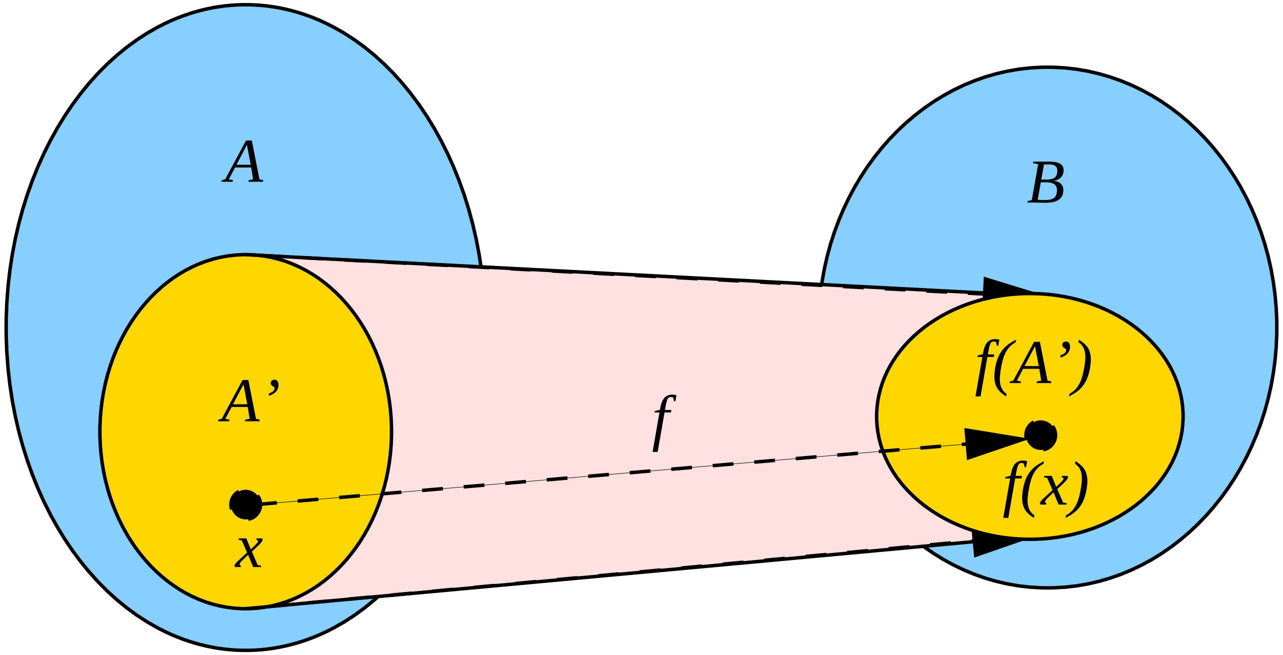
More on Functions

Wolfgang Schreiner
Research Institute for Symbolic Computation (RISC-Linz)
Johannes Kepler University, Linz, Austria

Wolfgang.Schreiner@risc.uni-linz.ac.at
http://www.risc.uni-linz.ac.at/people/schreine

Further Notions

Image and Inverse Image



$$f^{-1}(f(A')) = A'$$

Image and Inverse Image

Definition: Let $f : A \to B$, $A' \subseteq A$. The image of A' at f is the set of all values to which elements of A' are mapped by f:

