CISC 1100: Structures of Computer Science

Chapter 5
Functions

Arthur G. Werschulz

Fordham University Department of Computer and Information Sciences

Summer, 2015

Why functions?

- Sets: rigorous way to talk about collections of objects

Why functions?

- Sets: rigorous way to talk about collections of objects
- Logic: rigorous way to talk about conditions and decisions

Why functions?

- Sets: rigorous way to talk about collections of objects
- Logic: rigorous way to talk about conditions and decisions
- Relations: rigorous way to talk about how objects can relate to each other

Why functions?

- Sets: rigorous way to talk about collections of objects
- Logic: rigorous way to talk about conditions and decisions
- Relations: rigorous way to talk about how objects can relate to each other
- Function: a relation in which each element of the domain is related to *exactly one* element in the codomain

Some examples

- People may have gone to several high schools, only one of which was last

Some examples

- People may have gone to several high schools, only one of which was last
  - person $\rightarrow$ high school: relation

Some examples

- People may have gone to several high schools, only one of which was last
  - person $\rightarrow$ high school: relation
  - person $\rightarrow$ final high school: function
- Facebook users have email addresses, but typically only one favorite email address

Some examples

- People may have gone to several high schools, only one of which was last
  - person → high school: relation
  - person → final high school: function
- Facebook users have email addresses, but typically only one favorite email address
  - Facebook user → email address: relation

Some examples

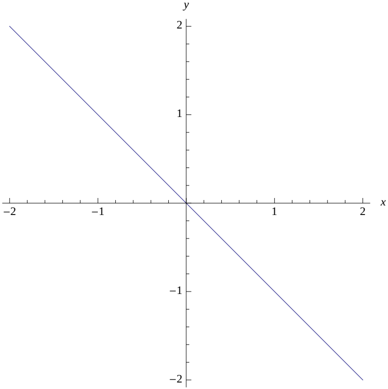
- People may have gone to several high schools, only one of which was last
  - person $\rightarrow$ high school: relation
  - person $\rightarrow$ final high school: function
- Facebook users have email addresses, but typically only one favorite email address
  - Facebook user $\rightarrow$ email address: relation
  - Facebook user $\rightarrow$ favorite email address: function

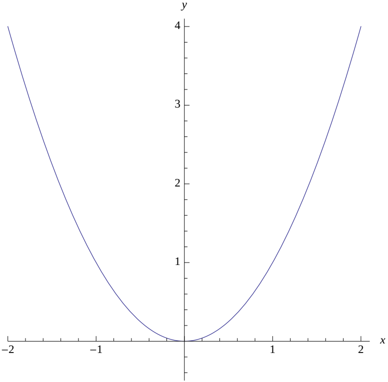
Outline

- What is a function?
- Relations and functions
- Properties of functions
- Function composition
- Identity and inverse functions
- An application: cryptography
- More about functions
- An application: secure storage of computer passwords

What is a function?

You may have already had some experience with functions, such as plotting curves such as $y = -x$ or $y = x^2$:





What is a function (cont'd)?

- The black-box model:

What is a function (cont'd)?

- The black-box model:

- Parts of speech:

What is a function (cont'd)?

- The black-box model:

- Parts of speech:
  - *domain* X: all possible inputs

What is a function (cont'd)?

- The black-box model:

- Parts of speech:
  - *domain* X: all possible inputs
  - *codomain* Y: all possible outputs

What is a function (cont'd)?

- The black-box model:

- Parts of speech:
  - *domain* X: all possible inputs
  - *codomain* Y: all possible outputs
  - f: the *name* of the function (represents the rule telling assigning the output value to a given input value)

What is a function (cont'd)?

- The black-box model:

- Parts of speech:
  - *domain* X: all possible inputs
  - *codomain* Y: all possible outputs
  - f: the *name* of the function (represents the rule telling assigning the output value to a given input value)
- Notation $f : X \to Y$

How to describe a function?

- Graphs work for numerical functions.

How to describe a function?

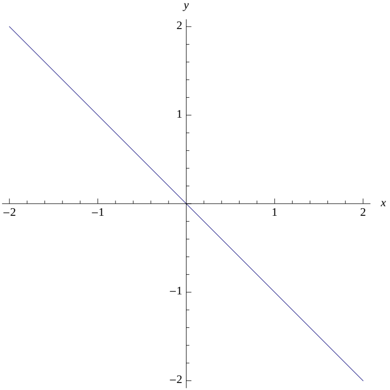
- Graphs work for numerical functions.
- Not all functions are numerical.

How to describe a function?

- Graphs work for numerical functions.
- Not all functions are numerical.
- Could use English (even for numerical functions).

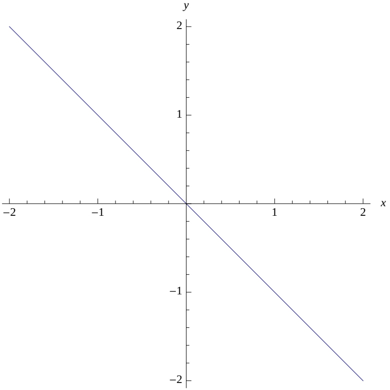
How to describe a function (cont'd)?

