But they can be different in a variety of ways.
  - Integers have a successor, real numbers do not.
  - $\mathbb{N}$ has a smallest element, $\mathbb{Z}$ does not.
  - Natural numbers always compare under $\leqslant$,

    but not every two sets compare under $\subseteq$.

Order relations

- Order relations are everywhere, starting with the order between integers.
- But they can be different in a variety of ways.
  - Integers have a successor, real numbers do not.
  - $\mathbb{N}$ has a smallest element, $\mathbb{Z}$ does not.
  - Natural numbers always compare under $\leqslant$,

    but not every two sets compare under $\subseteq$.
  - $\mathbb{Q}$ has an element between any two elements, $\mathbb{N}$ does not.

What is common to all order relations?

- Intuition of order is rooted in the natural order:

$$0 < 1 < 2 < 3 \cdots \quad .$$

- Its most essential features are
  - ***Asymmetry:*** uRv contradicts vRu
  - ***Transitivity:*** uRv and vRw together imply uRw.

What is common to all order relations?

- Intuition of order is rooted in the natural order:

$$0 < 1 < 2 < 3 \cdots \qquad .$$

- Its most essential features are
  - ***Asymmetry:*** uRv contradicts vRu
  - ***Transitivity:*** uRv and vRw together imply uRw.
- But historically $\leqslant$ was considered a more useful paradigm.

  So the common characterization of "order" has shifted to be:
- A relation R over a set A is an ***order on*** A if it is
  - Reflexive on A
  - Transitive
  - ***Anti-symmetric:*** uRv and vRu together imply $u = v$.

Order on strings

- We assume that each alphabet Σ comes with some order $\prec$.

Order on strings

- We assume that each alphabet Σ comes with some order $\prec$.
- $\prec$ can be extended to a $\boxed{\textit{size-lex order}}$ $\prec$ between strings. We let

  $\sigma_1 \cdots \sigma_p \prec \tau_1 \cdots \tau_q$ if either $p < q$

  or $p = q$ and for some $i < p$, $\sigma_1 \cdots \sigma_i = \tau_1 \cdots \tau_i$ and $\sigma_{i+1} \prec \tau_{i+1}$
- I.e. strings are ordered by length, and lexicographically within each length.

Order on strings

- We assume that each alphabet Σ comes with some order $\prec$.
- $\prec$ can be extended to a $\boxed{\textit{size-lex order}}$ $\prec$ between strings. We let

  $\sigma_1 \cdots \sigma_p \prec \tau_1 \cdots \tau_q$ if either $p < q$

  or $p = q$ and for some $i < p$, $\sigma_1 \cdots \sigma_i = \tau_1 \cdots \tau_i$ and $\sigma_{i+1} \prec \tau_{i+1}$
- I.e. strings are ordered by length, and lexicographically within each length.
- Any set of strings can be listed in increasing $\prec$ order.
- This is not possible with usual lexicographic order:

  For example, the one-letter Latin string **b**

  is preceded by the infinitely many strings that start with **a**.

MAPPINGS

Binary relations as input-output processes

- A relation from A to B can often be construed as a process that takes elements of A as input and yields corresponding output-values in B.
- For example, the relation *parent-of* can be construed as yielding for any person each one of their children.
- Interpreting relations as processes is not always natural. It is awkward to construe $<$ on $\mathbb{N}$ as a process that maps each x to each $y > x$.

Mappings

- A relation $R \subseteq A \times B$ does not determine the sets A and B,
  because $R \subseteq A' \times B'$ for every $A' \supseteq A$ and $B' \supseteq B$.
- For example, if R maps people to their ancestors aged $\leqslant 150$
  then it also maps people to their ancestor aged $\leqslant 200$.
- We define a $\boxed{\textbf{\textit{mapping}}}$ as a triple (R, A, B) where $R \subseteq A \times B$.
  We write $R: \ A \Rightarrow B$ to state that (A, R, B) is a mapping.
  A is the $\boxed{\textbf{\textit{domain}}}$ of the mapping and B its $\boxed{\textbf{\textit{range}}}$.

Image under a mapping

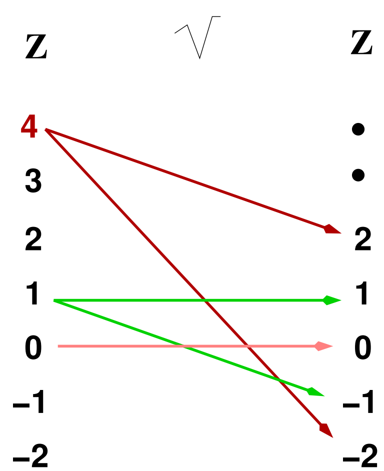
- If $R : A \Rightarrow B$ and $x \in A$ then $R[x]$ is the $\boxed{\textit{image of } x \textit{ under } R}$

Image under a mapping

- If $R : A \Rightarrow B$ and $x \in A$ then
  $R[x]$ is the $\boxed{\textit{image of } x \textit{ under } R}$
- Also, if $A_0 \subseteq A$ then
  $R[A_0] =_{\mathrm{df}} \{\, y \in B \mid x\,(R)\,y$ for some $x \in A_0 \,\}$
  is the $\boxed{\textit{image}}$ of A_0 under R.

Image under a mapping

- If $R : A \Rightarrow B$ and $x \in A$ then
  $R[x]$ is the $\boxed{\textit{image of } x \textit{ under } R}$
- Also, if $A_0 \subseteq A$ then
  $R[A_0] =_{\mathrm{df}} \{ y \in B \mid x\,(R)\,y$ for some $x \in A_0 \}$
  is the $\boxed{\textit{image}}$ of A_0 under R.
- Example: Consider the relation $\surd = \{\langle x^2, x\rangle \mid x \in \mathbb{R}\}$.
  Then $\surd[4] = \{2, -2\}$ $\surd[0] = \{0\}$ $\surd[-4] = \emptyset$



Operations on mappings

Mapping inverse

- The $\boxed{\textit{inverse}}$ of a mapping $R: A \Rightarrow B$ is the mapping $R^{-1}: B \Rightarrow A$ where $x\,(R^{-1})\,y$ iff $y\,(R)\,x$.
- The superscript -1 is borrowed from the reciprocal function $x^{-1} = 1/x$ over $\mathbb{R}$.

Examples

- Inverse of *parent-of* is *child-of*
- Inverse of *loves* is *is-loved-by*
- Inverse of *has-SSN* is *is-SSN-of*
- The inverse of $<$ is $>$,
  and the inverse of $\leqslant$ is $\geqslant$.

Inverting the inverse

- $(R^{-1})^{-1} = R$
- ***Proof.*** $x\,(R^{-1})^{-1}\,y$ iff $y\,(R^{-1})\,x$
  iff $x\,(R)\,y$

Relational-composition

- The $\boxed{\textit{relational-composition}}$ of mappings $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ is the mapping $(R\,;Q) : A \Rightarrow C$ where
  $x\,(R\,;Q)\,z$ iff for some $y \in B$ both $x\,R\,y$ and $y\,Q\,z$.

Relational-composition

- The $\boxed{\textit{relational-composition}}$ of mappings $R: A \Rightarrow B$ and $Q: B \Rightarrow C$
  is the mapping $(R;Q): A \Rightarrow C$ where
  $x\,(R;Q)\,z$ iff for some $y \in B$ both $x\,R\,y$ and $y\,Q\,z$.

- Relational-composition interprets mappings as processes,
  therefore following the procedural order.

  The semi-colon notation reflects this interpretation.

Examples

- Between people: *mother-of* **;** *parent-of* is *grandma-of*.

Examples

- Between people: *mother-of* $;$ *parent-of* is *grandma-of*.
- Over $\mathbb{N}$: $(\leqslant);(\leqslant)$ is $\leqslant$;
  but $(<);(<)$ is $\{\langle p, q\rangle \mid q \geqslant p+2\}$

Examples

- Between people: *mother-of* $;$ *parent-of* is *grandma-of*.
- Over $\mathbb{N}$: $(\leqslant);(\leqslant)$ is $\leqslant$;
  but $(<);(<)$ is $\{\langle p,q\rangle \mid q \geqslant p+2\}$
- Over $\mathbb{R}$: $(<);(<)$ is $(<)$

Examples

- Between people: *mother-of* $;$ *parent-of* is *grandma-of*.
- Over $\mathbb{N}$: $(\leqslant);(\leqslant)$ is $\leqslant$;
  but $(<);(<)$ is $\{\langle p,q\rangle \mid q \geqslant p+2\}$
- Over $\mathbb{R}$: $(<);(<)$ is $(<)$
- Over subsets of $\mathbb{N}$:
  $(\subseteq)\,;\,(\subseteq)$ is $\subseteq$

Examples

- Between people: *mother-of* $\mathbin{;}$ *parent-of* is *grandma-of*.
- Over $\mathbb{N}$: $(\leqslant);(\leqslant)$ is $\leqslant$;
  but $(<);(<)$ is $\{\langle p, q\rangle \mid q \geqslant p+2\}$
- Over $\mathbb{R}$: $(<);(<)$ is $(<)$
- Over subsets of $\mathbb{N}$:
  $(\subseteq)\ ;\ (\subseteq)$ is $\subseteq$

but $(\subset)\ ;\ (\subset)$ is "extending by at least 2 elements".

Inverse of a composition

- $(R\,;Q)^{-1} = Q^{-1}\,;R^{-1}$

Proof. $x\,(R\,;Q)^{-1}\,z$ ***iff*** $z\,(R\,;Q)\,x$ (dfn of inverse)

iff $z\,R\,y$ and $y\,Q\,x$ some y (dfn of $;$)

iff $y\,R^{-1}\,z$ and $x\,Q^{-1}\,y$ some y (dfn of inverse)

iff $x\,(Q^{-1}\,;R^{-1})\,z$ (dfn of $comp$)

Properties of mappings

Four input/output properties

We'll consider four properties that mappings $R\colon A \Rightarrow B$ may have.

[Univalent:]

For every $x \in A$ there is at most one $y \in B$ such that $x\,R\,y$.

Four input/output properties

We'll consider four properties that mappings $R: A \Rightarrow B$ may have.

[Univalent:]

For every $x \in A$ there is at most one $y \in B$ such that $x \, R \, y$.

[Injective:]

For every $y \in B$ there is at most one $x \in A$ such that $x \, R \, y$.

Four input/output properties

We'll consider four properties that mappings $R\colon\ A \Rightarrow B$ may have.

[Univalent:]

For every $x \in A$ there is at most one $y \in B$ such that $x\,R\,y$.

[Injective:]

For every $y \in B$ there is at most one $x \in A$ such that $x\,R\,y$.

[Total:]

For every $x \in A$ there is at least one $y \in B$ such that $x\,R\,y$.

Four input/output properties

We'll consider four properties that mappings $R: A \Rightarrow B$ may have.