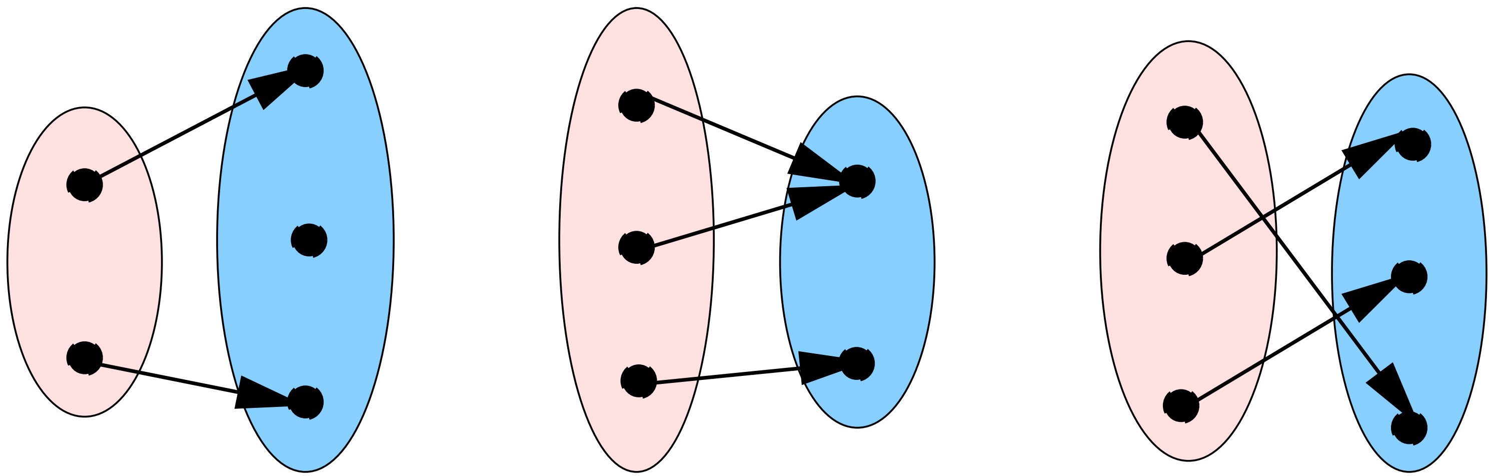
$$f(A') := \textbf{if } A' \subseteq \mathrm{domain}(f) \textbf{ then } \{f(x) : x \in A'\}.$$

The inverse image of B' at f is the set of all elements that are mapped to some elements of B' by f:

$$f^{-1}(B') := \{x \in \mathrm{domain}(f) : f(x) \in B'\}.$$

Function applied to set of arguments.

Function Properties



injective
(not surjective)

surjective
(not injective)

bijective

Function Properties

Definition: Let $f\colon A \to B$. f is injective (one-to-one) if it does not map different arguments to the same result:

$$f : A \overset{\text{injective}}{\longrightarrow} B :\Leftrightarrow$$
$$f : A \to B \land (\forall x_0 \in A, x_1 \in A : f(x_0) = f(x_1) \Rightarrow x_0 = x_1).$$

f is surjective (onto) if every element of B is hit by some argument:

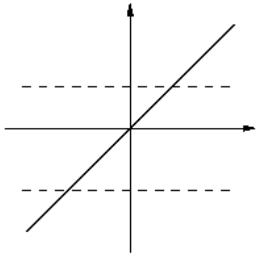
$$f : A \overset{\text{surjective}}{\longrightarrow} B :\Leftrightarrow$$
$$f : A \to B \land (\forall y \in B : \exists x \in A : f(x) = y).$$

f is bijective if it is injective and surjective:

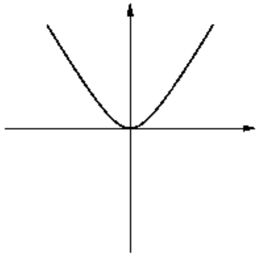
$$f : A \overset{\text{bijective}}{\longrightarrow} B :\Leftrightarrow f : A \overset{\text{injective}}{\longrightarrow} B \land f : A \overset{\text{surjective}}{\longrightarrow} B.$$

Example

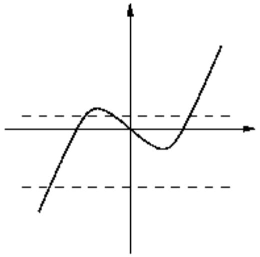
- The identity function $f(x) := x$ is bijective:



- The square function $f(x) := x^2$ is neither injective nor surjective:



- The function $f(x) := x^3 - x$ is surjective but not injective:



Function Composition and Inversion

Proposition: The composition of two bijective functions is bijective:

$$\forall A, B, C, f : A \xrightarrow{\text{bijective}} B, g : B \xrightarrow{\text{bijective}} C :$$
$$f \circ g : A \xrightarrow{\text{bijective}} C.$$

Proposition: If a function is injective, its inverse is also a function:

$$\forall A, B, f : A \xrightarrow{\text{injective}} B : f^{-1} \text{ is a function.}$$

If a function is bijective, its inverse is also bijective:

$$\forall A, B, f : A \xrightarrow{\text{bijective}} B : f^{-1} : B \xrightarrow{\text{bijective}} A.$$

Proofs: see lecture notes (later).

