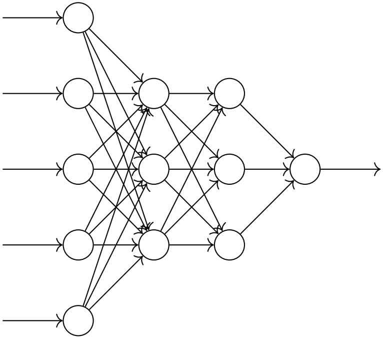
Chapter 9: Functions

CS1231S Discrete Structures

Wong Tin Lok

National University of Singapore

2021/22 Semester 1



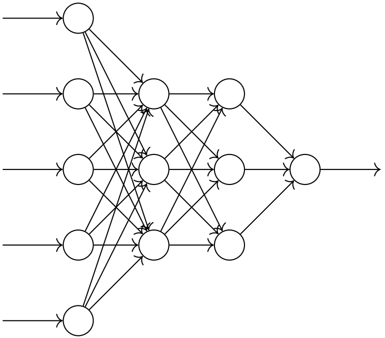
Much of the power of deep learning arises from the fact that repeated composition of multiple nonlinear functions has significant expressive power. Aggarwal 2018

Why functions?

- The language of functions is an important part of modern mathematical discourse.
- Function-like objects are interesting mathematical objects.
- For this module, they provide a topic on which we practise writing and understanding proofs.

Plan

- recapitulation
- equality of functions
- function composition
- bijections
- inverse functions



Much of the power of deep learning arises from the fact that repeated composition of multiple nonlinear functions has significant expressive power. Aggarwal 2018

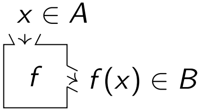
Functions on equivalence classes

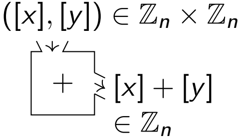
Definition 7.2.1

Let A, B be sets. A *function* or a *map* from A to B is an assignment to each element of A exactly one element of B. We write $f\colon A \to B$ for "f is a function from A to B". Suppose $f\colon A \to B$.

(1) Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to. We call $f(x)$ the *image* of x under f. If $y = f(x)$, then we say that *f maps x to y*, and we may write $f\colon x \mapsto y$.

(2) Here A is called the *domain* of f, and B is called the *codomain* of f.

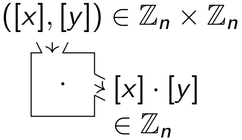




Definition 7.1.4 (rephrased)

Let $n \in \mathbb{Z}^+$. Define $+, \cdot\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ as follows: whenever $[x], [y] \in \mathbb{Z}_n$,

$$[x] + [y] = [x+y] \quad \text{and} \quad [x]\cdot[y] = [x\cdot y].$$



The Fibonacci sequence

Definition 7.2.1

Let A, B be sets. A *function* or a *map* from A to B is an assignment to each element of A exactly one element of B. We write $f \colon A \to B$ for "f is a function from A to B". Suppose $f \colon A \to B$.

(1) Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to. We call $f(x)$ the *image* of x under f. If $y = f(x)$, then we say that *f maps x to y*, and we may write $f \colon x \mapsto y$.

(2) Here A is called the *domain* of f, and B is called the *codomain* of f.

$x \in A$

$\boxed{f}$ $f(x) \in B$

$n \in \mathbb{Z}_{\geqslant 0}$

$\boxed{F}$ $F_n \in \mathbb{Z}_{\geqslant 0}$

Definition 8.2.2

The *Fibonacci sequence $F_0, F_1, F_2, \ldots$* is defined by setting, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$F_0 = 0 \quad \text{and} \quad F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n.$$

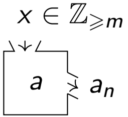
John Tenniel

Sequences

Remark 9.1.1

(1) A sequence $a_0, a_1, a_2, \dots$ can be represented by the function a whose domain is $\mathbb{Z}_{\geqslant 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.

(2) In this sense, any function whose domain is $\mathbb{Z}_{\geqslant m}$ for some $m \in \mathbb{Z}$ represents a sequence.

