Lecture 5
Part I

BIJECTIVITY AND INVERSES

Injectivity (đơn ánh)

surjective: toàn ánh
bijective: song ánh

Definition

A function $f : A \to B$ is **injective** (or **one-to-one**) if, and only if, distinct elements of A have distinct images under f.
Symbolically, f is injective if, and only if,

$$\forall a_1, a_2 \in A,\ (a_1 \neq a_2 \ \to\ f(a_1) \neq f(a_2)),$$

or equivalently (and more useful),

$$\forall a_1, a_2 \in A,\ (f(a_1) = f(a_2) \ \to\ a_1 = a_2).$$

Example

- Let A be a set. Then I_A is injective.
- Let B be a subset of A. Then ι_B^A is injective.
- Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. Then f is not injective since $f(1) = f(-1)$.

Arrow Diagram

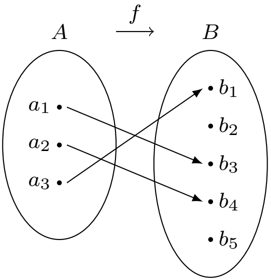


Figure: The arrow diagram of an injective function

The arrow diagram of an injective function has the additional characteristic that no two arrows terminate at the same point in the codomain (hence injective functions are also said to be one-to-one).

How to prove that a function is injective

To prove that a function $f : A \to B$ is injective:

- Take two (general) elements $a_1, a_2 \in A$ and assume that $f(a_1) = f(a_2)$;
- Work towards the conclusion $a_1 = a_2$.

Example

Prove that $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f(x) = x^2$ for all $x \in \mathbb{R}^+$ is injective.

Solution:

1. Take $x, y \in \mathbb{R}^+$, and assume that $f(x) = f(y)$.
2. Evaluating $f(x)$ and $f(y)$, we get $x^2 = y^2$, so that $0 = x^2 - y^2 = (x - y)(x + y)$.
3. Thus $x = y$ or $x = -y$.
4. But both $x, y > 0$, so $x \neq -y$.
5. (3) and (4) yield $x = y$.
6. Hence f is injective.

Composition of Functions Preserves Injectivity

Lemma

Let $f : A \to B$ and $g : B \to C$ be injective functions. Then $g \circ f$ is injective.

Proof.

1. Take $a_1, a_2 \in A$, and assume that $(g \circ f)(a_1) = (g \circ f)(a_2)$.
2. Then $g(f(a_1)) = g(f(a_2))$.
3. Let $b_1 = f(a_1)$ and $b_2 = f(a_2)$. Then $b_1, b_2 \in B$ and $g(b_1) = g(b_2)$.
4. Thus $b_1 = b_2$ by injectivity of g.
5. Now $f(a_1) = b_1 = b_2 = f(a_2)$ implies that $a_1 = a_2$ by injectivity of f.
6. Hence $g \circ f$ is injective.

$\square$

Exercise

no

If only f (or only g) is injective, can we conclude that $g \circ f$ is injective?

We have a partial converse of the last lemma:

Lemma

Let $f : A \to B$ and $g : B \to C$ be functions. If $g \circ f$ is injective, then f is injective.

Proof.

1. Take $a_1, a_2 \in A$, and assume that $f(a_1) = f(a_2)$.
2. Then $g(f(a_1)) = g(f(a_2))$.
3. Thus $(g \circ f)(a_1) = (g \circ f)(a_2)$, so that $a_1 = a_2$ by injectivity of $g \circ f$.
4. Hence f is injective.

$\square$

Exercise

If $g \circ f$ is injective, is g necessarily injective?

Surjectivity (toàn ánh)

Definition

A function $f : A \to B$ is **surjective** (or **onto**) if, and only if, its range equals its codomain, i.e. $\mathscr{R}(f) = B$.