[Univalent:]
For every $x \in A$ there is at most one $y \in B$ such that $x\,R\,y$.

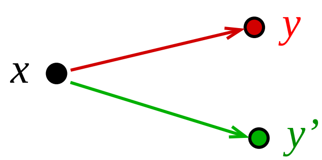
[Injective:]
For every $y \in B$ there is at most one $x \in A$ such that $x\,R\,y$.

[Total:]
For every $x \in A$ there is at least one $y \in B$ such that $x\,R\,y$.

[Surjective:]
For every $y \in B$ there is at least one $x \in A$ such that $x\,R\,y$.

Univalent mappings

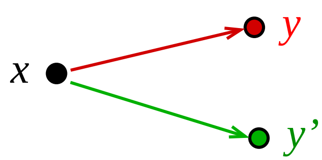
- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{univalent}}$ (or ***single-valued***) if $x(R)y$ and $x(R)y'$ together imply $y = y'$.



NOT ALLOWED

Univalent mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{univalent}}$ (or ***single-valued***) if $x(R)y$ and $x(R)y'$ together imply $y = y'$.



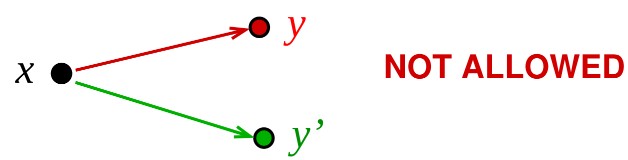
NOT ALLOWED

Examples.

- $\{\langle x, x^2\rangle \mid x \in \mathbb{N}\}$ is univalent:
  every $x \in \mathbb{N}$ yields no other number than x^2.

Univalent mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{univalent}}$ (or ***single-valued***)
  if $x(R)y$ and $x(R)y'$ together imply $y = y'$.

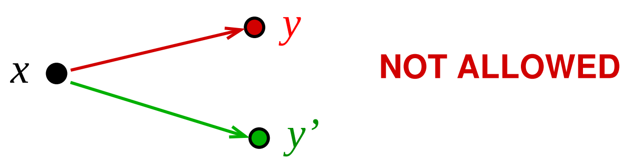


Examples.

- $\{\langle x, x^2\rangle \mid x \in \mathbb{N}\}$ is univalent:
  every $x \in \mathbb{N}$ yields no other number than x^2.
- $\{\langle x^2, x\rangle \mid x \in \mathbb{Z}\}$ is not univalent:
  we have both $\langle 4, 2\rangle$ and $\langle 4, -2\rangle$.

Univalent mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{univalent}}$ (or ***single-valued***) if $x(R)y$ and $x(R)y'$ together imply $y = y'$.

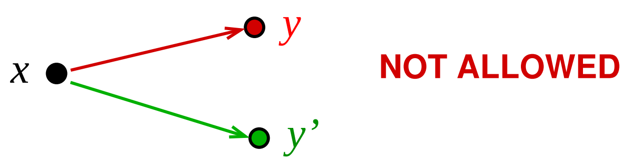


Examples.

- $\{\langle x, x^2\rangle \mid x \in \mathbb{N}\}$ is univalent: every $x \in \mathbb{N}$ yields no other number than x^2.
- $\{\langle x^2, x\rangle \mid x \in \mathbb{Z}\}$ is not univalent: we have both $\langle 4, 2\rangle$ and $\langle 4, -2\rangle$.
- *married-to* is univalent assuming monogamy.

Univalent mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{univalent}}$ (or ***single-valued***)
  if $x(R)y$ and $x(R)y'$ together imply $y = y'$.

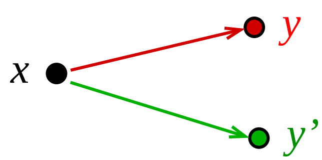


Non-examples.

- Neither *has-as-parent* nor *has-as-child* is univalent:
  people have more than one parent, and can have more than one child.

Univalent mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{univalent}}$ (or ***single-valued***)
  if $x(R)y$ and $x(R)y'$ together imply $y = y'$.



NOT ALLOWED

Non-examples.

- Neither *has-as-parent* nor *has-as-child* is univalent:
  people have more than one parent, and can have more than one child.
- $\leqslant$ on $\mathbb{N}$: any $x \in \mathbb{N}$ is mapped to each $y \geqslant x$.

Composition of univalent mappings

- If $R : A \Rightarrow B$ and $Q :\ B \Rightarrow C$ are univalent
  then so is $R;Q :\ A \Rightarrow C$.

Composition of univalent mappings

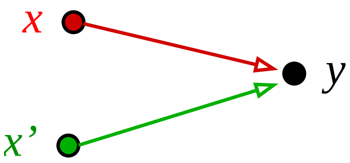
- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are univalent then so is $R\,;Q : A \Rightarrow C$.
- ***Proof.*** Suppose $x\,(R\,;Q)\,z$ and $x\,(R\,;Q)\,z'$, that is $x\,(R)\,y\,(Q)\,z$ and $x\,(R)\,y'\,(Q)\,z'$ for some $y, y' \in B$

Composition of univalent mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are univalent
  then so is $R ; Q : A \Rightarrow C$.
- ***Proof.*** Suppose $x\,(R ; Q)\,z$ and $x\,(R ; Q)\,z'$,
  that is $x\,(R)\,y\,(Q)\,z$ and $x\,(R)\,y'\,(Q)\,z'$ for some $y, y' \in B$
- Then $y = y'$ because R is univalent,
  and so $z = z'$ because Q is univalent.

Injective mappings

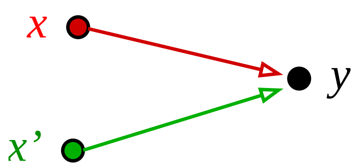
- $R: A \Rightarrow B$ is $\boxed{\textit{injective}}$ if
  $x\,R\,y$ and $x'\,R\,y$ together imply $x = x'$



NOT ALLOWED

Injective mappings

- $R: A \Rightarrow B$ is $\boxed{\textit{injective}}$ if
  $x\,R\,y$ and $x'\,R\,y$ together imply $x = x'$



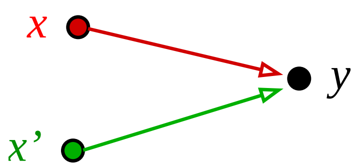
NOT ALLOWED

Examples:

- The mapping from cars to their plate-number is injective:
  No two cars have the same plate number.

Injective mappings

- $R: A \Rightarrow B$ is $\boxed{\textit{injective}}$ if
  $x\,R\,y$ and $x'\,R\,y$ together imply $x = x'$



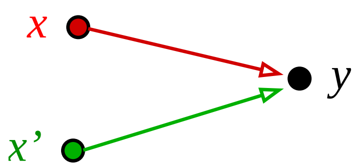
NOT ALLOWED

Examples:

  - The mapping from cars to their plate-number is injective:
    No two cars have the same plate number.
  - $\{\langle x^2, x\rangle \mid x \in \mathbb{N}\}$ is injective:
    different squares have different roots.

Injective mappings

- $R: A \Rightarrow B$ is $\boxed{\textit{injective}}$ if
  $x\,R\,y$ and $x'\,R\,y$ together imply $x = x'$



NOT ALLOWED

Examples:

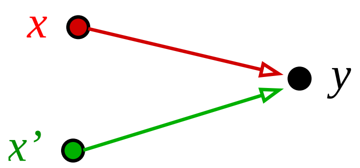
- The mapping from cars to their plate-number is injective:
  No two cars have the same plate number.
- $\{\langle x^2, x\rangle \mid x \in \mathbb{N}\}$ is injective:
  different squares have different roots.

Non-examples:

- $\{\langle x, x^2\rangle \mid x \in \mathbb{N}\}$ is not injective:
  2 and -2 are mapped to the same number.

Injective mappings

- $R: A \Rightarrow B$ is $\boxed{\textit{injective}}$ if
  $x\,R\,y$ and $x'\,R\,y$ together imply $x = x'$



NOT ALLOWED

Examples:

- The mapping from cars to their plate-number is injective: No two cars have the same plate number.
- $\{\langle x^2, x\rangle \mid x \in \mathbb{N}\}$ is injective: different squares have different roots.

Non-examples:

- $\{\langle x, x^2\rangle \mid x \in \mathbb{N}\}$ is not injective: 2 and -2 are mapped to the same number.
- The mapping from people to their name is not injective: different people may have the same name.

Which are injective?

- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$

Which are injective?

- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$ No. Both 2 and -2 map to 4.

Which are injective?

- $\{\langle x, x^2 \rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3 \rangle \mid x \in \mathbb{R}\}$

Which are injective?

- $\{\langle x, x^2 \rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3 \rangle \mid x \in \mathbb{R}\}$ Yes

Which are injective?

- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3\rangle \mid x \in \mathbb{R}\}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ first prime $\geqslant x\}$

Which are injective?

- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3\rangle \mid x \in \mathbb{R}\}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ first prime $\geqslant x\ \}$
  No. This maps both 8 and 9 to 11.

Which are injective?

- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3\rangle \mid x \in \mathbb{R}\}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ first prime $\geqslant x\ \}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ the n'th prime $\}$

Which are injective?

- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3\rangle \mid x \in \mathbb{R}\}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ first prime $\geqslant x\ \}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ the n'th prime $\}$ Yes.

Which are injective?

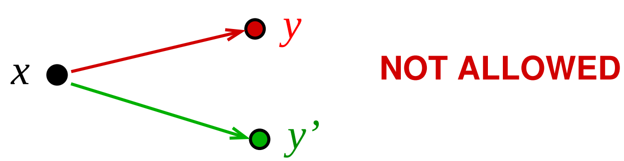
- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3\rangle \mid x \in \mathbb{R}\}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p = \text{ first prime } \geqslant x\ \}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p = \text{ the } n\text{'th prime }\}$
- The mapping from US residents to their SSN.

Which are injective?

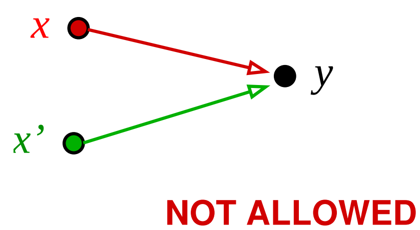
- $\{\langle x, x^2\rangle \mid x \in \mathbb{R}\}$
- $\{\langle x, x^3\rangle \mid x \in \mathbb{R}\}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ first prime $\geqslant x\ \}$
- $\{\langle n, p\rangle \mid n \in \mathbb{N},\ p =$ the n'th prime $\}$
- The mapping from US residents to their SSN.
  Yes. No SSN is assigned to two different persons.

Injective is the dual of univalent

- Univalent:
  At most one output per input.