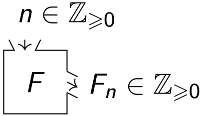


Example 9.1.2

One can represent the Fibonacci sequence $F_0, F_1, F_2, \dots$ by the unique function $F\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ that satisfies, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$F(0) = 0 \quad \text{and} \quad F(1) = 1 \quad \text{and} \quad F(n+2) = F(n+1) + F(n).$$

Such an F exists and is unique, essentially by Proposition 8.3.4.



Definition 8.2.2

The *Fibonacci sequence $F_0, F_1, F_2, \dots$* is defined by setting, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$F_0 = 0 \quad \text{and} \quad F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n.$$

John Tenniel

Strings

a_0	a_1	$\dots$	$a_{\ell-1}$

Let A be a set.

Definition 9.1.3

A *string* or a *word* over A is an expression of the form

$$a_0 a_1 \dots a_{\ell-1}$$

where $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \dots, a_{\ell-1} \in A$. Here ℓ is called the *length* of the string. Let A^* denote the set of all strings over A. The *empty string* ε is the string of length 0.

Example 9.1.4

Suppose $A = \{\mathrm{s}, \mathrm{u}\}$. The following are strings over A:

$$\mathrm{s}, \quad \mathrm{ssuu}, \quad \mathrm{susususu}, \quad \mathrm{uuuuuuu}, \quad \dots.$$

Their lengths are respectively 1, 4, 8, and 7.

Remark 9.1.5

(1) One can represent a string $a_0 a_1 \dots a_{\ell-1}$ over A by the function $a\colon \{0, 1, \dots, \ell-1\} \to A$ satisfying $a(n) = a_n$ for all $n \in \{0, 1, \dots, \ell-1\}$.

(2) Every function $a\colon \{m, m+1, \dots, m+\ell-1\} \to A$, where $m \in \mathbb{Z}$ and $\ell \in \mathbb{Z}_{\geqslant 0}$, represents a string of length ℓ over A, namely $a(m)\, a(m+1)\, \dots\, a(m+\ell-1)$.

Equality of functions

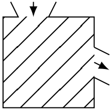
Definition 9.1.6

Two functions $f\colon A \to B$ and $g\colon C \to D$ are *equal* if

(1) $A = C$ and $B = D$; and

(2) $f(x) = g(x)$ for all $x \in A$.

In this case, we write $f = g$.



Example 9.1.7

Let $f\colon \{0,2\} \to \mathbb{Z}$ and $g\colon \{0,2\} \to \mathbb{Z}$ defined by setting, for all $x \in \{0,2\}$,

$$f(x) = 2x \quad \text{and} \quad g(x) = x^2.$$

Then $f = g$ because their domains are the same, their codomains are the same, and $f(x) = g(x)$ for every $x \in \{0,2\}$.

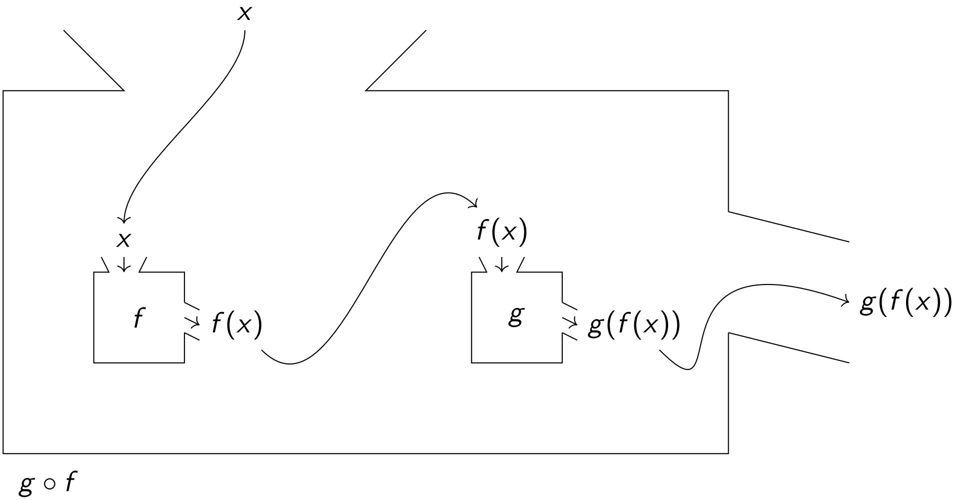
Example 9.1.8

Let $f\colon \mathbb{Z} \to \mathbb{Z}$ and $g\colon \mathbb{Z} \to \mathbb{Q}$ defined by setting, for all $x \in \mathbb{Z}$,

$$f(x) = x^3 = g(x).$$

Then $f \neq g$ because they have different codomains.