Note

Recall that $\mathscr{R}(f) = B$ if and only if $\mathscr{R}(f) \subseteq B$ and $B \subseteq \mathscr{R}(f)$. But $\mathscr{R}(f) \subseteq B$ is always true (i.e. a tautology). Thus $\mathscr{R}(f) = B$ if and only if $B \subseteq \mathscr{R}(f)$. In other words, f is surjective if and only if

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

Example

- Let A be a set. Then I_A is surjective.
- Let B be a subset of A, Then ι_B^A is surjective if and only if $B = A$.
- Let $f : \mathbb{R} \to \mathbb{R};\ x \mapsto x^2$. Then f is not surjective since $-1 \in \mathbb{R} - \mathscr{R}(f)$.

Arrow Diagram

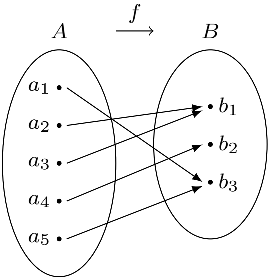


Figure: The arrow diagram of a surjective function

The arrow diagram of a surjective function has the additional characteristic that every element in the codomain has at least one arrow terminating there.

How to prove that a function is surjective

To prove that a function $f : A \to B$ is surjective, take a (general) element b of B, and find an element $a_b \in A$ such that $f(a_b) = b$.

Example

Prove that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 4x + 1$ for all $x \in \mathbb{R}$ is surjective.

Solution:

1. Take $b \in \mathbb{R}$.

   [We want to find $a_b \in \mathbb{R}$ such that $f(a_b) = b$, i.e. $4a_b + 1 = b$. Solving, we get $a_b = \frac{b-1}{4}$.]
2. Let $a_b = \frac{b-1}{4}$. Then $a_b \in \mathbb{R}$, and $f(a_b) = f(\frac{b-1}{4}) = 4(\frac{b-1}{4}) + 1 = b$.
3. Hence f is surjective.

Exercise

Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(x) = 4x + 1$ for all $x \in \mathbb{Z}$. Is g surjective?

Composition of Functions Preserves Surjectivity

Lemma

Let $f : A \to B$ and $g : B \to C$ be surjective functions. Then $g \circ f$ is surjective.

Proof.

1. Take $c \in C$.
2. There exists $b_c \in B$ such that $g(b_c) = c$ by surjectivity of g.
3. There exists $a_{b_c} \in A$ such that $f(a_{b_c}) = b_c$ by surjectivity of f.
4. Thus $a_{b_c} \in A$ and $(g \circ f)(a_{b_c}) = g(f(a_{b_c})) = g(b_c) = c$.
5. Hence $g \circ f$ is surjective.

$\square$

Exercise

NO

If only f (or only g) is surjective, can we conclude that $g \circ f$ is surjective?

We have a partial converse of the last lemma:

Lemma

Let $f : A \to B$ and $g : B \to C$ be functions. If $g \circ f$ is surjective, then g is surjective.

Proof.

1. Take $c \in C$.
2. There exists $a_c \in A$ such that $(g \circ f)(a_c) = c$ by surjectivity of $g \circ f$.
3. Let $b_c = f(a_c)$. Then $b_c \in B$ and

$$g(b_c) = g(f(a_c)) = (g \circ f)(a_c) = c.$$

4. Hence g is surjective.

$\square$

Exercise

If $g \circ f$ is surjective, is f necessarily surjective?

Bijectivity (Song ánh)

Definition

A function is **bijective** if and only if it is both injective and surjective.

Example

- Let A be a set. Then I_A is bijective.
- Let B be a subset of A. Then ι_B^A is bijective if and only if $B = A$.
- Let $f : A \to B$ be an injective function. Then $g : A \to f(A)$ defined by $g(a) = f(a)$ for all $a \in A$ is a well-defined bijective function.

Note

Let $f : A \to B$ and $g : B \to C$ be functions.

- If both f and g are bijective, then $g \circ f$ is bijective.
- If $g \circ f$ is bijective, then f is injective and g is surjective.

An Important Example

Let $f : \mathbb{Z} \to \mathbb{Z}^+$ be defined by

$$f(n) = \begin{cases} 2n, & \text{if } n > 0; \\ -2n+1, & \text{if } n \leq 0. \end{cases}$$

(Check: f is well-defined.)

Claim: f is bijective.

Proof.