Inverse Function Properties

$$1_A : A \to A, 1_A(x) := x$$

Proposition: For every $A, B, f : A \to B$, we have

$$\begin{aligned} f \circ 1_B &= f \\ 1_A \circ f &= f. \end{aligned}$$

If f is injective, then we have

$$f \circ f^{-1} = 1_A$$

If f is also surjective (i.e., bijective), then we have

$$f^{-1} \circ f = 1_B.$$

Permutations

Permutations

Definition: A permutation of length n is a bijection from $\mathbb{N}_n$ to $\mathbb{N}_n$:

$$p \text{ is permutation of length } n :\Leftrightarrow p : \mathbb{N}_n \xrightarrow{\text{bijective}} \mathbb{N}_n.$$

Example: Take the sequence $s = [a, b, c, d, e]$ and the permutation $p = [1, 0, 4, 3, 2]$. Then we have

$$p \circ s = [b, a, e, d, c].$$

Proposition: The number of permutations of length n is $n!$.

$$\forall n \in \mathbb{N} : |\{f : f \text{ is permutation of length } n\}| = n!.$$

Example: Sorting Problem

- **Input**:
  - $n \in \mathbb{N}$ . . . the length of the sequence,
  - $s : \mathbb{N}_n \to \mathbb{R}$ . . . a sequence of length n on $\mathbb{R}$.
- **Output**: $t : \mathbb{N}_n \to \mathbb{R}$ such that
  - t is permutation of s,
  - t is sorted with respect to $\leq$.

$$
\begin{array}{l}
t \text{ is permutation of } s :\Leftrightarrow \\
\quad \textbf{let } n = \text{length}(t) : \\
\qquad n = \text{length}(s) \land \\
\qquad \exists p : p \text{ is permutation of length } n \land p \circ s = t;
\end{array}
$$

$$
\begin{array}{l}
t \text{ is sorted with respect to } \leq :\Leftrightarrow \\
\quad \forall 0 \leq i < \text{length}(t) - 1 : t_i \leq t_{i+1}.
\end{array}
$$

Further Results

- The composition of two permutations is also a permutation:

$$\begin{aligned}&\forall n \in \mathbb{N}, p_0, p_1 :\\&\quad (p_0 \text{ is permutation of length } n \wedge\\&\quad p_1 \text{ is permutation of length } n) \;\Rightarrow\\&\qquad p_0 \circ p_1 \text{ is permutation of length } n.\end{aligned}$$

- The inverse of a permutation is a permutation of the same length:

$$\begin{aligned}&\forall n \in \mathbb{N}, p :\\&\quad p \text{ is permutation of length } n \Rightarrow\\&\qquad p^{-1} \text{ is permutation of length } n.\end{aligned}$$

The set of permutations is closed under function composition.

Example

Take the permutations $p = [1, 0, 4, 3, 2]$ and $q = [2, 1, 3, 4, 0]$. Then

$$r := p \circ q = [1, 2, 0, 4, 3],$$

e.g., $r(2) = (p \circ q)(2) = q(p(2)) = q(4) = 0$. We also have

$$r^{-1} = [2, 0, 1, 4, 3]$$

e.g., $r^{-1}(2) = 1$ because $r(1) = 2$, and thus

$$r \circ r^{-1} = r^{-1} \circ r = [0, 1, 2, 3, 4].$$

Counting Set Elements

Number of Set Elements

Definition: A set S is finite if it is empty or there is a bijection to $\mathbb{N}_n$ for some $n > 0$. We then call 0 resp. n the size or cardinality of S:

$$S \text{ is finite} :\Leftrightarrow S = \emptyset \vee (\exists n \in \mathbb{N}_{>0}, f : f : \mathbb{N}_n \xrightarrow{\text{bijective}} S);$$

$$|S| := \textbf{if } S = \emptyset \textbf{ then } 0 \textbf{ else } (\textbf{such } n \in \mathbb{N}_{>0} : \exists f : f : \mathbb{N}_n \xrightarrow{\text{bijective}} S).$$

A set is infinite if is not finite:

$$S \text{ is infinite } :\Leftrightarrow \neg S \text{ is finite.}$$

Example

- The set $S := \{0, 2, 4\}$ is finite; its size is 3 because we can define a function $f : \mathbb{N}_3 \xrightarrow{\text{bijective}} S$ as

$$\begin{aligned} f(0) &:= 0 \\ f(1) &:= 2 \\ f(2) &:= 4 \end{aligned}$$

  i.e., $f = [0, 2, 4]$. The length of f is the same as the length of $[0, 4, 2]$, $[4, 2, 0]$ or of any other bijection to S.