One after another



Function composition

"g composed with f" or "g circle f"

Definition 9.2.1

Let $f\colon A \to B$ and $g\colon B \to C$. Then $g \circ f\colon A \to C$ such that for every $x \in A$,

$$(g \circ f)(x) = g(f(x)).$$

$$\begin{tikzcd} & B \arrow[dr, "g"] & \\ A \arrow[ur, "f"] \arrow[rr, dashed, "g \circ f"'] & & C \end{tikzcd}$$

Note 9.2.2

For $g \circ f$ to be defined, the codomain of f must equal the domain of g.

$$\begin{aligned} \mathrm{id}_A\colon A &\to A; & \mathrm{id}_B\colon B &\to B;\\ x &\mapsto x, & y &\mapsto y. \end{aligned}$$

$$\begin{tikzcd} A \arrow[r, "\mathrm{id}_A"] \arrow[dr, dashed, "f"'] & A \arrow[d, "f"] \arrow[dr, dashed, "f"] & \\ & B \arrow[r, "\mathrm{id}_B"'] & B \end{tikzcd}$$

Example 9.2.3

Let $f\colon A \to B$.

(1) $f \circ \mathrm{id}_A = f$ because
- the domain of $f \circ \mathrm{id}_A$ and the domain of f are both A;
- the codomain of $f \circ \mathrm{id}_A$ and the codomain of f are both B;
- $(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x)$ for all $x \in A$.

(2) $\mathrm{id}_B \circ f = f$ because
- the domain of $\mathrm{id}_B \circ f$ and the domain of f are both A;
- the codomain of $\mathrm{id}_B \circ f$ and the codomain of f are both B;
- $(\mathrm{id}_B \circ f)(x) = \mathrm{id}_B(f(x)) = f(x)$ for all $x \in A$.

Idempotent functions

Question 9.2.4

Which of the following define a function $f\colon \mathbb{Z} \to \mathbb{Z}$ that satisfies $f \circ f = f$?

(1) $f(x) = 1231$ for all $x \in \mathbb{Z}$.

(2) $f(x) = x$ for all $x \in \mathbb{Z}$.

(3) $f(x) = -x$ for all $x \in \mathbb{Z}$.

(4) $f(x) = 3x + 1$ for all $x \in \mathbb{Z}$.

(5) $f(x) = x^2$ for all $x \in \mathbb{Z}$.

$$\begin{tikzcd} & \mathbb{Z} \arrow[dr, "f"] & \\ \mathbb{Z} \arrow[ur, "f"] \arrow[rr, "f"'] & & \mathbb{Z} \end{tikzcd}$$

Answer

(1) Yes, because $(f \circ f)(x) = f(f(x)) = f(1231) = 1231 = f(x)$ for all $x \in \mathbb{Z}$.

(2) Yes, because $(f \circ f)(x) = f(f(x)) = f(x)$ for all $x \in \mathbb{Z}$.

(3) No, because $(f \circ f)(1) = f(f(1)) = f(-1) = 1 \neq -1 = f(1)$.

(4) No, because $(f \circ f)(0) = f(f(0)) = f(1) = 4 \neq 1 = f(0)$.

(5) No, because $(f \circ f)(2) = f(f(2)) = f(4) = 16 \neq 4 = f(2)$.