Example: For the function



How to describe a function (cont'd)?

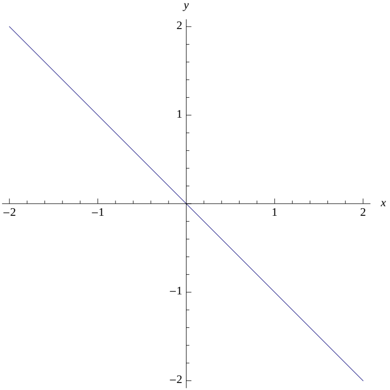
Example: For the function



- Domain is $\mathbb{R}$.

How to describe a function (cont'd)?

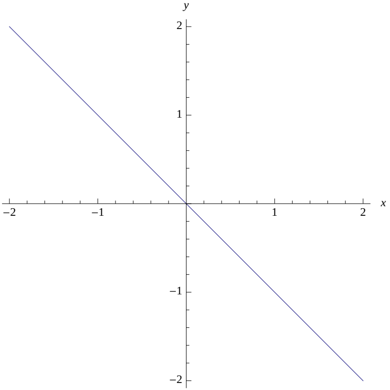
Example: For the function



- Domain is $\mathbb{R}$.
- Codomain is $\mathbb{R}$.

How to describe a function (cont'd)?

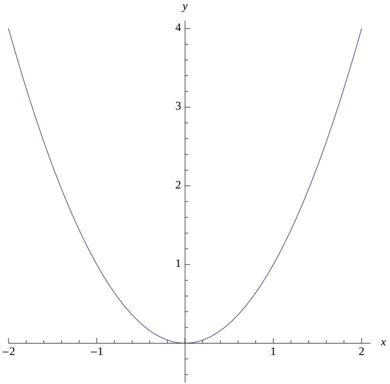
Example: For the function



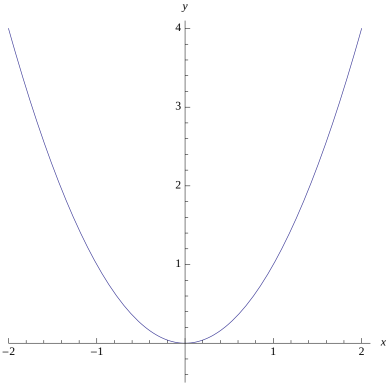
- Domain is $\mathbb{R}$.
- Codomain is $\mathbb{R}$.
- Rule: This function returns the output value $-x$ for any given input value x.

How to describe a function (cont'd)?

Example: For the function

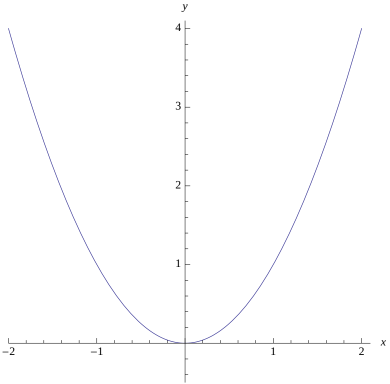


Example: For the function



- Domain is $\mathbb{R}$.

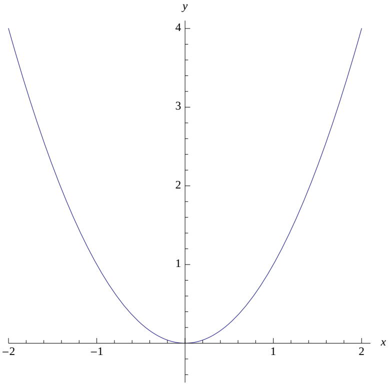
Example: For the function



- Domain is $\mathbb{R}$.
- Codomain is $\mathbb{R}$

How to describe a function (cont'd)?

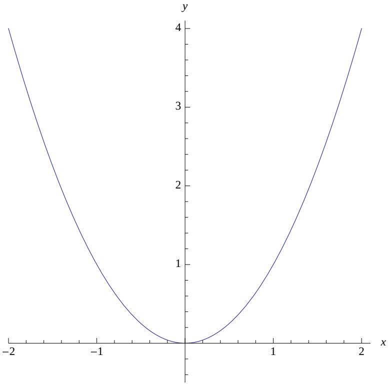
Example: For the function



- Domain is $\mathbb{R}$.
- Codomain is $\mathbb{R}$ (but could've been $\mathbb{R}^{\geq 0}$).

How to describe a function (cont'd)?

Example: For the function



- Domain is $\mathbb{R}$.
- Codomain is $\mathbb{R}$ (but could've been $\mathbb{R}^{\geq 0}$).
- Rule: This function returns the output value x^2 for any given input value x.

How to describe a function (cont'd)?

- Can use a table . . . more convenient than English.

How to describe a function (cont'd)?