- The set $\mathbb{N}$ is infinite. If it were finite, we had some $n \in \mathbb{N}$ and some $f : \mathbb{N}_n \xrightarrow{\text{bijective}} \mathbb{N}$. Take $k := 1 + \max\{f(i) : i \in \mathbb{N}_n\}$. Then $k \in \mathbb{N}$ but $\forall i \in \mathbb{N}_n : f(i) \neq k$, i.e., f is not surjective on $\mathbb{N}$.

Unicity of Bijection

Proposition: If S is not empty and both $f : \mathbb{N}_n \rightarrow S$ and $g : \mathbb{N}_m \rightarrow S$ are bijections, then $n = m$:

$$(\forall S \neq \emptyset, n \in \mathbb{N}, m \in \mathbb{N}, f : \mathbb{N}_n \xrightarrow{\text{bijective}} S, g : \mathbb{N}_m \xrightarrow{\text{bijective}} S : m = n).$$

Proof: see lecture notes.

The size of a set is uniquely defined.

Number Quantifier

Definition: For every variable x and formula F, the phrase

$$\#x : F$$

is a term where x is bound and whose value equals

$$|\{x : F\}|.$$

The term value is only well defined if the base formula is true for a finite number of assignments for the bound variable.

Set Sizes

Proposition: If A and B are disjoint with sizes m and n, respectively, then the size of their union is $m+n$:

$$\forall A, B, m \in \mathbb{N}, n \in \mathbb{N} : \\ (A \cap B = \emptyset \land |A| = m \land |B| = n) \Rightarrow |A \cup B| = m + n.$$

The size of the Cartesian product of two sets is the product of their sizes:

$$\forall A, B, m \in \mathbb{N}, n \in \mathbb{N} : \\ (|A| = m \land |B| = n) \Rightarrow |A \times B| = m * n.$$

Set Sizes (Continued)

Proposition: If A and B have size m and n, respectively, then the size of the set of functions from A to B is n^m:

$$\begin{array}{l}\forall A, B, m \in \mathbb{N}, n \in \mathbb{N} : \\ \quad (|A| = m \wedge |B| = n) \Rightarrow |A \to B| = n^m.\end{array}$$

If A is of size n, then A has 2^n subsets:

$$\begin{array}{l}\forall A, n \in \mathbb{N} : \\ \quad |A| = n \Rightarrow |\mathbb{P}(A)| = 2^n.\end{array}$$

Countable Sets

Definition: A set is countable if it has an enumeration, i.e., a bijective mapping from $\mathbb{N}$:

$$S \text{ is countable } :\Leftrightarrow \exists f : f : \mathbb{N} \xrightarrow{\text{bijective}} S.$$

A criterium to distinguish "degrees of infinity".

Example

$\mathbb{Z}$ is infinite but it is countable because we can define

$$f : \mathbb{N} \xrightarrow{\text{bijective}} \mathbb{Z}$$
$$f(x) := \textbf{if } x \text{ is even } \textbf{then } -x/2 \textbf{ else } (x+1)/2$$

i.e.,

$$f = [0, 1, -1, 2, -2, 3, -3, \ldots].$$

While $\mathbb{Z}$ is infinite, we can enumerate all its elements.

Example

The set $\mathbb{Q}$ is infinite but countable: we can list all positive rationals in an infinite matrix that holds at position $\langle i, j \rangle$ the rational $\frac{i+1}{j+1}$:

$$\begin{array}{ccccccccc}
\frac{1}{1} & & \frac{1}{2} & & \frac{1}{3} & & \frac{1}{4} & & \dots \\
& \swarrow & & \swarrow & & \swarrow & & & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \dots & & \dots \\
& \swarrow & & \swarrow & & & & & \\
\frac{3}{1} & & \frac{3}{2} & & \dots & & \dots & & \dots \\
& \swarrow & & & & & & & \\
\frac{4}{1} & & \dots & & \dots & & \dots & & \dots \\
& & & & & & & & \\
\dots & & \dots & & \dots & & \dots & & \dots
\end{array}$$

We can enumerate all elements in this matrix in a sequence f.