Noncommutativity of function composition

Definition 9.2.1

Let $f\colon A \to B$ and $g\colon B \to C$. Then $g \circ f\colon A \to C$ such that for every $x \in A$,
$$(g \circ f)(x) = g(f(x)).$$

Example 9.2.5

Let $f, g\colon \mathbb{Z} \to \mathbb{Z}$ such that for every $x \in \mathbb{Z}$,
$$f(x) = 3x \quad \text{and} \quad g(x) = x + 1.$$
Then for every $x \in \mathbb{Z}$,
$$(g \circ f)(x) = g(f(x)) = g(3x) = 3x + 1 \quad \text{and}$$
$$(f \circ g)(x) = f(g(x)) = f(x + 1) = 3(x + 1).$$
Note $(g \circ f)(0) = 1 \neq 3 = (f \circ g)(0)$.

$$\begin{tikzcd}
 & x \arrow[rr, mapsto, "f"] & & 3x \arrow[dd, mapsto, "g"] \\
x \arrow[dd, mapsto, "g"'] & \mathbb{Z} \arrow[r, "f"] \arrow[d, "g"'] & \mathbb{Z} \arrow[d, "g"] & \\
 & \mathbb{Z} \arrow[r, "f"'] & \mathbb{Z} & 3x+1 \\
x+1 \arrow[rr, mapsto, "f"'] & & 3(x+1) &
\end{tikzcd}$$

Associativity of function composition

Definition 9.2.1

Let $f\colon A \to B$ and $g\colon B \to C$. Then $g \circ f\colon A \to C$ such that for every $x \in A$,

$$(g \circ f)(x) = g(f(x)).$$

Theorem 9.2.6 (associativity of function composition)

Let $f\colon A \to B$ and $g\colon B \to C$ and $h\colon C \to D$. Then

$$(h \circ g) \circ f = h \circ (g \circ f).$$

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, dashed, "g \circ f"'] & B \arrow[d, "g"] \arrow[dr, dashed, "h \circ g"] & \\
& C \arrow[r, "h"'] & D
\end{tikzcd}$$

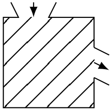
Proof

1. The domains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are both A.
2. The codomains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are both D.
3. For every $x \in A$,

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x). \qquad \square$$

Checkpoint

Sequences and strings can be represented by functions.



Definition 9.1.6
Two functions $f\colon A \to B$ and $g\colon C \to D$ are *equal* if

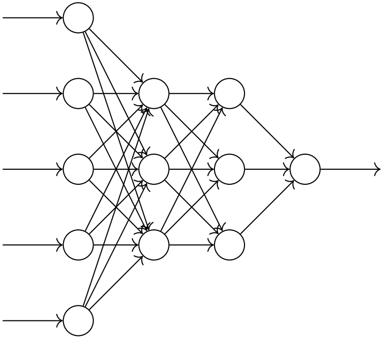
(1) $A = C$ and $B = D$; and

(2) $f(x) = g(x)$ for all $x \in A$.

In this case, we write $f = g$.

Definition 9.2.1
Let $f\colon A \to B$ and $g\colon B \to C$. Then $g \circ f\colon A \to C$ such that for every $x \in A$,

$$(g \circ f)(x) = g(f(x)).$$

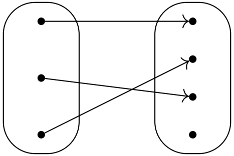


Next

- bijections
- inverse functions

Arrow diagrams

Definition 7.2.1. A *function* from A to B is an assignment to each element of A exactly one element of B.

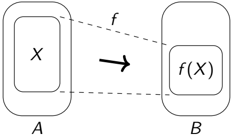


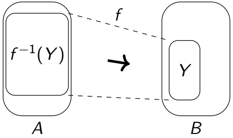
The figure above represents a function in the following sense.

- The dots on the left denote the elements of the domain.
- The dots on the right denote the elements of the codomain.
- An arrow from a left dot to a right dot indicates that the left dot is assigned the right dot.

Since every dot on the left is joined to exactly one dot on the right in the figure above, this function is well defined.

Setwise image and preimage





Definition 9.3.1

Let $f : A \to B$.

(1) If $X \subseteq A$, then let $f(X) = \{f(x) : x \in X\}$.

(2) If $Y \subseteq B$, then let $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$.