- Can use a table ... more convenient than English.
- **Example:** A function $d\colon \{1,2,3,4,5\} \to \mathbb{N}$ whose table is given by

t	1	2	3	4	5
$d(t)$	2	4	6	8	10

How to describe a function (cont'd)?

- Can use a table . . . more convenient than English.
- **Example:** A function $d\colon \{1,2,3,4,5\} \to \mathbb{N}$ whose table is given by

t	1	2	3	4	5
$d(t)$	2	4	6	8	10

This tells us that $d(1) = 2$, $d(2) = 4$, etc.

How to describe a function (cont'd)?

- Can use a table ... more convenient than English.
- **Example:** A function $d\colon \{1,2,3,4,5\} \to \mathbb{N}$ whose table is given by

t	1	2	3	4	5
$d(t)$	2	4	6	8	10

  This tells us that $d(1) = 2$, $d(2) = 4$, etc.
- **Example:** A function $d^*\colon \{1,2,3,4,5\} \to \{2,4,6,8,10\}$ given by

z	1	2	3	4	5
$d^*(z)$	2	4	6	8	10

How to describe a function (cont'd)?

- Can use a table . . . more convenient than English.
- **Example:** A function $d\colon \{1, 2, 3, 4, 5\} \to \mathbb{N}$ whose table is given by

t	1	2	3	4	5
$d(t)$	2	4	6	8	10

  This tells us that $d(1) = 2$, $d(2) = 4$, etc.
- **Example:** A function $d^*\colon \{1, 2, 3, 4, 5\} \to \{2, 4, 6, 8, 10\}$ given by

z	1	2	3	4	5
$d^*(z)$	2	4	6	8	10

- The functions d and d^* are different.
  Why?

How to describe a function (cont'd)?

- Can use a table ... more convenient than English.
- **Example:** A function $d\colon \{1,2,3,4,5\} \to \mathbb{N}$ whose table is given by

t	1	2	3	4	5
$d(t)$	2	4	6	8	10

  This tells us that $d(1) = 2$, $d(2) = 4$, etc.
- **Example:** A function $d^*\colon \{1,2,3,4,5\} \to \{2,4,6,8,10\}$ given by

z	1	2	3	4	5
$d^*(z)$	2	4	6	8	10

- The functions d and d^* are different.
  Why? Different codomains!

How to describe a function (cont'd)?

Example: A function $d^{**} \colon \mathbb{Z}^+ \to \mathbb{Z}^+$ given by the table

z	1	2	3	4	5	6	7	8	9	10	...
$d^{**}(z)$	2	4	6	8	10	12	14	16	18	20	...

Example: A function $d^{**}\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ given by the table

z	1	2	3	4	5	6	7	8	9	10	...
$d^{**}(z)$	2	4	6	8	10	12	14	16	18	20	...

Alternatively, can say that $d^{**}\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ is given by the rule

$$d^{**}(x) = 2x \qquad \forall\, x \in \mathbb{Z}^+.$$

More examples

- Coffee shop's menu:

c	$p(c)$
small	\$1.25
medium	\$2.15
large	\$2.75

This describes a function

$$p\colon \{\text{small}, \text{medium}, \text{large}\} \to \mathbb{Q}$$

More examples

- Coffee shop's menu:

c	$p(c)$
small	\$1.25
medium	\$2.15
large	\$2.75

  This describes a function

$$p\colon \{\text{small}, \text{medium}, \text{large}\} \to \mathbb{Q}$$

- Bakery's menu:

i	$b(i)$
bagel	\$1.00
croissant	\$1.25
danish	\$2.25
muffin	\$1.50

  This describes a function

$$b\colon \{\text{bagel}, \text{croissant}, \text{danish}, \text{muffin}\} \to \mathbb{Q}$$

Still more examples

My address book looks something like this:

n	$e(n)$
⋮	⋮
Harry Q. Bovik	`bovik@cs.cmu.edu`
James T. Kirk	`kirk@starfleet.federation.gov`
Darth Vader	`vader@empire.gov`
⋮	⋮

Still more examples

My address book looks something like this:

n	$e(n)$
$\vdots$	$\vdots$
Harry Q. Bovik	`bovik@cs.cmu.edu`
James T. Kirk	`kirk@starfleet.federation.gov`
Darth Vader	`vader@empire.gov`
$\vdots$	$\vdots$

This table describes a function

$$e\colon \{\text{my friends}\} \to \{\text{all possible email addresses}\}$$

Still more examples

Each Facebook user has a gender (which s/he needn't specify):

p	$g(p)$
⋮	⋮
Bovik, Harry Q.	U
Lyons, Damian M.	M
Weiss, Gary M.	M
Papadakis-Kanaris, Christina	F
Werschulz, Arthur G.	M
⋮	⋮

Still more examples

Each Facebook user has a gender (which s/he needn't specify):

p	$g(p)$
⋮	⋮
Bovik, Harry Q.	U
Lyons, Damian M.	M
Weiss, Gary M.	M
Papadakis-Kanaris, Christina	F
Werschulz, Arthur G.	M
⋮	⋮

This table describes a function

$$g\colon \{\text{all Facebook users}\} \to G$$

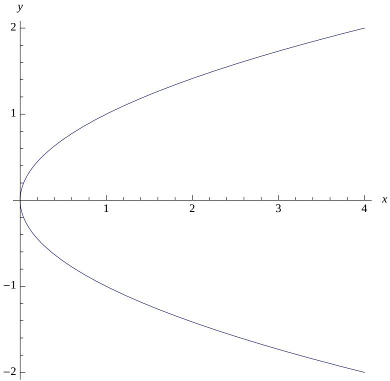
where $G = \{\text{M}, \text{F}, \text{U}\}$.