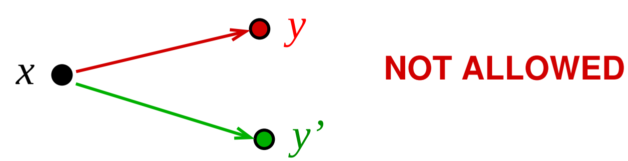
- Injective:
  at most one input per output.



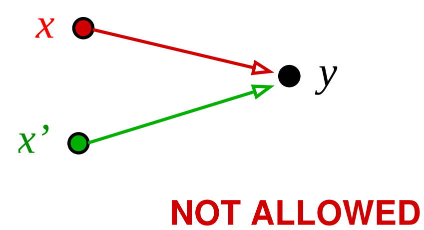
- $R : A \Rightarrow B$ is univalent iff $R^{-1} : B \Rightarrow A$ is injective

Injective is the dual of univalent

- Univalent:
  At most one output per input.



- Injective:
  at most one input per output.



- $R : A \Rightarrow B$ is univalent iff $R^{-1} : B \Rightarrow A$ is injective

- ***Proof.*** $x\,(R)\,y$ plus $x\,(R)\,y'$ imply $y = y'$
  iff
  $y\,(R^{-1})\,x$ plus $y'\,(R^{-1})\,x$ imply $y = y'$,

Composition of injective mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are injective then so is $R;Q : A \Rightarrow C$.

Composition of injective mappings

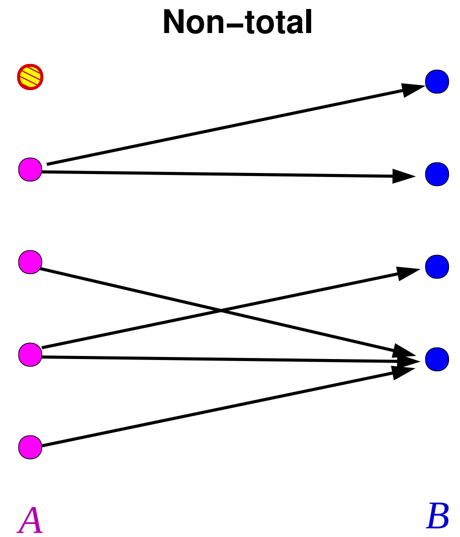
- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are injective
  then so is $R ; Q : A \Rightarrow C$.
- ***Proof.*** Assume $x\,(R;Q)\,z$ and $x'\,(R;Q)\,z$.
  That is, $x\,(R)\,y\,(Q)\,z$ and $x'\,(R)\,y'\,(Q)\,z$ for some $y, y' \in B$.

Composition of injective mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are injective
  then so is $R \mathbin{;} Q : A \Rightarrow C$.
- ***Proof.*** Assume $x\,(R \mathbin{;} Q)\,z$ and $x'\,(R \mathbin{;} Q)\,z$.
  That is, $x\,(R)\,y\,(Q)\,z$ and $x'\,(R)\,y'\,(Q)\,z$ for some $y, y' \in B$.
- $y = y'$ because Q is injective,
  and therefore $x = x'$ because R is injective.

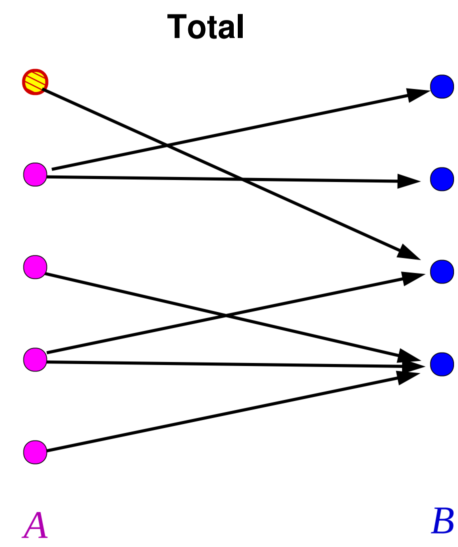
Total mappings

- A mapping $R:\ A \Rightarrow B$ is $\boxed{\textit{total}}$ if
  for each $x \in A$ there is a y such that $x\,(R)\,y$.



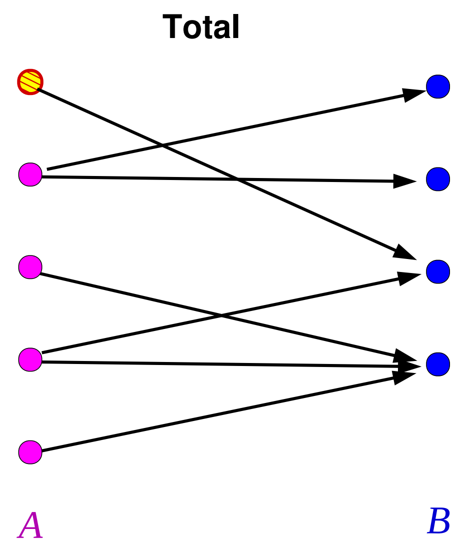
Total mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{total}}$ if for each $x \in A$ there is a y such that $x\,(R)\,y$.



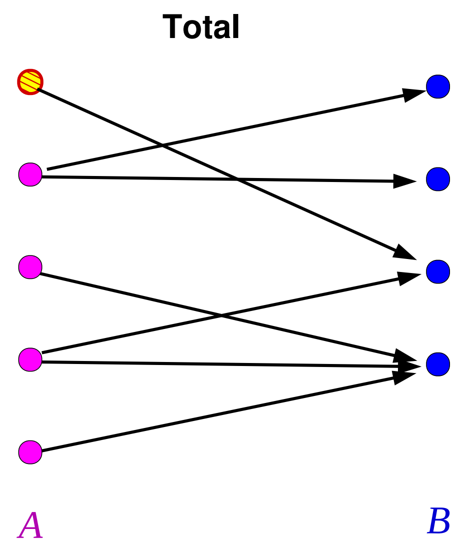
Total mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{total}}$ if for each $x \in A$ there is a y such that $x\,(R)\,y$.
- Note: Totality is a property of the mapping, not just the relation R.



Total mappings

- A mapping $R : A \Rightarrow B$ is $\boxed{\textit{total}}$ if for each $x \in A$ there is a y such that $x\,(R)\,y$.
- Note: Totality is a property of the mapping, not just the relation R.

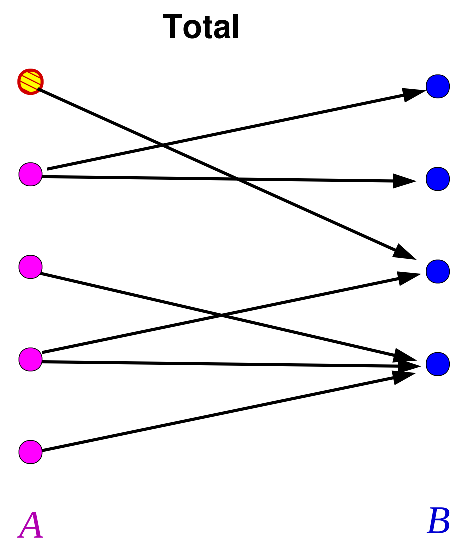


Examples.

- *born-on* over people.

Total mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{total}}$ if
  for each $x \in A$ there is a y such that $x\,(R)\,y$.
- Note: Totality is a property of the mapping,
  not just the relation R.

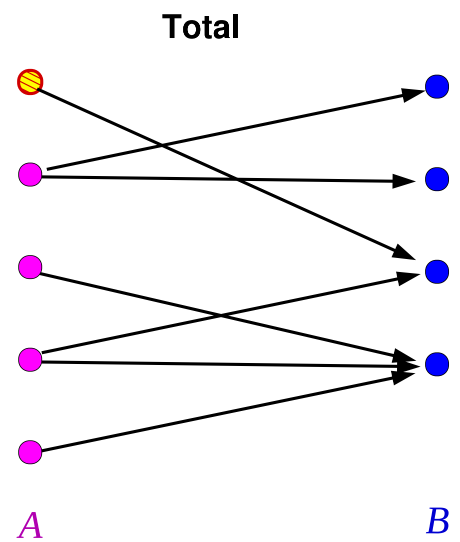


Examples.

- *born-on* over people.
- The mapping *has-integer-value* from real numbers to integers

Total mappings

- A mapping $R : A \Rightarrow B$ is $\boxed{\textit{total}}$ if for each $x \in A$ there is a y such that $x\,(R)\,y$.
- Note: Totality is a property of the mapping, not just the relation R.



Examples.

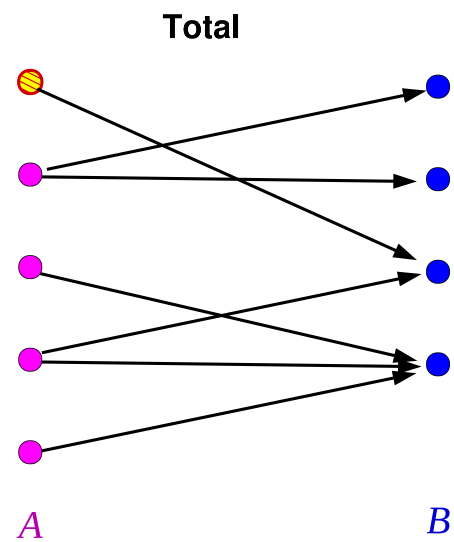
- *born-on* over people.
- The mapping *has-integer-value* from real numbers to integers

Non-examples.

- The reciprocal mapping $(1/x)$ on $\mathbb{R}$ has no output for input 0.

Total mappings

- A mapping $R : A \Rightarrow B$ is $\boxed{\textit{total}}$ if for each $x \in A$ there is a y such that $x\,(R)\,y$.
- Note: Totality is a property of the mapping, not just the relation R.



Examples.

- *born-on* over people.
- The mapping *has-integer-value* from real numbers to integers

Non-examples.

- The reciprocal mapping $(1/x)$ on $\mathbb{R}$ has no output for input 0.
- The trigonometric mapping $\tan$ (tangent) has no output for input $k\pi/2$ for odd integers k.

Composition of total mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are total
  then so is $R;Q : A \Rightarrow C$.

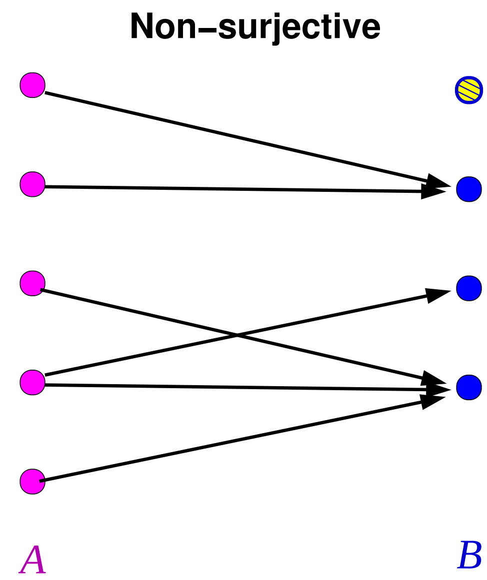
Composition of total mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are total
  then so is $R ; Q : A \Rightarrow C$.
- ***Proof.*** If $x \in A$ then $x \,(R), y$ for some $y \in B$,
  since R is total.