Example (Continued)

From f, we remove all "doubles" constructing a sequence $f' : \mathbb{N} \to \mathbb{Q}$ that contains each positive rational number in exactly one position. Finally we can define an enumeration of all rationals

$$
\begin{array}{l}
g : \mathbb{N} \xrightarrow{\text{bijective}} \mathbb{Q} \\
g(x) := \\
\quad \textbf{if } x = 0 \textbf{ then } 0 \\
\quad \textbf{else if } x \text{ is even} \\
\quad\quad \textbf{then } -f'(x/2) \\
\quad\quad \textbf{else } f'((x-1)/2)
\end{array}
$$

$$g = [0, 1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}, \ldots].$$

Example

The set of all infinite sequences over $\{0,1\}$ is not countable.

If it were, we had an $f : \mathbb{N} \xrightarrow{\text{bijective}} (\mathbb{N} \rightarrow \{0,1\})$. Let $s : \mathbb{N} \rightarrow \{0,1\}$

$$s(i) := \overline{f(i)_i}$$

where $\overline{d} := 1 - d$. Then s differs from $f(i)$ in the i-th digit (for every $i \in \mathbb{N}$), thus s is not contained in f.

$$\begin{array}{rlllll}
f(0) = & [\boldsymbol{f(0)_0} & f(0)_1 & f(0)_2 & f(0)_3 & \ldots] \\
f(1) = & [f(1)_0 & \boldsymbol{f(1)_1} & f(1)_2 & f(1)_3 & \ldots] \\
f(2) = & [f(2)_0 & f(2)_1 & \boldsymbol{f(2)_2} & f(2)_3 & \ldots] \\
f(3) = & [f(3)_0 & f(3)_1 & f(3)_2 & \boldsymbol{f(3)_3} & \ldots] \\
 & \ldots & \ldots & \ldots & \ldots & \ldots \\
s := & [\overline{f(0)_0}, & \overline{f(1)_1} & \overline{f(2)_2} & \overline{f(3)_3}, & \ldots]
\end{array}$$

Example

The set $\mathbb{R}$ is not countable.
Every infinite sequence d of decimal digits represents a real number

$$0.d_0 d_1 d_2 \ldots.$$

Since the set of all infinite sequences is not countable (and every real number is represented by a countable set of such sequences), also $\mathbb{R}$ is not countable.

Not all number domains are countable.

Set Cardinalities

Proposition: Two sets have same size, if there is a bijection between:

$$A \text{ and } B \text{ are of same size } :\Leftrightarrow \exists f : f : A \xrightarrow{\text{bijective}} B.$$

One set is not larger than another set, if there exists an injection from the first set into the second set:

$$A \text{ is not larger than } B :\Leftrightarrow \exists f : f : A \xrightarrow{\text{injective}} B.$$

One set is smaller than another set, if they are not of same size and the second one is not larger than the first one.

$$A \text{ is smaller than } B :\Leftrightarrow$$
$$(A \text{ is not larger than } B) \wedge \neg(A \text{ and } B \text{ have same size}).$$

Finite Sets

Proposition: For all finite sets A and B, the following holds:

$$\begin{aligned}
|A| = |B| &\Leftrightarrow A \text{ and } B \text{ have same size;}\\
|A| \leq |B| &\Leftrightarrow A \text{ is not larger than } B;\\
|A| < |B| &\Leftrightarrow A \text{ is smaller than } B.
\end{aligned}$$

For finite sets, the new notions coincide with the old ones.

Infinite Sets

We can now also compare the size of infinite sets:

- $\mathbb{N}$ has the same size as $\mathbb{Z}$.
- $\mathbb{Z}$ has the same size as $\mathbb{Q}$.
- $\mathbb{Q}$ is smaller than $\mathbb{R}$.
- $\mathbb{R}$ has the same size as $\mathbb{C}$.

The first results were just shown above.