- If r is a relation from X to Y:
  - Some elements of X might not participate in the relation, i.e., there might be $x \in X$ such that $(x, y) \notin r$ for *any* $y \in Y$.
  - Some elements of X might be related to *more than one* element of Y, i.e., there might be $x \in X$ such that both $(x, y_1) \in r$ and $(x, y_2) \in r$, where $y_1 \neq y_2$.

Functions and relations

- If r is a relation from X to Y:
  - Some elements of X might not participate in the relation, i.e., there might be $x \in X$ such that $(x, y) \notin r$ for *any* $y \in Y$.
  - Some elements of X might be related to *more than one* element of Y, i.e., there might be $x \in X$ such that both $(x, y_1) \in r$ and $(x, y_2) \in r$, where $y_1 \neq y_2$.
- This cannot happen with functions. If $f \colon X \to Y$, then
  - Every $x \in X$ participates in the function, i.e., $f(x)$ is defined for each $x \in X$.
  - Each $x \in X$ is associated with *exactly one* $y \in Y$, i.e., $f(x)$ is "well-defined" for each $x \in X$.

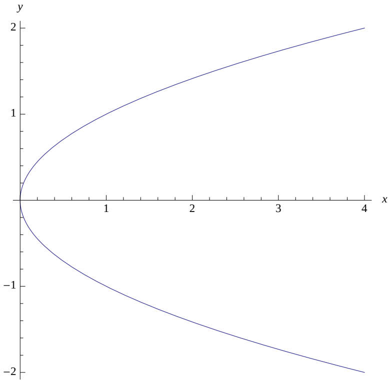
Example: The curve $x = y^2$ looks like



Does it define a function from x-values to y-values?

Functions and relations (cont'd)

Example: The curve $x = y^2$ looks like



Does it define a function from x-values to y-values? No.

Let's look at some examples.

- Define $f\colon \{1,2,3,4\} \to \{1,2,3,4\}$ by

x	1	2	3
$f(x)$	3	1	2

Is f a function?

Functions and relations (cont'd)

Let's look at some examples.

- Define $f: \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ by

x	1	2	3
$f(x)$	3	1	2

  Is f a function? No! What's $f(4)$?

Let's look at some examples.

- Define $f\colon \{1,2,3,4\} \to \{1,2,3,4\}$ by

x	1	2	3
$f(x)$	3	1	2

  Is f a function? No! What's $f(4)$?

- Let r be a relation from $\{1,2,3,4\}$ to $\{1,2,3,4\}$ given by

$$r = \{(1,3),(2,4),(3,1),(4,4),(1,4)\}$$

  Does r determine a function?

Let's look at some examples.

- Define $f\colon \{1,2,3,4\} \to \{1,2,3,4\}$ by

x	1	2	3
$f(x)$	3	1	2

  Is f a function? No! What's $f(4)$?

- Let r be a relation from $\{1,2,3,4\}$ to $\{1,2,3,4\}$ given by

$$r = \{(1,3),(2,4),(3,1),(4,4),(1,4)\}$$

  Does r determine a function? No! $r(1)$ would need to be both 3 and 4.

Functions and relations (cont'd)

More examples:

- Let q be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$q(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is q a function?

Functions and relations (cont'd)

More examples:

- Let q be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$q(x) = y \qquad \text{iff} \qquad x = y^2$$

Is q a function? No! Since $1 = 1^2$ and $1 = (-1)^2$, the value $q(1)$ isn't well-defined.

More examples:

- Let q be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$q(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is q a function? No! Since $1 = 1^2$ and $1 = (-1)^2$, the value $q(1)$ isn't well-defined.

- Let s be a relation from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}^{\geq 0}$ defined by

$$s(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is s a function?

More examples:

- Let q be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$q(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is q a function? No! Since $1 = 1^2$ and $1 = (-1)^2$, the value $q(1)$ isn't well-defined.

- Let s be a relation from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}^{\geq 0}$ defined by

$$s(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is s a function? Yes! $s(x) = y$ iff $x = y^2$ iff $y = \sqrt{x}$.

Functions and relations (cont'd)

More examples:

- Let q be a relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$q(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is q a function? No! Since $1 = 1^2$ and $1 = (-1)^2$, the value $q(1)$ isn't well-defined.