  So $y \,(Q)\, z$ for some $z \in C$, since Q is total.
  Put together, we obtain $x \,(R ; Q)\, z$ for some z.

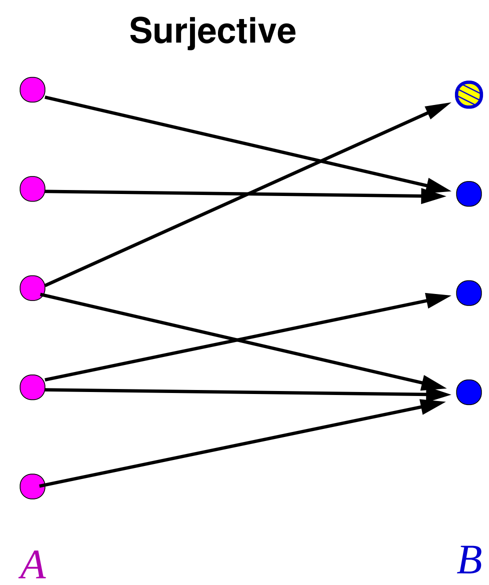
Surjective mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.



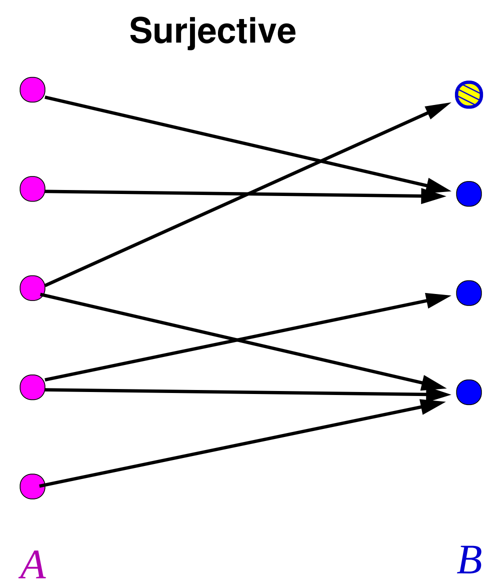
Surjective mappings

- A mapping $R:\ A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.



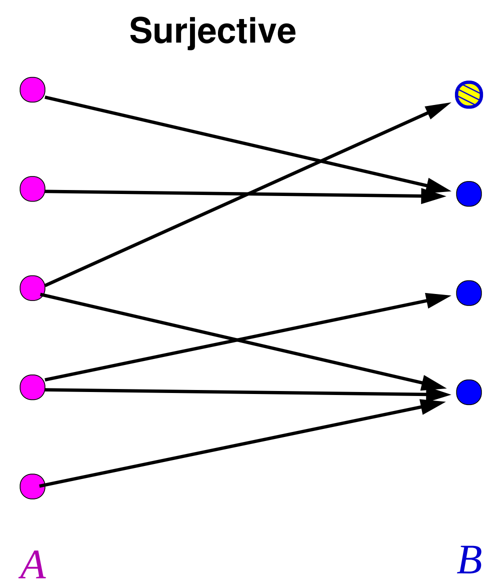
Surjective mappings

- A mapping $R:\ A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.
- Surjectivity is the dual of totality:
  $R:\ A \Rightarrow B$ is total iff $R^{-1}:\ B \Rightarrow A$ is surjective.



Surjective mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.
- Surjectivity is the dual of totality:
  $R: A \Rightarrow B$ is total iff $R^{-1}: B \Rightarrow A$ is surjective.



Examples.

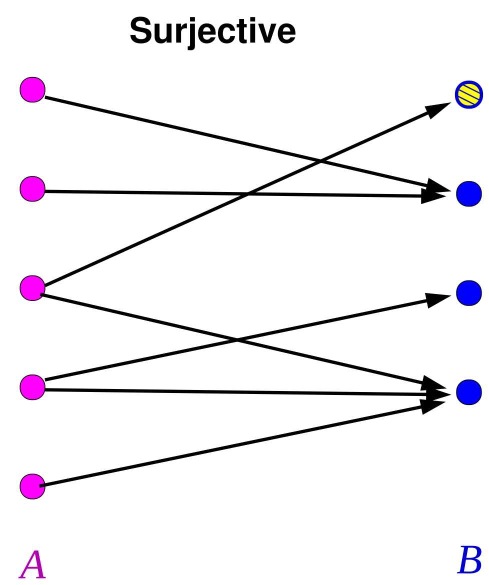
- The trigonometric function $\sin: \mathbb{R} \Rightarrow [-1..1]$.

Surjective mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.
- Surjectivity is the dual of totality:
  $R: A \Rightarrow B$ is total iff $R^{-1}: B \Rightarrow A$ is surjective.

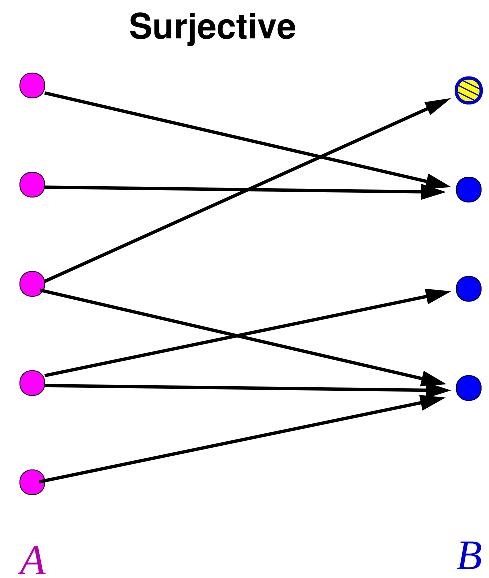
Examples.

- The trigonometric function $\sin: \mathbb{R} \Rightarrow [-1..1]$.
- The cubic function over $\mathbb{R}$.



Surjective mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.
- Surjectivity is the dual of totality:
  $R: A \Rightarrow B$ is total iff $R^{-1}: B \Rightarrow A$ is surjective.

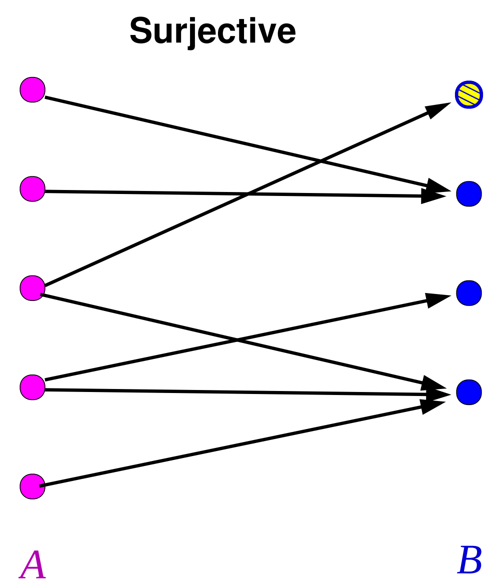


Examples.

- The trigonometric function $\sin: \mathbb{R} \Rightarrow [-1..1]$.
- The cubic function over $\mathbb{R}$.
- The mapping over humanity that maps people to their children

Surjective mappings

- A mapping $R: A \Rightarrow B$ is **surjective** (or **onto**) if for each $y \in B$ there is an x such that $x\,(R)\,y$.
- Surjectivity is the dual of totality: $R: A \Rightarrow B$ is total iff $R^{-1}: B \Rightarrow A$ is surjective.



Examples.

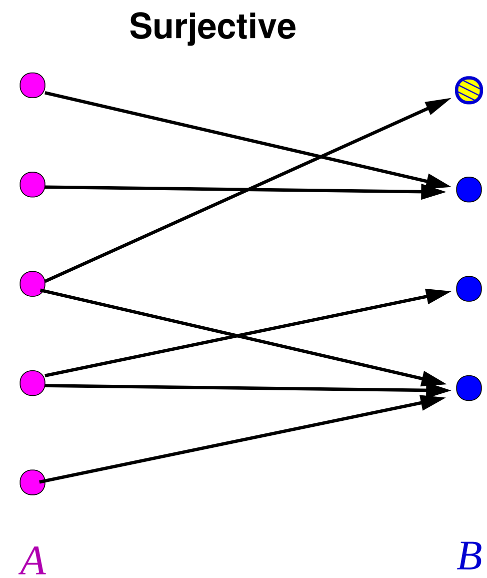
- The trigonometric function $\sin: \mathbb{R} \Rightarrow [-1..1]$.
- The cubic function over $\mathbb{R}$.
- The mapping over humanity that maps people to their children

Non-Examples.

- The squaring function over $\mathbb{N}$.

Surjective mappings

- A mapping $R: A \Rightarrow B$ is $\boxed{\textit{surjective}}$ (or $\boxed{\textit{onto}}$) if for each $y \in B$ there is an x such that $x\,(R)\,y$.
- Surjectivity is the dual of totality:
  $R: A \Rightarrow B$ is total iff $R^{-1}: B \Rightarrow A$ is surjective.



Examples.

- The trigonometric function $\sin: \mathbb{R} \Rightarrow [-1..1]$.
- The cubic function over $\mathbb{R}$.
- The mapping over humanity that maps people to their children

Non-Examples.

- The squaring function over $\mathbb{N}$.
- The mapping over humanity that maps people to their spouse

Composition of surjective mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are surjective
  then so is $R ; Q : A \Rightarrow C$.

Composition of surjective mappings

- If $R : A \Rightarrow B$ and $Q : B \Rightarrow C$ are surjective then so is $R;Q : A \Rightarrow C$.
- ***Proof.*** Given that $Q : B \Rightarrow C$ is surjective, for every $z \in C$ there is a $y \in B$ such that $y\,(Q)\,z$.
- This implies, Since $R : A \Rightarrow B$ is surjective, that $x\,(R)\,y$ for some $x \in A$.
- Thus $x\,(R;Q)\,z$.
  Since this holds for every $z \in C$, $R;Q : A \Rightarrow C$ is surjective.

FUNCTIONS

Functions: univalent and total

- When a mapping $R: A \Rightarrow B$ is univalent
  we also say that it is a $\boxed{\textit{partial-function}}$ (from A to B),
  and write $R: A \rightharpoonup B$ (note the maimed arrow).

Functions: univalent and total

- When a mapping $R : A \Rightarrow B$ is univalent
  we also say that it is a $\boxed{\textit{partial-function}}$ (from A to B),
  and write $R : A \rightharpoonup B$ (note the maimed arrow).