1.
   1. Take $m \in \mathbb{Z}^+$.
      1. Case 1: m is even.
         Then $\frac{1}{2}m \in \mathbb{Z}^+$, and $f(\frac{1}{2}m) = m$.
      2. Case 2: m is odd.
         Then $\frac{1}{2}(m-1) \in \mathbb{Z}_{\geq 0}$, so $\frac{1}{2}(1-m) \in \mathbb{Z}_{\leq 0}$, and $f(\frac{1}{2}(1-m)) = m$.
   2. Hence there exists $n_m \in \mathbb{Z}$ such that $f(n_m) = m$, and f is surjective.

continue on next frame . . .

Proof (Cont'd).

2. 1. Take n_1, n_2 in $\mathbb{Z}$ and assume that $f(n_1) = f(n_2)$.
      1. Case 1: $n_1 > 0$, $n_2 > 0$.
         $f(n_1) = 2n_1$ and $f(n_2) = 2n_2$. Thus $f(n_1) = f(n_2)$ yields $n_1 = n_2$.
      2. Case 2: $n_1 > 0$, $n_2 \leq 0$.
         $f(n_1) = 2n_1$ and $f(n_2) = -2n_2 + 1$. Then $f(n_1) = f(n_2)$ yields $1 = 2(n_1 + n_2)$, a contradiction.
         Thus this case does not happen.
      3. Case 3: $n_1 \leq 0$, $n_2 > 0$.
         $f(n_2) = -2n_1 + 1$ and $f(n_2) = 2n_2$. Then $f(n_1) = f(n_2)$ yields $1 = 2(n_1 + n_2)$, a contradiction.
         Thus this case does not happen.
      4. Case 4: $n_1 \leq 0$, $n_2 < 0$.
         $f(n_1) = -2n_1 + 1$ and $f(n_2) = -2n_2 + 1$. Thus $f(n_1) = f(n_2)$ yields $n_1 = n_2$.
   2. Hence $n_1 = n_2$, and f is injective.

$\square$

Lemma

Let $f : A \to B$ be a function. Then f is bijective if and only if for every $b \in B$, there exists a unique $a_b \in A$ such that $f(a_b) = b$.

Proof.

1. Suppose that f is bijective.
   1. For every $b \in B$, there exists $a_b \in A$ such that $f(a_b) = b$ by surjectivity of f.
   2. If $a_b' \in A$ such that $f(a_b') = b$, then $f(a_b') = f(a_b)$, so that $a_b' = a_b$ by injectivity of f, showing the uniqueness of a_b.
2. Suppose that for every $b \in B$, there exists a unique $a_b \in A$ such that $f(a_b) = b$.
   1. Clearly, f is surjective.
   2. Take $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$. Let $b = f(a_1)$. Then $b \in B$, and so there exists unique $a_b \in A$ such that $f(a_b) = b$. Thus $a_1 = a_b = a_2$. Hence f is injective.

$\square$

Inverse

Definition

Let $f : A \to B$ be a function. An **inverse** of f is a function $g : B \to A$ such that

$$g \circ f = I_A \qquad \textbf{and} \qquad f \circ g = I_B.$$

Example

- Let $f, g : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x$ and $g(x) = \frac{1}{2}x$ for all $x \in \mathbb{R}$. Then g is an inverse of f.
- Let $h : \mathbb{R} \to \mathbb{R}_{\geq 0}$ be the absolute value function, i.e. $h(x) = |x|$. Then

$$(h \circ \iota_{\mathbb{R}_{\geq 0}}^{\mathbb{R}})(x) = h(\iota_{\mathbb{R}_{\geq 0}}^{\mathbb{R}}(x)) = h(x) = |x| = x = I_{\mathbb{R}_{\geq 0}}(x)$$

for all $x \in \mathbb{R}_{\geq 0}$, so that $h \circ \iota_{\mathbb{R}_{\geq 0}}^{\mathbb{R}} = I_{\mathbb{R}_{\geq 0}}$.

Is h an inverse of $\iota_{\mathbb{R}_{\geq 0}}^{\mathbb{R}}$? Is $\iota_{\mathbb{R}_{\geq 0}}^{\mathbb{R}}$ an inverse of h?