- Let s be a relation from $\mathbb{R}^{\geq 0}$ to $\mathbb{R}^{\geq 0}$ defined by

$$s(x) = y \qquad \text{iff} \qquad x = y^2$$

  Is s a function? Yes! $s(x) = y$ iff $x = y^2$ iff $y = \sqrt{x}$.

Moral of the story? All three pieces (the domain, the codomain, and the "rule") are important.

More terminology

- The *range* of a function is the set of all values it can assume, i.e.,
$$\text{Range}(f) = f(X) = \{\, f(x) : x \in X \,\}.$$
- We sometimes write $f(X)$ for the range of $f: X \to Y$.
- Note that $\text{Range}(f) \subseteq Y$, i.e., the range is always a subset of the codomain.

More terminology

- The *range* of a function is the set of all values it can assume, i.e.,
$$\text{Range}(f) = f(X) = \{ f(x) : x \in X \}.$$
- We sometimes write $f(X)$ for the range of $f\colon X \to Y$.
- Note that $\text{Range}(f) \subseteq Y$, i.e., the range is always a subset of the codomain.
  - **Example:** Define $g\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$g(t)$	3	1	2	1

    Then

More terminology

- The *range* of a function is the set of all values it can assume, i.e.,

$$\text{Range}(f) = f(X) = \{\, f(x) : x \in X \,\}.$$

- We sometimes write $f(X)$ for the range of $f\colon X \to Y$.
- Note that $\text{Range}(f) \subseteq Y$, i.e., the range is always a subset of the codomain.
  - **Example:** Define $g\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$g(t)$	3	1	2	1

  Then $\text{Range}(g) = \text{Codomain}(g)$.

More terminology

- The *range* of a function is the set of all values it can assume, i.e.,
$$\text{Range}(f) = f(X) = \{\, f(x) : x \in X \,\}.$$
- We sometimes write $f(X)$ for the range of $f\colon X \to Y$.
- Note that $\text{Range}(f) \subseteq Y$, i.e., the range is always a subset of the codomain.
  - **Example:** Define $g\colon \{1, 2, 3, 4\} \to \{1, 2, 3\}$ by

t	1	2	3	4
$g(t)$	3	1	2	1

    Then $\text{Range}(g) = \text{Codomain}(g)$.
  - **Example:** Define $h\colon \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ by

t	1	2	3	4
$h(t)$	3	1	2	1

    Then

More terminology

- The *range* of a function is the set of all values it can assume, i.e.,
$$\text{Range}(f) = f(X) = \{\, f(x) : x \in X \,\}.$$
- We sometimes write $f(X)$ for the range of $f\colon X \to Y$.
- Note that $\text{Range}(f) \subseteq Y$, i.e., the range is always a subset of the codomain.
    - **Example:** Define $g\colon \{1, 2, 3, 4\} \to \{1, 2, 3\}$ by

t	1	2	3	4
$g(t)$	3	1	2	1

      Then $\text{Range}(g) = \text{Codomain}(g)$.
    - **Example:** Define $h\colon \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ by

t	1	2	3	4
$h(t)$	3	1	2	1

      Then $\text{Range}(h) \neq \text{Codomain}(h)$.

Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity).
  Ditto with functions.

Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity). Ditto with functions.
- Let $f\colon S \to T$ be a function.

Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity).
  Ditto with functions.
- Let $f \colon S \to T$ be a function.
  - f is *injective* if $f(x) = f(y) \Rightarrow x = y$, for any $x, y \in S$.

Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity).
  Ditto with functions.
- Let $f\colon S \to T$ be a function.
  - f is *injective* if $f(x) = f(y) \Rightarrow x = y$, for any $x, y \in S$.
    Equivalent formulation: $x, y \in S$ and $x \neq y \Rightarrow f(x) \neq f(y)$.

Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity).
  Ditto with functions.
- Let $f\colon S \to T$ be a function.
  - f is *injective* if $f(x) = f(y) \Rightarrow x = y$, for any $x, y \in S$.
    Equivalent formulation: $x, y \in S$ and $x \neq y \Rightarrow f(x) \neq f(y)$.
  - f is *surjective* if $\forall\, t \in T, \exists\, s \in S : t = f(s)$.

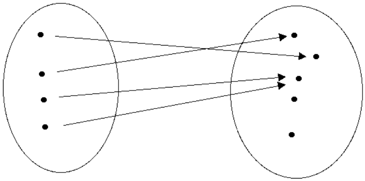
Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity).
  Ditto with functions.
- Let $f: S \to T$ be a function.
  - f is *injective* if $f(x) = f(y) \Rightarrow x = y$, for any $x, y \in S$.
    Equivalent formulation: $x, y \in S$ and $x \neq y \Rightarrow f(x) \neq f(y)$.
  - f is *surjective* if $\forall\, t \in T, \exists\, s \in S : t = f(s)$.
    Equivalent formulation: $\text{Range}(f) = T$.