We call $f(X)$ the *image* of X, and $f^{-1}(Y)$ the *preimage* of Y under f.

Example 9.3.2

Ambiguity!

Define $g : \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$.

(1) If $X = \{-1, 0, 1\}$, then $g(X) = \{g(-1), g(0), g(1)\} = \{1, 0, 1\} = \{0, 1\}$.

(2) If $Y = \{0, 1, 2\}$, then $g^{-1}(Y) = \{0, -1, 1\}$.

Note 9.3.3

In general, we cannot make f^{-1} operate on elements instead of subsets.

Let $f : A \to B$.

(1) If $X \subseteq A$, then $f(X) = \{f(x) : x \in X\}$, which is a set. If $x \in A$, then $f(x) \in B$.

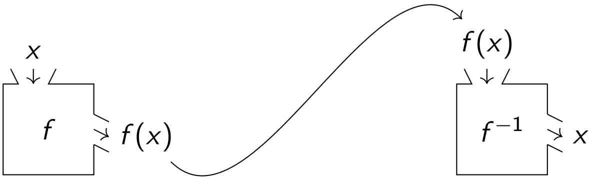
(2) If $Y \subseteq B$, then $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$, which exists even when the inverse function f^{-1} does not. If $y \in B$ and f^{-1} exists, then $f^{-1}(y) \in A$.

Zoom poll

Why inverses

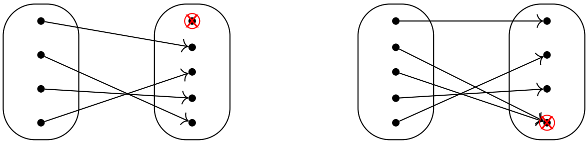
F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12

It is often useful to know when and how one can undo a function.



[T]he security of these cryptosystems rests on the assumption that inverting the underlying function (or finding the private key from the public one) is a hard problem.
Hoffstein–Pipher–Silverman 2014

Injections and surjections



Definition 7.2.1. A *function* from A to B is an assignment to each element of A exactly one element of B.

Suppose we invert the arrows in the diagrams above. Do the inverted diagrams represent functions from the right set to the left set?

- No for the left diagram, because the top dot on the right is not joined to any dot on the left.
- No for the right diagram, because the bottom dot on the right is joined to more than one dot on the left.

surjective function = *surjection*
injective function = *injection*
bijective function = *bijection*

Definition 9.3.6

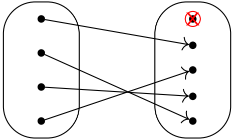
Let $f : A \to B$.

(1) f is *surjective* or *onto* if $\forall y \in B \ \exists x \in A \ (y = f(x))$.

(2) f is *injective* or *one-to-one* if $\forall x_1, x_2 \in A \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

(3) f is *bijective* if it is surjective and injective, i.e., $\forall y \in B \ \exists! x \in A \ (y = f(x))$.

Surjectivity



Definition 9.3.6(1)

A function $f\colon A \to B$ is *surjective* if $\forall y \in B\ \exists x \in A\ (y = f(x))$.

Example 9.3.7

The function $f\colon \mathbb{Q} \to \mathbb{Q}$, defined by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$, is surjective.

Proof

1. Take any $y \in \mathbb{Q}$.
2. Let $x = (y - 1)/3$.
3. Then $x \in \mathbb{Q}$ and $f(x) = 3x + 1 = y$. $\square$

Remark 9.3.8. A function $f\colon A \to B$ is *not* surjective if and only if
$$\exists y \in B\ \forall x \in A\ (y \neq f(x)).$$

Example 9.3.9

Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then g is not surjective.

Proof

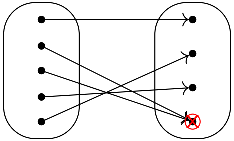
1. Note $g(x) = x^2 \geqslant 0 > -1$ for all $x \in \mathbb{Z}$.
2. So $g(x) \neq -1$ for all $x \in \mathbb{Z}$, although $-1 \in \mathbb{Z}$. $\square$

Injectivity

Definition 9.3.6(2)

A function $f\colon A \to B$ is *injective* if

$$\forall x_1, x_2 \in A \ \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$



Example 9.3.10

The function $f\colon \mathbb{Q} \to \mathbb{Q}$, defined by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$, is injective.