- When that mapping is also total
  we say that it is a $\boxed{\textit{total-function}}$ (or $\boxed{\textit{function}}$ for short),
  and write $R : A \to B$.

Functions: univalent and total

- When a mapping $R : A \Rightarrow B$ is univalent
  we also say that it is a $\boxed{\textit{partial-function}}$ (from A to B),
  and write $R : A \rightharpoonup B$ (note the maimed arrow).

- When that mapping is also total
  we say that it is a $\boxed{\textit{total-function}}$ (or $\boxed{\textit{function}}$ for short),
  and write $R : A \to B$.

- A partial-function $R : A \rightharpoonup B$ is "partial" in that
  it is ***not necessarily*** total (on B).

  So every total-function is also a partial-function!

  And a partial-function may be total or ***non-total***.

Functions and naming

- ***Univalence***

  is the most consequential property that a mapping can have:

  it enables the naming of new mathematical objects!

Functions and naming

- ***Univalence***

  is the most consequential property that a mapping can have:

  it enables the naming of new mathematical objects!

- If $F : A \to B$ and $x\,(F)\,y$ we write $F(x)$ for y.

Functions and naming

- ***Univalence***

  is the most consequential property that a mapping can have:

  it enables the naming of new mathematical objects!

- If $F : A \to B$ and $x\,(F)\,y$ we write $F(x)$ for y.

- When $F : A \rightharpoonup B$ (i.e. totality not assumed),

  we still write $F(x)$ for the y satisfying $x\,(F)\,y$,

  and say that F is ***undefined*** if no such y exists.

Explicit function definitions

- Consider a function definition: $F(x, y) = 2 \cdot x + y$.
  Here F is defined in terms of 2, addition, and multiplication.

Explicit function definitions

- Consider a function definition: $F(x, y) = 2 \cdot x + y$.

  Here F is defined in terms of 2, addition, and multiplication.

- An $\boxed{\textit{explicit definition}}$ of a function $F : A \Rightarrow B$ from objects $c_1, c_2 \ldots \in A$ and functions $g_1, g_2 \ldots$ over A can be given by an equation

$$F(x_1, \ldots, x_k) = E$$

  where E is an "algebraic expression" built from

  the c_i's, g_j's and variables $x_1 \ldots x_k$

  by function application.

Explicit function definitions

- Consider a function definition: $F(x, y) = 2 \cdot x + y$.
  Here F is defined in terms of 2, addition, and multiplication.

- An $\boxed{\textit{explicit definition}}$ of a function $F : A \Rightarrow B$ from objects $c_1, c_2 \ldots \in A$ and functions $g_1, g_2 \ldots$ over A can be given by an equation

$$F(x_1, \ldots, x_k) = E$$

  where E is an "algebraic expression" built from
  the c_i's, g_j's and variables $x_1 \ldots x_k$
  by function application.

- To refer to a function on the fly, without naming it,
  we use the ***"maps-to"*** notation: $x \mapsto E$.
  Example: $x \mapsto 2x + 1$.

Examples of total-functions

- over the set of people:

  $F(p) =$ the (biological) mother of p.

Examples of total-functions

- over the set of people:

  $F(p) =$ the (biological) mother of p.

- Predecessor over the integers: $x \mapsto x{-}1$.

  Cut-off predecessor over $\mathbb{N}$: $x \mapsto$ if $x = 0$ then 0 else $x{-}1$.

Examples of total-functions

- over the set of people:

  $F(p) =$ the (biological) mother of p.

- Predecessor over the integers: $x \mapsto x-1$.

  Cut-off predecessor over $\mathbb{N}$: $x \mapsto$ if $x = 0$ then 0 else $x-1$.

- A function $F : A \to B$ for which $F(x) = b$

  for a fixed $b \in B$ is a **constant-function**.

Examples of total-functions

- over the set of people:
  $F(p) =$ the (biological) mother of p.
- Predecessor over the integers: $x \mapsto x-1$.
  Cut-off predecessor over $\mathbb{N}$: $x \mapsto$ if $x = 0$ then 0 else $x-1$.
- A function $F : A \to B$ for which $F(x) = b$
  for a fixed $b \in B$ is a ***constant-function***.
- For any set A the ***identity function*** over A $\mathrm{Id}_A : A \to A$ defined by $x \mapsto x$.

Examples of total-functions

- over the set of people:
  $F(p) =$ the (biological) mother of p.
- Predecessor over the integers: $x \mapsto x-1$.
  Cut-off predecessor over $\mathbb{N}$: $x \mapsto$ if $x = 0$ then 0 else $x-1$.
- A function $F : A \to B$ for which $F(x) = b$
  for a fixed $b \in B$ is a ***constant-function***.
- For any set A the ***identity function*** over A $\mathrm{Id}_A : A \to A$ defined by $x \mapsto x$.
- The reciprocal-function over $\mathbb{R}^+$ $x \mapsto 1/x$ is a total-function.

Examples of total-functions

- over the set of people:
  $F(p) =$ the (biological) mother of p.
- Predecessor over the integers: $x \mapsto x-1$.
  Cut-off predecessor over $\mathbb{N}$: $x \mapsto$ if $x = 0$ then 0 else $x-1$.
- A function $F : A \to B$ for which $F(x) = b$
  for a fixed $b \in B$ is a **constant-function**.
- For any set A the **identity function** over A $\mathrm{Id}_A : A \to A$ defined by $x \mapsto x$.
- The reciprocal-function over $\mathbb{R}^+$ $x \mapsto 1/x$ is a total-function.
- $F(n) =$ the first prime number $\geqslant n$.
  That this function is total is akin to saying that
  there are infinitely many primes.

Examples of partial-functions

Examples of partial-functions

- The reciprocal function over $\mathbb{R}$
  (it is undefined for 0).

Examples of partial-functions

- The reciprocal function over $\mathbb{R}$
  (it is undefined for 0).
- Over the set of people: $p \mapsto$ the spouse of p
  (not every person is married).

Examples of partial-functions

- The reciprocal function over $\mathbb{R}$
  (it is undefined for 0).
- Over the set of people: $p \mapsto$ the spouse of p
  (not every person is married).
- Over $\mathcal{P}(\mathbb{N})$: $A \mapsto$ the smallest element of A
  (Undefined for $\emptyset$.)

Examples of partial-functions

- The reciprocal function over $\mathbb{R}$
  (it is undefined for 0).
- Over the set of people: $p \mapsto$ the spouse of p
  (not every person is married).
- Over $\mathcal{P}(\mathbb{N})$: $A \mapsto$ the smallest element of A
  (Undefined for $\emptyset$.)
- For any sets A, B we have an ***empty partial-function*** $\emptyset : A \rightharpoonup B$.
  That is, $\emptyset(x)$ is undefined for all $x \in A$.

Functions of several arguments

- Let $F : A \times B \rightharpoonup C$.
  We write $F(a, b)$ for $F(\langle a, b\rangle)$.
- This convention can be applied to functions with more than two arguments.

Functions of several arguments

- Let $F : A \times B \rightharpoonup C$.
  We write $F(a, b)$ for $F(\langle a, b\rangle)$.
- This convention can be applied to functions with more than two arguments.
- Example: Addition, multiplication and exponentiation
  are binary functions over $\mathbb{R}$.

Functions of several arguments

- Let $F : A \times B \rightharpoonup C$.
  We write $F(a,b)$ for $F(\langle a,b\rangle)$.

- This convention can be applied to functions with more than two arguments.

- Example: Addition, multiplication and exponentiation
  are binary functions over $\mathbb{R}$.

- We use infix notation for most binary functions: $x+y$ for $+(x,y)$.

Bijections

- An injective function is an $\boxed{\textbf{\textit{injection.}}}$
- A surjective function is a $\boxed{\textbf{\textit{surjection.}}}$

Bijections

- An injective function is an $\boxed{\textit{injection.}}$
- A surjective function is a $\boxed{\textit{surjection.}}$
- If $f : A \to B$ is both injective and surjective then it is a $\boxed{\textit{bijection}}$ and we write $f : A \cong B$.

Bijections

- An injective function is an $\boxed{\textit{injection.}}$
- A surjective function is a $\boxed{\textit{surjection.}}$
- If $f : A \to B$ is both injective and surjective
  then it is a $\boxed{\textit{bijection}}$ and we write $f : A \cong B$.
- So a bijection has all four I/O properties:
  univalent, injective, total and surjective.

Bijections

- An injective function is an $\boxed{\textit{injection.}}$
- A surjective function is a $\boxed{\textit{surjection.}}$
- If $f : A \to B$ is both injective and surjective
  then it is a $\boxed{\textit{bijection}}$ and we write $f : A \cong B$.
- So a bijection has all four I/O properties:
  univalent, injective, total and surjective.
- If there is a bijection from A to B
  then we write $A \cong B$ and say that A and B are $\boxed{\textit{equipollent.}}$

Examples

- In a concert hall filled to capacity
  the function that maps each person to their seat.

Examples

- In a concert hall filled to capacity
  the function that maps each person to their seat.
- The mapping $x \mapsto 1/x$ over the positive real numbers.

Examples

- In a concert hall filled to capacity
  the function that maps each person to their seat.
- The mapping $x \mapsto 1/x$ over the positive real numbers.
- The successor-modulo-12 function over $[0..11]$.

Examples

- In a concert hall filled to capacity
  the function that maps each person to their seat.
- The mapping $x \mapsto 1/x$ over the positive real numbers.
- The successor-modulo-12 function over $[0..11]$.
- Let $d(x) = 2x$.

$d : \mathbb{R} \rightharpoonup \mathbb{R}$ is a bijection.
$d : \mathbb{N} \rightharpoonup \mathbb{N}$ is not: it is not surjective.
$d : \mathbb{N} \rightharpoonup \textit{Even}$ is a bijection.

Closure properties of bijections

- **Theorem.** The inverse of a bijection $F : A \Rightarrow B$ is a bijection.

Closure properties of bijections

- **Theorem.** The inverse of a bijection $F : A \Rightarrow B$ is a bijection.
- ***Proof.*** A bijection $f : A \Rightarrow B$ is univalent, total, injective and surjective, so $f^{-1} : B \Rightarrow A$ is injective, surjective, univalent and total.

Closure properties of bijections

- **Theorem.** The inverse of a bijection $F : A \Rightarrow B$ is a bijection.
- ***Proof.*** A bijection $f : A \Rightarrow B$ is univalent, total, injective and surjective, so $f^{-1} : B \Rightarrow A$ is injective, surjective, univalent and total.
- **Theorem** The composition of bijections $f : A \Rightarrow B$ and $g : B \Rightarrow C$ is a bijection $(f\,;g) : A \Rightarrow C$.