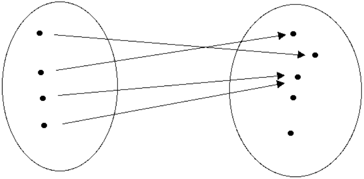
Properties of functions

- Relations sometimes have useful properties (reflexivity, irreflexity, symmetry, anstisymmetry, transitivity).
  Ditto with functions.
- Let $f\colon S \to T$ be a function.
  - f is *injective* if $f(x) = f(y) \Rightarrow x = y$, for any $x, y \in S$.
    Equivalent formulation: $x, y \in S$ and $x \neq y \Rightarrow f(x) \neq f(y)$.
  - f is *surjective* if $\forall\, t \in T, \exists\, s \in S : t = f(s)$.
    Equivalent formulation: $\text{Range}(f) = T$.
  - f is *bijective* if f is both injective and surjective.

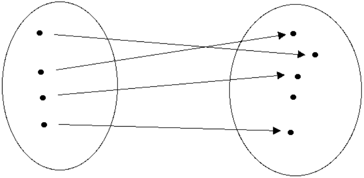
Properties of functions (cont'd)



Not injective,
not surjective.

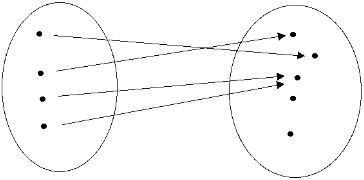


Not injective,
not surjective.

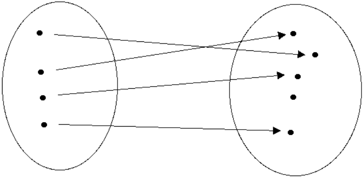


Injective.

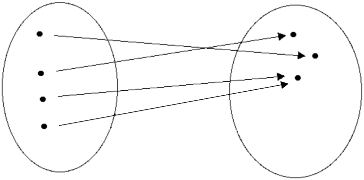
Properties of functions (cont'd)



Not injective,
not surjective.

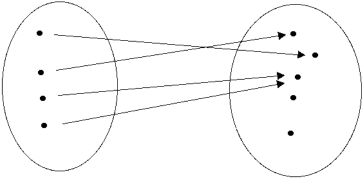


Injective.

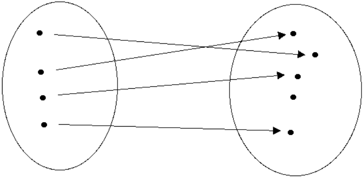


Surjective.

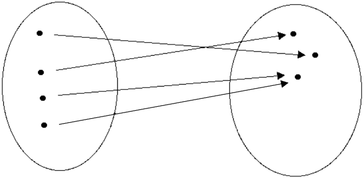
Properties of functions (cont'd)



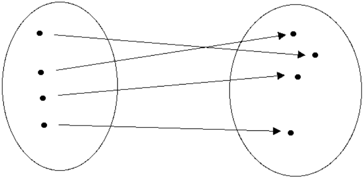
Not injective,
not surjective.



Injective.



Surjective.



Bijective.

Properties of functions (cont'd)

Alternative terminology:

Properties of functions (cont'd)

Alternative terminology:

- Using nouns instead of adjectives:
  - "f is an injection."
  - "f is a surjection."
  - "f is a bijection."

Properties of functions (cont'd)

Alternative terminology:

- Using nouns instead of adjectives:
  - "f is an injection."
  - "f is a surjection."
  - "f is a bijection."
- Simpler language.
  - "f is *one-to-one*" instead of "f is injective."
  - "f maps S *onto* T," instead of "$f : S \to T$ is surjective."

Properties of functions (cont'd)

Alternative terminology:

- Using nouns instead of adjectives:
  - "f is an injection."
  - "f is a surjection."
  - "f is a bijection."
- Simpler language.
  - "f is *one-to-one*" instead of "f is injective."
  - "f maps S *onto* T," instead of "$f : S \to T$ is surjective."
    - The word "onto" is a preposition, and not an adjective.
    - Please do not say "The function f is onto."

Another way of looking at these properties:
Think of $f\colon S \to T$ as labeling S-points with T-values, i.e.,

$$s \in S \text{ is labeled by } f(s) \in T.$$

Properties of functions (cont'd)

Another way of looking at these properties:
Think of $f : S \to T$ as labeling S-points with T-values, i.e.,

$$s \in S \text{ is labeled by } f(s) \in T.$$

- For f to be injective, no two distinct points in S can have the same label.

Properties of functions (cont'd)

Another way of looking at these properties:
Think of $f: S \to T$ as labeling S-points with T-values, i.e.,

$$s \in S \text{ is labeled by } f(s) \in T.$$

- For f to be injective, no two distinct points in S can have the same label.
- For f to be surjective, every point in T must have *at least* one label.

Properties of functions (cont'd)

Another way of looking at these properties:
Think of $f : S \to T$ as labeling S-points with T-values, i.e.,

$$s \in S \text{ is labeled by } f(s) \in T.$$

- For f to be injective, no two distinct points in S can have the same label.
- For f to be surjective, every point in T must have *at least* one label.
- For f to be bijective, every point in T must have *exactly* one label.