Proof

1. Let $x_1, x_2 \in \mathbb{Q}$ such that $f(x_1) = f(x_2)$.
2. Then $3x_1 + 1 = 3x_2 + 1$.
3. So $x_1 = x_2$. $\square$

Remark 9.3.11. A function $f\colon A \to B$ is *not* injective if and only if $\exists x_1, x_2 \in A \ \ (f(x_1) = f(x_2) \wedge x_1 \neq x_2)$.

Example 9.3.12

Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then g is not injective.

Proof

Note $g(1) = 1^2 = 1 = (-1)^2 = g(-1)$, although $1 \neq -1$. $\square$

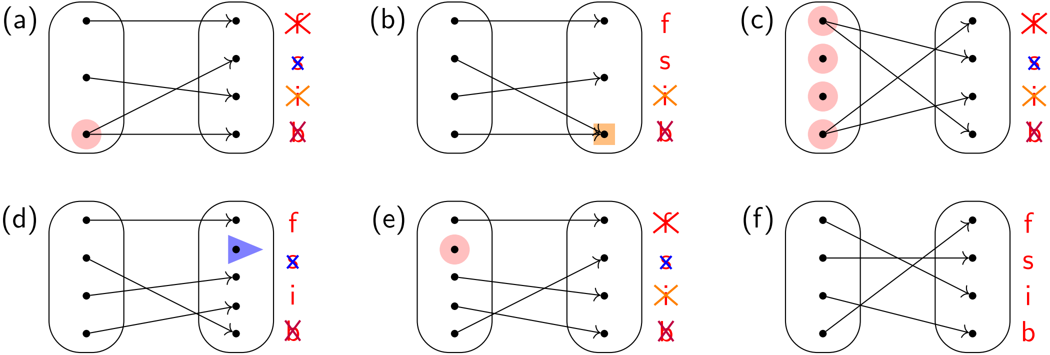
Which of the following represent functions or sur-/in-/bijections?

Definition 9.3.6. Let $f\colon A \to B$.

(1) f is *surjective* or *onto* if $\forall y \in B\ \exists x \in A\ (y = f(x))$.

(2) f is *injective* or *one-to-one* if $\forall x_1, x_2 \in A\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

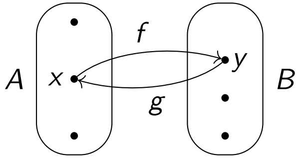
(3) f is *bijective* if it is surjective and injective, i.e., $\forall y \in B\ \exists! x \in A\ (y = f(x))$.



Zoom poll

Inverses

Definition 9.3.14



Let $f\colon A \to B$. Then $g\colon B \to A$ is an *inverse* of f if

$$\forall x \in A \ \forall y \in B \ \big(y = f(x) \quad \Leftrightarrow \quad x = g(y) \big).$$

Example 9.3.15

Define $f\colon \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Note that for all $x, y \in \mathbb{Q}$,

$$y = 3x + 1 \quad \Leftrightarrow \quad x = (y - 1)/3.$$

Let $g\colon \mathbb{Q} \to \mathbb{Q}$ such that $g(y) = (y - 1)/3$ for all $y \in \mathbb{Q}$. Then the equivalence above tells us

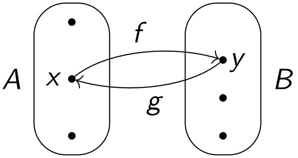
$$\forall x, y \in \mathbb{Q} \ \big(y = f(x) \quad \Leftrightarrow \quad x = g(y) \big).$$

So g is an inverse of f.

Note 9.3.16

We have no guarantee of a description of an inverse of a general function that is much different from what is given by the definitions.

Uniqueness of inverses



Definition 9.3.14

Let $f : A \to B$. Then $g : B \to A$ is an *inverse* of f if

$$\forall x \in A \ \forall y \in B \ \big(y = f(x) \quad \Leftrightarrow \quad x = g(y) \big).$$

Proposition 9.3.17 (uniqueness of inverses)

If g_1, g_2 are inverses to $f : A \to B$, then $g_1 = g_2$.