Intuitively, an inverse of f is a function whose arrow diagram is obtained from by reversing the arrows in the arrow diagram $\mathscr{A}$ of f. But does reversing the arrows in $\mathscr{A}$ really give an inverse of f?

For this, we need to ask if the arrow diagram so obtained (call it $\mathscr{A}'$) has the characteristics of the arrow diagram of a function.

- Does all arrows in $\mathscr{A}'$ originate from B and terminate in A?
  Yes, since all arrows in $\mathscr{A}$ originate from A and terminate in B.
- Does every element $b \in B$ has at least one arrow in $\mathscr{A}'$ originating from it?
  This is true if and only if every element $b \in B$ has at least one arrow in $\mathscr{A}$ terminating at it. In other words this is true if and only if f is surjective.
- Does every element $b \in B$ has at most one arrow in $\mathscr{A}'$ originating from it?
  This is true if and only if every element $b \in B$ has at most one arrow in $\mathscr{A}$ terminating at it. In other words this is true if and only if f is injective.

Lemma

Let $f : A \to B$ be a function. Then f has an inverse if and only if f is bijective.

Proof.

1. Suppose that f has an inverse g.
   1. Then $g \circ f = I_A$ and I_A bijective imply that f is injective.
   2. Also $f \circ g = I_B$ and I_B bijective imply that f is surjective.
   3. Thus f is bijective.
2. Suppose that f is bijective.
   1. Then for every $b \in B$, there exists a unique $a_b \in A$ such that $f(a_b) = b$.
   2. Define $g : B \to A$ by $g(b) = a_b$.
   3. Then g is a well-defined function, and $(f \circ g)(b) = f(g(b)) = f(a_b) = b$ for all $b \in B$, so that $f \circ g = I_B$.
   4. Furthermore, $(g \circ f)(a) = g(f(a)) = a_{f(a)}$ for all $a \in A$. But $f(a_{f(a)}) = f(a)$, so that $a_{f(a)} = a$ since f is injective. Thus $(g \circ f)(a) = a$ for all $a \in A$, i.e. $g \circ f = I_A$.
   5. Hence g is an inverse of f.

□

Lemma

Let $f : A \to B$ be a function. Suppose that $g, h : B \to A$ such that $g \circ f = I_A$ and $f \circ h = I_B$. Then $g = h$.

Proof.

We have

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

□

Corollary

Let $f : A \to B$ be a bijective function. If g and h are both inverses of f, then $g = h$.
In other words, the inverse of a bijective function is unique.

Proof.

If g and h are both inverses of f, then they satisfy the conditions of the last lemma, and hence its conclusion applies. □

Let $f : A \to B$ be a function. We saw that f has an inverse if and only if f is bijective, in which case the inverse of f is unique, which shall henceforth be denoted as f^{-1}.

Caution!

- The notation f^{-1} makes sense only when f is bijective, but the notation $f^{-1}(Y)$ makes sense all the time (when $Y \subseteq B$).
- Do not write $f^{-1}(b)$ for $b \in B$ when f is not bijective, even when $f^{-1}(\{b\})$ has only one element.

Exercise

Let f be a bijective function. Prove that:

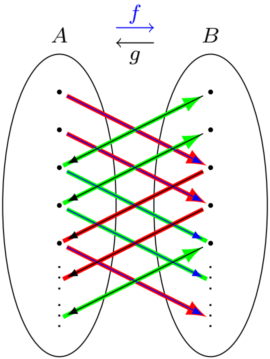
1. f^{-1} is bijective;
2. $(f^{-1})^{-1} = f$.

Cantor-Bernstein Theorem

Theorem (Cantor-Bernstein)

Let $f : A \to B$ and $g : B \to A$ be injective functions. Then there exists a bijective function $h : A \to B$.

Idea of Proof



The red and green arrows show how the bijective function $h : A \to B$ should be defined.