Closure properties of bijections

- **Theorem.** The inverse of a bijection $F : A \Rightarrow B$ is a bijection.
- ***Proof.*** A bijection $f : A \Rightarrow B$ is univalent, total, injective and surjective, so $f^{-1} : B \Rightarrow A$ is injective, surjective, univalent and total.
- **Theorem** The composition of bijections $f : A \Rightarrow B$ and $g : B \Rightarrow C$ is a bijection $(f \mathbin{;} g) : A \Rightarrow C$.
- ***Proof.*** We saw above that the properties univalent, total, injective and surjective are all closed under composition.

Equipollence is an equivalence

- **Theorem** $\cong$ is reflexive, symmetric and transitive.
- ***Proof.*** $\cong$ is

Equipollence is an equivalence

- **Theorem** $\cong$ is reflexive, symmetric and transitive.
- ***Proof.*** $\cong$ is
  - Reflexive: For each A we have $\mathsf{Id}_A : A \cong A$.

Equipollence is an equivalence

- **Theorem** $\cong$ is reflexive, symmetric and transitive.
- ***Proof.*** $\cong$ is
  - Reflexive: For each A we have $\mathsf{Id}_A : A \cong A$.
  - Symmetric: If $f : A \cong B$ then $f^{-1} : B \cong A$.

Equipollence is an equivalence

- **Theorem** $\cong$ is reflexive, symmetric and transitive.
- ***Proof.*** $\cong$ is
  - Reflexive: For each A we have $\mathsf{Id}_A : A \cong A$.
  - Symmetric: If $f : A \cong B$ then $f^{-1} : B \cong A$.
  - Transitive: If $F : A \cong B$ and $G : B \cong C$ then $F\,;G : A \cong C$.

SET SIZE

Comparing set size

- When we say that a set S *"is smaller than"* B
  we commonly mean that
  - The count $p \in \mathbb{N}$ of A's elements
    is $<$ than the count q of B.

Comparing set size

- When we say that a set S *"is smaller than"* B
  we commonly mean that
  - The count $p \in \mathbb{N}$ of A's elements
    is $<$ than the count q of B.
- "Counting" A means defining a bijection $j: \{1, \ldots, p\} \to A$.

Comparing set size

- When we say that a set S *"is smaller than"* B
  we commonly mean that
  - The count $p \in \mathbb{N}$ of A's elements
    is $<$ than the count q of B .
- "Counting" A means defining a bijection $j : \{1, \ldots, p\} \to A$.
- This size-comparison of A and B makes a ***detour*** via $\mathbb{N}$.
  Is that detour useful? necessary?

Comparing set size

- When we say that a set S *"is smaller than"* B
  we commonly mean that
  - The count $p \in \mathbb{N}$ of A's elements
    is $<$ than the count q of B.
- "Counting" A means defining a bijection $j : \{1, \ldots, p\} \rightarrow A$.
- This size-comparison of A and B makes a ***detour*** via $\mathbb{N}$.
  Is that detour useful? necessary?

  It is a strole of genius for finite sets.

  It is not necessary.

  It hinders generalization of size to infinite sets!

Comparing size, in general

- ***Show "set A is no larger than set B" without counting.***

Comparing size, in general

- ***Show "set A is no larger than set B" without counting.***
- One option is clear: $A \subseteq B$.
  What if A is not related to B ?

Comparing size, in general

- ***Show "set A is no larger than set B" without counting.***
- One option is clear: $A \subseteq B$.
  What if A is not related to B ?
- **Dfn.** *An* $\boxed{\textbf{\textit{embedding}}}$ *of* A *in* B *is an injection* $j:\ A \to B$.

Comparing size, in general

- ***Show "set A is no larger than set B" without counting.***
- One option is clear: $A \subseteq B$.
  What if A is not related to B ?
- **Dfn.** *An* $\boxed{\textbf{\textit{embedding}}}$ *of A in B is an injection $j: A \to B$.*
- If such an embedding exists, we write $A \preccurlyeq B$.

Comparing size, in general

- ***Show "set A is no larger than set B" without counting.***
- One option is clear: $A \subseteq B$.
  What if A is not related to B ?
- **Dfn.** *An* $\boxed{\textbf{\textit{embedding}}}$ *of A in B is an injection $j:\ A \to B$.*
- If such an embedding exists, we write $A \preccurlyeq B$.

Think of it as assigning a "name" in B to each element of A .

Comparing size, in general

- ***Show "set A is no larger than set B" without counting.***
- One option is clear: $A \subseteq B$.
  What if A is not related to B ?
- **Dfn.** *An* $\boxed{\textit{embedding}}$ *of A in B is an injection $j : A \to B$.*
- If such an embedding exists, we write $A \preccurlyeq B$.

  Think of it as assigning a "name" in B to each element of A .
- The composition of injections is an injection, so:
  Theorem. $\preccurlyeq$ is transitive: If $A \preccurlyeq B \preccurlyeq C$ then $A \preccurlyeq C$.

Examples

- For any set A $\quad \mathrm{Id}_A : A \preccurlyeq A$
  (Id_A is the identity function on A)

Examples

- For any set A $\quad \mathrm{Id}_A : A \preccurlyeq A$
  (Id_A is the identity function on A)

- For a seated class, the mapping from students to chairs they occupy
  is an embedding from the set of students to the set of chairs.i

Examples

- For any set A $\quad \mathrm{Id}_A : A \preccurlyeq A$
  (Id_A is the identity function on A)
- For a seated class, the mapping from students to chairs they occupy
  is an embedding from the set of students to the set of chairs.i
- $\mathrm{Id}_{Even} : \textit{Even} \preccurlyeq \mathbb{N}$

Examples

- For any set A $\quad \mathrm{Id}_A : A \preccurlyeq A$
  (Id_A is the identity function on A)
- For a seated class, the mapping from students to chairs they occupy
  is an embedding from the set of students to the set of chairs.i
- $\mathrm{Id}_{\mathit{Even}} : \textit{Even} \preccurlyeq \mathbb{N}$
- The injection $x \mapsto 2x$ embeds $\mathbb{N}$ in ***Even***.

Examples

- For any set A $\quad \mathrm{Id}_A : A \preccurlyeq A$
  (Id_A is the identity function on A)
- For a seated class, the mapping from students to chairs they occupy is an embedding from the set of students to the set of chairs.i
- $\mathrm{Id}_{\textit{Even}} : \textit{Even} \preccurlyeq \mathbb{N}$
- The injection $x \mapsto 2x$ embeds $\mathbb{N}$ in ***Even***.
- $x \mapsto x/1000$ is an embedding of $(0..1000]$ in $(0..1]$.

Examples

- For any set A $\quad \mathrm{Id}_A : A \preccurlyeq A$
  (Id_A is the identity function on A)
- For a seated class, the mapping from students to chairs they occupy
  is an embedding from the set of students to the set of chairs.i
- $\mathrm{Id}_{\textit{Even}} : \textit{\textbf{Even}} \preccurlyeq \mathbb{N}$
- The injection $x \mapsto 2x$ embeds $\mathbb{N}$ in ***Even***.
- $x \mapsto x/1000$ is an embedding of $(0..1000]$ in $(0..1]$.
- $[1..\infty) \preccurlyeq (0..1]$ by the embedding $x \mapsto 1/x$.

Examples

Over the set $\mathbb{R}$ of real numbers:

- Stretch: For $a, b > 0$ we have $(0\,..\,a) \preccurlyeq (0\,..\,b)$ by the injection $x \mapsto bx/a$.

Examples

Over the set $\mathbb{R}$ of real numbers:

- Stretch: For $a, b > 0$ we have $(0 \mathinner{..} a) \preccurlyeq (0 \mathinner{..} b)$ by the injection $x \mapsto bx/a$.
- Displacement: $(a \mathinner{..} b) \preccurlyeq (a{+}d \mathinner{..} b{+}d)$ by the injection $x \mapsto x + d$

Examples

Over the set $\mathbb{R}$ of real numbers:

- Stretch: For $a, b > 0$ we have $(0 \mathinner{..} a) \preccurlyeq (0 \mathinner{..} b)$ by the injection $x \mapsto bx/a$.
- Displacement: $(a \mathinner{..} b) \preccurlyeq (a{+}d \mathinner{..} b{+}d)$ by the injection $x \mapsto x + d$

Examples

Over the set $\mathbb{R}$ of real numbers:

- Stretch: For $a, b > 0$ we have $(0 \mathinner{..} a) \preccurlyeq (0 \mathinner{..} b)$ by the injection $x \mapsto bx/a$.
- Displacement: $(a \mathinner{..} b) \preccurlyeq (a{+}d \mathinner{..} b{+}d)$ by the injection $x \mapsto x + d$

Using transitivity of $\preccurlyeq$

- For $a < b,\ c < d \quad (a\,..\,b) \preccurlyeq (c..d)$:

$$\begin{aligned}(a\,..\,b) &\preccurlyeq (0\,..\,b-a) && \text{(displace by } -a\text{)}\\ &\preccurlyeq (0..d-c && \text{(stretch)}\\ &\preccurlyeq (c..d) && \text{(displace)}\end{aligned}$$

Using transitivity of $\preccurlyeq$

- For $a < b,\ c < d \quad (a\,..\,b) \preccurlyeq (c..d)$:

$$\begin{aligned} (a\,..\,b) &\preccurlyeq (0\,..\,b{-}a) && \text{(displace by } -a\text{)} \\ &\preccurlyeq (0..d{-}c && \text{(stretch)} \\ &\preccurlyeq (c..d) && \text{(displace)} \end{aligned}$$

- **Do we have** $[0..1] \preccurlyeq (0..1)$ **?**

Using transitivity of $\preccurlyeq$

- For $a < b, c < d \quad (a \,..\, b) \preccurlyeq (c..d)$:

$$
\begin{aligned}
(a \,..\, b) &\preccurlyeq (0 \,..\, b{-}a) && \text{(displace by } -a\text{)}\\
&\preccurlyeq (0..d{-}c && \text{(stretch)}\\
&\preccurlyeq (c..d) && \text{(displace)}
\end{aligned}
$$

- **Do we have** $[0..1] \preccurlyeq (0..1)$ **?**

- $(1..2) \preccurlyeq [1..2] \preccurlyeq (0..3)$ (by identities)
  $\preccurlyeq (1..2)$ (Stretch)

Equipollence

- Recall that A is $\boxed{\textit{equipollent}}$ with B when there is a bijection $j : A \cong B$.
  - Example: $\mathbb{N}$ is equipollent to the set E of even naturals since $x \mapsto 2x$ is a bijection.

Equipollence

- Recall that A is $\boxed{\textit{equipollent}}$ with B when there is a bijection $j : A \cong B$.
  - Example: $\mathbb{N}$ is equipollent to the set E of even naturals since $x \mapsto 2x$ is a bijection.
- If $j : A \cong B$ then $A \preccurlyeq B$ since j is an injection, and $B \preccurlyeq A$ since j^{-1} is an injection.