Properties of functions (cont'd)

Example: Let C be a can of paint and let F be a floor.
Let's transfer the paint from the can to the floor.
Define $p\colon C \to F$ by

$p(d)$ is the spot on the floor where the paint drop d lands.

Example: Let C be a can of paint and let F be a floor.
Let's transfer the paint from the can to the floor.
Define $p\colon C \to F$ by

$p(d)$ is the spot on the floor where the paint drop d lands.

- If no spot on floor winds up with more than one drop of paint, the p is injective.

Properties of functions (cont'd)

Example: Let C be a can of paint and let F be a floor.
Let's transfer the paint from the can to the floor.
Define $p\colon C \to F$ by

$p(d)$ is the spot on the floor where the paint drop d lands.

- If no spot on floor winds up with more than one drop of paint, the p is injective.
- If the entire floor gets covered with paint, then p is surjective.

Properties of functions (cont'd)

Example: Let C be a can of paint and let F be a floor.
Let's transfer the paint from the can to the floor.
Define $p\colon C \to F$ by

$$p(d) \text{ is the spot on the floor where the paint drop } d \text{ lands.}$$

- If no spot on floor winds up with more than one drop of paint, the p is injective.
- If the entire floor gets covered with paint, then p is surjective.
- If every spot on entire floor gets covered with exactly one drop of paint, then p is bijective.

Properties of functions (cont'd)

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective,

Properties of functions (cont'd)

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective,

Properties of functions (cont'd)

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f

Properties of functions (cont'd)

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective,

Properties of functions (cont'd)

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective, is not surjective,

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective, is not surjective, f is not bijective.

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective, is not surjective, f is not bijective.

- Define $q\colon \{1,2,3,4\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ by

τ	1	2	3	4
$q(\tau)$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$

  q

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective, is not surjective, f is not bijective.

- Define $q\colon \{1,2,3,4\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ by

τ	1	2	3	4
$q(\tau)$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$

  q is injective,

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective, is not surjective, f is not bijective.

- Define $q\colon \{1,2,3,4\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ by

τ	1	2	3	4
$q(\tau)$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$

  q is injective, is surjective,

More examples:

- Define $h\colon \{1,2,3,4\} \to \{1,2,3\}$ by

t	1	2	3	4
$h(t)$	3	1	2	2

  h is not injective, is surjective, is not bijective.

- Define $f\colon \{1,2,3\} \to \{1,2,3,4\}$ by

s	1	2	3
$f(s)$	3	2	1

  f is injective, is not surjective, f is not bijective.

- Define $q\colon \{1,2,3,4\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ by

τ	1	2	3	4
$q(\tau)$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$

  q is injective, is surjective, is bijective.

Properties of functions (cont'd)

- Can we ever rule out the existence of injections or surjections?

- Can we ever rule out the existence of injections or surjections?
- **Pigeonhole Principle:**

Let A and B be finite sets.

1. If $|A| < |B|$, then there can be no surjection from A to B.
2. If $|A| > |B|$, then there can be no injection from A to B.
3. If $|A| \neq |B|$, then there can be no bijection from A to B.

Pigeonhole Principle Example:

- Suppose we have five softball players, and four pre-existing softball teams.
  Then at least two of them will play on the same team.

Pigeonhole Principle Example:

- Suppose we have five softball players, and four pre-existing softball teams.
  Then at least two of them will play on the same team.
- Why? Let $S = \{\text{the softball players}\}$ and $T = \{\text{the teams}\}$.
  Define $p\colon S \to T$ by

$$p(s) \in T \text{ is the team on which } s \in S \text{ plays.}$$

Pigeonhole Principle Example:

- Suppose we have five softball players, and four pre-existing softball teams.
  Then at least two of them will play on the same team.
- Why? Let $S = \{\text{the softball players}\}$ and $T = \{\text{the teams}\}$.
  Define $p \colon S \to T$ by
  $$p(s) \in T \text{ is the team on which } s \in S \text{ plays.}$$
- Pigeonhole Principle: p cannot be an injection.

Pigeonhole Principle Example:

- Suppose we have five softball players, and four pre-existing softball teams.
  Then at least two of them will play on the same team.
- Why? Let $S = \{\text{the softball players}\}$ and $T = \{\text{the teams}\}$.
  Define $p\colon S \to T$ by
  $$p(s) \in T \text{ is the team on which } s \in S \text{ plays.}$$
- Pigeonhole Principle: p cannot be an injection.
- Thus, there exist distinct i and j such that $p(i) = p(j)$.

Properties of functions (cont'd)

Pigeonhole Principle Example:

- Suppose we have five softball players, and four pre-existing softball teams.
  Then at least two of them will play on the same team.
- Why? Let $S = \{\text{the softball players}\}$ and $T = \{\text{the teams}\}$.
  Define $p \colon S \to T$ by
  $$p(s) \in T \text{ is the team on which } s \in S \text{ plays.}$$
- Pigeonhole Principle: p cannot be an injection.
- Thus, there exist distinct i and j such that $p(i) = p(j)$.
- So players i and j must be on the same team. □

Pigeonhole Principle Example:

- Suppose that people in a room shake hands with some other people in the room.