Proof

1. Note $g_1, g_2 : B \to A$.
2. Since g_1, g_2 are inverses of f, for all $x \in A$ and all $y \in B$,

$$x = g_1(y) \quad \Leftrightarrow \quad y = f(x) \quad \Leftrightarrow \quad x = g_2(y).$$

3. So $g_1 = g_2$. □

Definition 9.3.18

The inverse of a function f is denoted f^{-1}.

Bijectivity and invertibility

g is an inverse of f $\Leftrightarrow$ $g = f^{-1}$
$\Leftrightarrow$ $\forall x \in A\ \forall y \in B\ (y = f(x) \Leftrightarrow x = g(y))$

Theorem 9.3.19

A function $f\colon A \to B$ is bijective if and only if it has an inverse.

Proof

1. ("If")
 1.1. Suppose f has an inverse, say $g\colon B \to A$.
 1.2. We first show injectivity.
  1.2.1. Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$.
  1.2.2. Define $y = f(x_1) = f(x_2)$.
  1.2.3. Then $x_1 = g(y)$ and $x_2 = g(y)$ as g is an inverse of f.
  1.2.4. Thus $x_1 = x_2$.
 1.3. Next we show surjectivity.
  1.3.1. Let $y \in B$.
  1.3.2. Define $x = g(y)$.
  1.3.3. Then $y = f(x)$ as g is an inverse of f.
2. ("Only if") ...

- f is *surjective* if
  $$\forall y \in B\ \exists x \in A\ (y = f(x)).$$
- f is *injective* if
  $$\forall x_1, x_2 \in A\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

- f is *bijective* if it is both injective and surjective, i.e.,
  $$\forall y \in B\ \exists! x \in A\ (y = f(x)).$$

Bijectivity and invertibility

g is an inverse of f $\quad \Leftrightarrow \quad g = f^{-1}$
$\Leftrightarrow \quad \forall x \in A \ \forall y \in B \ (y = f(x) \Leftrightarrow x = g(y))$

Theorem 9.3.19

A function $f : A \to B$ is bijective if and only if it has an inverse.

- f is *surjective* if
$$\forall y \in B \ \exists x \in A \ (y = f(x)).$$
- f is *injective* if
$\forall x_1, x_2 \in A \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$

Proof

1. ("If") ...
2. ("Only if")
   - 2.1. Suppose f is bijective.
   - 2.2. Then $\forall y \in B \ \exists! x \in A \ (y = f(x))$.
   - 2.3. Define the function $g : B \to A$ by setting $g(y)$ to be the unique $x \in A$ such that $y = f(x)$ for all $y \in B$.
   - 2.4. This g is well defined and is an inverse of f by the definition of inverse functions. $\square$

- f is *bijective* if it is both injective and surjective, i.e.,
$$\forall y \in B \ \exists! x \in A \ (y = f(x)).$$

Checkpoint

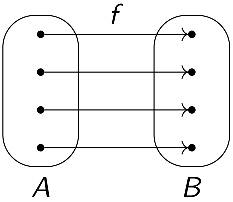
Definition 9.3.14

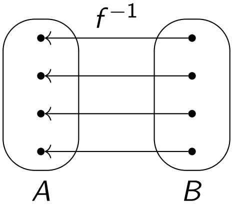
Let $f\colon A \to B$. Then $g\colon B \to A$ is an *inverse* of f if

$$\forall x \in A\ \forall y \in B\ \big(\, y = f(x) \quad \Leftrightarrow \quad x = g(y)\,\big).$$

Theorem 9.3.19

A function $f\colon A \to B$ is bijective if and only if it has an inverse.





Next

Cardinality

> [...] "[S]et" turns out to have many meanings, so that the purported foundation of all of Mathematics upon set theory totters. But there are other possibilities. For example, the membership relation for sets can often be replaced by the composition operation for functions. This leads to an alternative foundation for Mathematics upon categories [...]
>
> Mac Lane 1986