Proof of Cantor-Bernstein Theorem

1. Let $\gamma : B \to g(B)$ be defined by $\gamma(b) = g(b)$ for all $b \in B$. Then γ is bijective, with inverse $\gamma^{-1} : g(B) \to B$; $g(b) \mapsto b$ for all $b \in B$.
2. Let $B' = \{(f \circ g)^n(b) \mid b \in B - f(A),\ n \in \mathbb{Z}_{\geq 0}\}$. Then $B - f(A) \subseteq B' \subseteq B$.
3. Let $a \in A$ such that $f(a) \in B'$.
   1. Then $f(a) = (f \circ g)^n(b)$ for some $b \in B - f(A)$ and $n \in \mathbb{Z}_{\geq 0}$.
   2. If $n = 0$, then $f(a) = b \in B - f(A)$, contradicting $f(a) \in f(A)$. Thus $n > 0$.
   3. Hence $f(a) = (f \circ g)((f \circ g)^{n-1}(b)) = f(g((f \circ g)^{n-1}(b)))$, so that $a = g((f \circ g)^{n-1}(b))$ by injectivity of f.
   4. In particular, $a \in g(B)$, and $\gamma^{-1}(a) = (f \circ g)^{n-1}(b) \in B'$.
4. Define $h : A \to B$ by

$$h(a) = \begin{cases} \gamma^{-1}(a), & \text{if } f(a) \in B'; \\ f(a), & \text{if } f(a) \in B - B'. \end{cases}$$

Then h is well-defined by (3.4).

Proof of Cantor-Bernstein Theorem (Cont'd)

5. By (3.4) and (4), we have

$$h(a) \in \begin{cases} B', & \text{if } f(a) \in B'; \\ B - B', & \text{if } f(a) \in B - B'. \end{cases}$$

6. Take $a_1, a_2 \in A$, and assume that $h(a_1) = h(a_2)$.
   1. Case 1: $h(a_1) = h(a_2) \in B'$.
      1. Then $f(a_1), f(a_2) \in B'$ by (5).
      2. $h(a_1) = \gamma^{-1}(a_1)$ and $h(a_2) = \gamma^{-1}(a_2)$ by (4).
      3. $\gamma^{-1}(a_1) = \gamma^{-1}(a_2)$ by (6) and (6.1.2).
      4. $a_1 = a_2$ by injectivity of γ^{-1}.
   2. Case 2: $h(a_1) = h(a_2) \in B - B'$.
      1. Then $f(a_1), f(a_2) \in B - B'$ by (5).
      2. $h(a_1) = f(a_1)$ and $h(a_2) = f(a_2)$ by (4).
      3. $f(a_1) = f(a_2)$ by (6) and (6.2.2).
      4. $a_1 = a_2$ by injectivity of f.

   Thus h is injective.

Proof of Cantor-Bernstein Theorem (Cont'd)

7. Take $b \in B$.
   1. Case 1: $b \in B'$.
      1. $b = (f \circ g)^n(b')$ for some $b' \in B - f(A)$ and $n \in \mathbb{Z}_{\geq 0}$.
      2. $(f \circ g)(b) = (f \circ g)^{n+1}(b') \in B'$.
      3. Let $a = g(b)$. Then $f(a) = f(g(b)) = (f \circ g)(b) \in B'$ by (7.1.2).
      4. Thus $h(a) = \gamma^{-1}(a) = \gamma^{-1}(g(b)) = b$, by definition of h.
   2. Case 2: $b \in B - B'$.
      1. If $b \notin f(A)$, then $b \in B - f(A)$, so that $b \in B'$ by (2), contradicting (7.2).
      2. Thus $b \in f(A)$, and so there exists $a \in A$ such that $f(a) = b$.
      3. By definition of h, we have $h(a) = f(a) = b$.

   Thus h is surjective.
8. By (6) and (7), h is bijective, and the proof is complete.

Summary

We have covered:

- Injective and surjective functions
- The additional characteristic of the arrow diagram of an injective/a surjective function
- How to prove that a function is injective/surjective
- Composition of functions preserves injectivity and surjectivity, and its partial converse
- Equivalence of bijectivity and invertibility
- Cantor-Bernstein Theorem