Equipollence

- Recall that A is $\boxed{\textit{equipollent}}$ with B when there is a bijection $j : A \cong B$.
  - Example: $\mathbb{N}$ is equipollent to the set E of even naturals since $x \mapsto 2x$ is a bijection.
- If $j : A \cong B$ then $A \preccurlyeq B$ since j is an injection, and $B \preccurlyeq A$ since j^{-1} is an injection.
- Surprisingly, the converse also holds:

  Cantor-Bernstein-Schröder Theorem. (1896/97)
  If $A \preccurlyeq B$ and $B \preccurlyeq A$ then $A \cong B$.

Using CBS

1. The CBS Theorem is useful in proving set equipollence,
   because mutual embeddings are often easier to find than a bijection.

2. We showed that all real number intervals are embedable in each other.
   So by CBS they are all equipollent to each other.

   Not a big deal, you say, because the embedding are in fact bijections.

   Not so fast...

Using CBS

1. The CBS Theorem is useful in proving set equipollence,
   because mutual embeddings are often easier to find than a bijection.
2. We showed that all real number intervals are embedable in each other.
   So by CBS they are all equipollent to each other.

   Not a big deal, you say, because the embedding are in fact bijections.

   Not so fast...
3. $\{0,1\}^* \cong \mathbb{N}$:
   - $f : \{0,1\}^* \preccurlyeq \mathbb{N}$
     where $f(w)$ is the numeric value of $\mathbf{1}w$.

Using CBS

1. The CBS Theorem is useful in proving set equipollence,
   because mutual embeddings are often easier to find than a bijection.

2. We showed that all real number intervals are embedable in each other.
   So by CBS they are all equipollent to each other.
   Not a big deal, you say, because the embedding are in fact bijections.
   Not so fast...

3. $\{0,1\}^* \cong \mathbb{N}$:
   - $f : \{0,1\}^* \preccurlyeq \mathbb{N}$
     where $f(w)$ is the numeric value of $\mathbf{1}w$.
   - $g : \mathbb{N} \preccurlyeq \{0,1\}^*$
     where g is the injection $n \mapsto$ binary numeral for n.

Countable sets

- A set A is $\boxed{\textit{denumerable}}$ if $A \cong \mathbb{N}$.
- A is $\boxed{\textit{countable}}$ if $A \preccurlyeq \mathbb{N}$.

Countable sets

- A set A is $\boxed{\textbf{\textit{denumerable}}}$ if $A \cong \mathbb{N}$.
- A is $\boxed{\textbf{\textit{countable}}}$ if $A \preccurlyeq \mathbb{N}$.
- So A is countable iff it is either finite or denumerable.

Examples of denumerable sets.

1. The set $\mathbb{Z}$ of integers:

   $\mathbb{Z} \cong \mathbb{N}$ by the bijection

   $x \mapsto$ if $x \geqslant 0$ then $2x$ else $-2x - 1$.

   I.e. $\mathbb{Z}$ is listed as $0, -1, 1, -2, 2, -3, \ldots$.

Examples of denumerable sets.

1. The set $\mathbb{Z}$ of integers:

   $\mathbb{Z} \cong \mathbb{N}$ by the bijection

   $x \mapsto$ if $x \geqslant 0$ then $2x$ else $-2x - 1$.

   I.e. $\mathbb{Z}$ is listed as $0, -1, 1, -2, 2, -3, \ldots$.

2. $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$.

Examples of denumerable sets.

1. The set $\mathbb{Z}$ of integers:

   $\mathbb{Z} \cong \mathbb{N}$ by the bijection

   $x \mapsto$ if $x \geqslant 0$ then $2x$ else $-2x-1$.

   I.e. $\mathbb{Z}$ is listed as $0, -1, 1, -2, 2, -3, \ldots$.

2. $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$.

   - $\mathbb{N} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection $n \mapsto \langle 0, n \rangle$

Examples of denumerable sets.

1. The set $\mathbb{Z}$ of integers:

   $\mathbb{Z} \cong \mathbb{N}$ by the bijection

   $x \mapsto$ if $x \geqslant 0$ then $2x$ else $-2x - 1$.

   I.e. $\mathbb{Z}$ is listed as $0, -1, 1, -2, 2, -3, \ldots$.

2. $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$.

   - $\mathbb{N} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection $n \mapsto \langle 0, n \rangle$
   - $\mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$ by the injection $\langle p, q \rangle \mapsto 2^p \cdot 3^q$

Examples of denumerable sets.

1. The set $\mathbb{Z}$ of integers:
   $\mathbb{Z} \cong \mathbb{N}$ by the bijection
   $x \mapsto$ if $x \geqslant 0$ then $2x$ else $-2x-1$.
   I.e. $\mathbb{Z}$ is listed as $0, -1, 1, -2, 2, -3, \ldots$.

2. $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$.
   - $\mathbb{N} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection $n \mapsto \langle 0, n \rangle$
   - $\mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$ by the injection $\langle p, q \rangle \mapsto 2^p \cdot 3^q$
   - So $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$ by CBS.

1. $\mathbb{Q}^+$ is the set of positive rational numbers.

1. $\mathbb{Q}^+$ is the set of positive rational numbers.

   - $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ by the identity function on $\mathbb{N}$.

1. $\mathbb{Q}^+$ is the set of positive rational numbers.

   - $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ by the identity function on $\mathbb{N}$.
   - $\mathbb{Q} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection
     that maps $x \in \mathbb{Q}^+$ to the pair $\langle p, q\rangle$ where $x = \frac{p}{q}$ p, q are relatively prime.
     (Example: 0.75 is mapped to $\langle 3, 4\rangle$.)

1. $\mathbb{Q}^+$ is the set of positive rational numbers.

- $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ by the identity function on $\mathbb{N}$.
- $\mathbb{Q} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection that maps $x \in \mathbb{Q}^+$ to the pair $\langle p, q \rangle$ where $x = \frac{p}{q}$ p, q are relatively prime.
(Example: 0.75 is mapped to $\langle 3, 4 \rangle$.)
- But we already know that $\mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$, so $\mathbb{Q} \preccurlyeq \mathbb{N}$.

1. $\mathbb{Q}^+$ is the set of positive rational numbers.

- $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ by the identity function on $\mathbb{N}$.
- $\mathbb{Q} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection that maps $x \in \mathbb{Q}^+$ to the pair $\langle p, q \rangle$ where $x = \frac{p}{q}$ p, q are relatively prime.
(Example: 0.75 is mapped to $\langle 3, 4 \rangle$.)
- But we already know that $\mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$, so $\mathbb{Q} \preccurlyeq \mathbb{N}$.
- Since $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ and $\mathbb{Q}^+ \preccurlyeq \mathbb{N}$ it follows by CBS that $\mathbb{Q}^+ \cong \mathbb{N}$.

1. $\mathbb{Q}^+$ is the set of positive rational numbers.

   - $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ by the identity function on $\mathbb{N}$.
   - $\mathbb{Q} \preccurlyeq \mathbb{N} \times \mathbb{N}$ by the injection that maps $x \in \mathbb{Q}^+$ to the pair $\langle p, q \rangle$ where $x = \frac{p}{q}$ p, q are relatively prime.
     (Example: 0.75 is mapped to $\langle 3, 4 \rangle$.)
   - But we already know that $\mathbb{N} \times \mathbb{N} \preccurlyeq \mathbb{N}$, so $\mathbb{Q} \preccurlyeq \mathbb{N}$.
   - Since $\mathbb{N} \preccurlyeq \mathbb{Q}^+$ and $\mathbb{Q}^+ \preccurlyeq \mathbb{N}$ it follows by CBS that $\mathbb{Q}^+ \cong \mathbb{N}$.

2. **Seems like all infinite sets are countable. Are they?**

The size of $\mathcal{P}(A)$

- Not all infinite sets are countable!
- **Cantor's Theorem** (1891)
  For all sets A: $\boxed{\mathcal{P}(A) \not\preceq A}$.
- ***Proof.*** We show that for ever set A and function $g : A \to \mathcal{P}(A)$,
  g is not surjective.
  I.e. no way to name each $B \subseteq A$ by an element of A .

The size of $\mathcal{P}(A)$

- Not all infinite sets are countable!

- **Cantor's Theorem** (1891)
  For all sets A : $\boxed{\mathcal{P}(A) \not\preceq A}$.

- ***Proof.*** We show that for ever set A and function $g : A \to \mathcal{P}(A)$,
  g is not surjective.
  I.e. no way to name each $B \subseteq A$ by an element of A .
  - Let $D =_{\mathrm{df}} \{x \in A \mid x \notin g(x)\}$,
    i.e. $x \in D$ IFF $x \notin g(x)$.

  We show that D cannot be in the image of g .

The size of $\mathcal{P}(A)$

- Not all infinite sets are countable!
- **Cantor's Theorem** (1891)
  For all sets A: $\boxed{\mathcal{P}(A) \not\preceq A}$.
- ***Proof.*** We show that for ever set A and function $g : A \to \mathcal{P}(A)$,
  g is not surjective.
  I.e. no way to name each $B \subseteq A$ by an element of A .
  - Let $D =_{\text{df}} \{x \in A \mid x \notin g(x)\}$,
    i.e. $x \in D$ IFF $x \notin g(x)$.

  We show that D cannot be in the image of g .
  - If we had $D = g(d)$ for some $d \in A$
    then taking d for x above, we'd get
    $d \in D$ IFF $d \notin g(d) = D$, a contradiction. QED.

The size of $\mathcal{P}(A)$

- Not all infinite sets are countable!

- **Cantor's Theorem** (1891)
  For all sets A: $\boxed{\mathcal{P}(A) \not\preceq A}$.

- ***Proof.*** We show that for ever set A and function $g : A \to \mathcal{P}(A)$,
  g is not surjective.
  I.e. no way to name each $B \subseteq A$ by an element of A .

  - Let $D =_{\text{df}} \{x \in A \mid x \notin g(x)\}$,
    i.e. $x \in D$ IFF $x \notin g(x)$.

  We show that D cannot be in the image of g .

  - If we had $D = g(d)$ for some $d \in A$
    then taking d for x above, we'd get
    $d \in D$ IFF $d \notin g(d) = D$, a contradiction. QED.

  – In particular, $\mathcal{P}(\mathbb{N}) \not\cong \mathbb{N}$, that is: $\mathcal{P}(\mathbb{N})$ is not countable!

Comments on Cantor's Theorem

- Of course, $f: A \preccurlyeq \mathcal{P}(A)$
  where f is the embedding
- Compare:
  For all A we have $A \prec \mathcal{P}(A)$ (strict size-increase)
  For all n we have $n \ll 2^n$ (big jump)

Comments on Cantor's Theorem

- Of course, $f: A \preccurlyeq \mathcal{P}(A)$
  where f is the embedding $x \mapsto \{x\}$
- Compare:
  For all A we have $A \prec \mathcal{P}(A)$ (strict size-increase)
  For all n we have $n \ll 2^n$ (big jump)

Comments on Cantor's Theorem

- Of course, $f: A \preccurlyeq \mathcal{P}(A)$
  where f is the embedding $x \mapsto \{x\}$
- Compare:
  For all A we have $A \prec \mathcal{P}(A)$ (strict size-increase)
  For all n we have $n \ll 2^n$ (big jump)
- The set $\mathcal{P}^{fin}(\mathbb{N})$ of ***finite*** subsets of $\mathbb{N}$ is $\preccurlyeq \{0,1\}^*$
  by our familiar embedding, e.g. $\{0,2,3\} \mapsto$ **1011**.

But $\{0,1\}^* \preccurlyeq \mathbb{N}$ so $\mathcal{P}^{fin}(\mathbb{N}) \preccurlyeq \mathbb{N}$ by CBS.

⋆ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

⋆ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

- $\mathbb{R} \cong (0..1)$, so enough to show $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$.

$\star$ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

- $\mathbb{R} \cong (0..1)$, so enough to show $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$.

  $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$:

  - Given $a \in (0..1)$ write a as an ***infinite*** binary fraction $0.d_0 d_1 d_2 \ldots$.
    For example, $1/4 = 0.01 = 0.001111\ldots$.
    Such an expansion is unique to a.

⋆ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

- $\mathbb{R} \cong (0..1)$, so enough to show $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$.

  $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$:

  - Given $a \in (0..1)$ write a as an ***infinite*** binary fraction $0.d_0 d_1 d_2 \ldots$.
    For example, $1/4 = 0.01 = 0.001111\ldots$.
    Such an expansion is unique to a.
  - Map the binary expansion to the set $\{n \mid d_n = 1\}$.

  For example $1/4$ is mapped to the set $\{2, 3, 4, \ldots\}$.

⋆ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

- $\mathbb{R} \cong (0..1)$, so enough to show $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$.

  $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$:

  - Given $a \in (0..1)$ write a as an ***infinite*** binary fraction $0.d_0 d_1 d_2 \ldots$.
    For example, $1/4 = 0.01 = 0.001111...$.
    Such an expansion is unique to a.
  - Map the binary expansion to the set $\{n \mid d_n = 1\}$.

  For example $1/4$ is mapped to the set $\{2, 3, 4, \ldots\}$.

- $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$:

  - Map $A \subseteq \mathbb{N}$ to the real number with ***decimal*** expansion
    $0.d_0 d_1 d_2 \ldots$ where $d_i = 0$ if $d_i \in A$ and $= 0$ otherwise.

  That real number is unique to A.

⋆ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

- $\mathbb{R} \cong (0..1)$, so enough to show $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$.

  $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$:

  - Given $a \in (0..1)$ write a as an ***infinite*** binary fraction $0.d_0 d_1 d_2 \ldots$.
    For example, $1/4 = 0.01 = 0.001111...$.
    Such an expansion is unique to a.
  - Map the binary expansion to the set $\{n \mid d_n = 1\}$.

  For example $1/4$ is mapped to the set $\{2, 3, 4, \ldots\}$.

- $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$:

  - Map $A \subseteq \mathbb{N}$ to the real number with ***decimal*** expansion
    $0.d_0 d_1 d_2 \ldots$ where $d_i = 0$ if $d_i \in A$ and $= 0$ otherwise.

  That real number is unique to A.

  - For example, the set ***Even*** is mapped
    to the real number $0.101010\cdots$ (in decimal).

⋆ $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$

- $\mathbb{R} \cong (0..1)$, so enough to show $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$.

  $(0..1) \preccurlyeq \mathcal{P}(\mathbb{N})$:

  - Given $a \in (0..1)$ write a as an ***infinite*** binary fraction $0.d_0d_1d_2\ldots$.
    For example, $1/4 = 0.01 = 0.001111...$.
    Such an expansion is unique to a.
  - Map the binary expansion to the set $\{n \mid d_n = 1\}$.

  For example $1/4$ is mapped to the set $\{2, 3, 4, \ldots\}$.

- $\mathcal{P}(\mathbb{N}) \preccurlyeq (0..1)$:

  - Map $A \subseteq \mathbb{N}$ to the real number with ***decimal*** expansion
    $0.d_0d_1d_2\ldots$ where $d_i = 0$ if $d_i \in A$ and $= 0$ otherwise.

  That real number is unique to A.

  - For example, the set ***Even*** is mapped
    to the real number $0.101010\cdots$ (in decimal).

- By CBS conclude $\mathbb{R} \cong (0..1) \cong \mathcal{P}(\mathbb{N})$.

⋆ ***Proof of CBS***

- Given injections $f : A \to B$ and $g : B \to A$
  we construct a bijection $j : A \cong B$.

⋆ *Proof of CBS*

- Given injections $f : A \to B$ and $g : B \to A$
  we construct a bijection $j : A \cong B$.
- For $a \in A$ there is a chain

$$a \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} b_2 \xrightarrow{g} a_2 \xrightarrow{f} b_3 \cdots$$

⋆ *Proof of CBS*

- Given injections $f : A \to B$ and $g : B \to A$
  we construct a bijection $j : A \cong B$.
- We might also go backwards:

$$\cdots a_{-2} \xrightarrow{f} b_{-2} \xrightarrow{g} a_{-1} \xrightarrow{f} b_{-1} \xrightarrow{g} a \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} b_2 \xrightarrow{g} a_2 \xrightarrow{f} b_3 \cdots$$

⋆ *Proof of CBS*

- Given injections $f : A \to B$ and $g : B \to A$
  we construct a bijection $j : A \cong B$.

- We might also go backwards:
  $\cdots a_{-2} \xrightarrow{f} b_{-2} \xrightarrow{g} a_{-1} \xrightarrow{f} b_{-1} \xrightarrow{g} a \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} b_2 \xrightarrow{g} a_2 \xrightarrow{f} b_3 \cdots$

- Similarly, each $b \in B$ starts a chain $b \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} a_2 \xrightarrow{f} b_2 \xrightarrow{g} a_3 \cdots$,
  which might be extended also to the left.

$\star$ *Proof of CBS*

- Given injections $f: A \to B$ and $g: B \to A$
  we construct a bijection $j: A \cong B$.

- We might also go backwards:
  $\cdots a_{-2} \xrightarrow{f} b_{-2} \xrightarrow{g} a_{-1} \xrightarrow{f} b_{-1} \xrightarrow{g} a \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} b_2 \xrightarrow{g} a_2 \xrightarrow{f} b_3 \cdots$

- Similarly, each $b \in B$ starts a chain $b \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} a_2 \xrightarrow{f} b_2 \xrightarrow{g} a_3 \cdots$,
  which might be extended also to the left.

- Every $x \in A \cup B$ is in some chain.
  Repetitions, e.g. $a \xrightarrow{f} b \xrightarrow{g} a \xrightarrow{f} b \quad \cdots$ are harmless.

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$, and f_c, g_c be the restrictions of f, g to C.

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.
- If C is infinite to the left, or starts with $a \in A$ then
  $f_c : A_c \cong B_c$:

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.

- If C is infinite to the left, or starts with $a \in A$ then

  $f_c : A_c \cong B_c$:

  The chain above

$$a_{-2} \xrightarrow{f} b_{-2} \xrightarrow{g} a_{-1} \xrightarrow{f} b_{-1} \xrightarrow{g} a \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} b_2 \xrightarrow{g} a_2 \xrightarrow{f} b_3 \cdots$$

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.

- If C is infinite to the left, or starts with $a \in A$ then
  $f_c : A_c \cong B_c$:

  The chain above yields $f_c : A_c \cong B_c$:

$$a_{-2} \xrightarrow{f} b_{-2} \qquad a_{-1} \xrightarrow{f} b_{-1} \qquad a \xrightarrow{f} b_1 \qquad a_1 \xrightarrow{f} b_2 \qquad a_2 \xrightarrow{f} b_3 \cdots$$

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.

- If C is infinite to the left, or starts with $a \in A$ then
  $f_c : A_c \cong B_c$:

  The chain above yields $f_c : A_c \cong B_c$:

$$a_{-2} \xrightarrow{f} b_{-2} \qquad a_{-1} \xrightarrow{f} b_{-1} \qquad a \xrightarrow{f} b_1 \qquad a_1 \xrightarrow{f} b_2 \qquad a_2 \xrightarrow{f} b_3 \cdots$$

- If C starts with $b \in B$ then

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.

- If C is infinite to the left, or starts with $a \in A$ then
  $f_c : A_c \cong B_c$:

  The chain above yields $f_c : A_c \cong B_c$:

  $$a_{-2} \xrightarrow{f} b_{-2} \qquad a_{-1} \xrightarrow{f} b_{-1} \qquad a \xrightarrow{f} b_1 \qquad a_1 \xrightarrow{f} b_2 \qquad a_2 \xrightarrow{f} b_3 \cdots$$

- If C starts with $b \in B$ then

  the chain above

  $$b \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} a_2 \xrightarrow{f} b_2 \xrightarrow{g} a_3 \cdots$$

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.
- If C is infinite to the left, or starts with $a \in A$ then
  $f_c : A_c \cong B_c$:

  The chain above yields $f_c : A_c \cong B_c$:

  $a_{-2} \xrightarrow{f} b_{-2} \qquad a_{-1} \xrightarrow{f} b_{-1} \qquad a \xrightarrow{f} b_1 \qquad a_1 \xrightarrow{f} b_2 \qquad a_2 \xrightarrow{f} b_3 \cdots$

- If C starts with $b \in B$ then

  the chain above yields $g_c : B_c \cong A_c$:

  $b \xrightarrow{g} a_1 \qquad b_1 \xrightarrow{g} a_2 \qquad b_2 \xrightarrow{g} a_3 \cdots$

  and so $(g_c)^{-1} : A_c \cong B_c$

⋆ *A bijection within each chain*

- For a chain C let $A_c = A \cap C$, $B_c = B \cap C$,
  and f_c, g_c be the restrictions of f, g to C.

- If C is infinite to the left, or starts with $a \in A$ then
  $f_c : A_c \cong B_c$:

  The chain above yields $f_c : A_c \cong B_c$:

  $$a_{-2} \xrightarrow{f} b_{-2} \qquad a_{-1} \xrightarrow{f} b_{-1} \qquad a \xrightarrow{f} b_1 \qquad a_1 \xrightarrow{f} b_2 \qquad a_2 \xrightarrow{f} b_3 \cdots$$

- If C starts with $b \in B$ then

  the chain above yields $g_c : B_c \cong A_c$:

  $$b \xrightarrow{g} a_1 \qquad b_1 \xrightarrow{g} a_2 \qquad b_2 \xrightarrow{g} a_3 \cdots$$

  and so $(g_c)^{-1} : A_c \cong B_c$

- The union (over all chains) of these bijections is a bijection from A to B.
  QED.