Pigeonhole Principle Example:

- Suppose that people in a room shake hands with some other people in the room.
  Then at least two of these people will shake hands the same number of times.

Pigeonhole Principle Example:

- Suppose that people in a room shake hands with some other people in the room.
  Then at least two of these people will shake hands the same number of times.
- Why? Let $P = \{\text{people in the room}\}$.
  Let $n = |P|$, and define $f\colon P \to \{1, \ldots, n-1\}$ by
  $f(j) =$the number of people with whom $j \in P$ shakes hands
  (Note that you don't shake hands with yourself.)

Pigeonhole Principle Example:

- Suppose that people in a room shake hands with some other people in the room.
  Then at least two of these people will shake hands the same number of times.
- Why? Let $P = \{\text{people in the room}\}$.
  Let $n = |P|$, and define $f : P \to \{1, \ldots, n-1\}$ by
  $f(j) =$the number of people with whom $j \in P$ shakes hands
  (Note that you don't shake hands with yourself.)
- Pigeonhole Principle: f cannot be an injection.

Pigeonhole Principle Example:

- Suppose that people in a room shake hands with some other people in the room.
  Then at least two of these people will shake hands the same number of times.
- Why? Let $P = \{\text{people in the room}\}$.
  Let $n = |P|$, and define $f\colon P \to \{1, \ldots, n-1\}$ by

  $$f(j) = \text{the number of people with whom } j \in P \text{ shakes hands}$$

  (Note that you don't shake hands with yourself.)
- Pigeonhole Principle: f cannot be an injection.
- Thus, there exist distinct i and j such that $f(i) = f(j)$.

Pigeonhole Principle Example:

- Suppose that people in a room shake hands with some other people in the room.
  Then at least two of these people will shake hands the same number of times.
- Why? Let $P = \{\text{people in the room}\}$.
  Let $n = |P|$, and define $f : P \to \{1, \ldots, n-1\}$ by
  $f(j) =$the number of people with whom $j \in P$ shakes hands
  (Note that you don't shake hands with yourself.)
- Pigeonhole Principle: f cannot be an injection.
- Thus, there exist distinct i and j such that $f(i) = f(j)$.
- So persons i and j shake hands the same number of times. □

Function composition

- How to design a big piece of software?

Function composition

- How to design a big piece of software?
  - Word processor
  - Web browser
  - Kernel of an operating system

Function composition

- How to design a big piece of software?
  - Word processor
  - Web browser
  - Kernel of an operating system
- Decompose it into smaller “modules”, with well-defined communication channels
  - Loose coupling
  - High cohesion

Function composition

- How to design a big piece of software?
  - Word processor
  - Web browser
  - Kernel of an operating system
- Decompose it into smaller "modules", with well-defined communication channels
  - Loose coupling
  - High cohesion
- Other direction: design *software components* for reuse (*object-oriented design*)

Function composition

- How to design a big piece of software?
    - Word processor
    - Web browser
    - Kernel of an operating system
- Decompose it into smaller "modules", with well-defined communication channels
    - Loose coupling
    - High cohesion
- Other direction: design *software components* for reuse (*object-oriented design*)
- All this is part of *software engineering*.

Function composition (cont'd)

- **Example:** We want to compute a complicated function, such as $h\colon \mathbb{R} \to \mathbb{R}$ defined as

$$h(x) = (3x^2+2x+7)^{14}+32(3x^2+2x+7)^5-11(3x^2+2x+7)^3 \quad \forall\, x \in \mathbb{R}.$$

- **Example:** We want to compute a complicated function, such as $h\colon \mathbb{R} \to \mathbb{R}$ defined as

$$h(x) = (3x^2+2x+7)^{14}+32(3x^2+2x+7)^5-11(3x^2+2x+7)^3 \quad \forall\, x \in \mathbb{R}.$$

- Break up the calculation of $z = h(x)$ into two pieces:
  1. Calculate $y = 3x^2 + 2x + 7$.
  2. Calculate $z = y^{14} + 32y^5 - 11y^3$.

- **Example:** We want to compute a complicated function, such as $h\colon \mathbb{R} \to \mathbb{R}$ defined as

$$h(x) = (3x^2+2x+7)^{14}+32(3x^2+2x+7)^5-11(3x^2+2x+7)^3 \qquad \forall\, x \in \mathbb{R}.$$

- Break up the calculation of $z = h(x)$ into two pieces:
  1. Calculate $y = 3x^2 + 2x + 7$.
  2. Calculate $z = y^{14} + 32y^5 - 11y^3$.
- Write $y = f(x)$, where the $f\colon \mathbb{R} \to \mathbb{R}$ is defined as

$$f(x) = 3x^2 + 2x + 7 \qquad \forall\, x \in \mathbb{R}.$$

Function composition (cont'd)

- **Example:** We want to compute a complicated function, such as $h\colon \mathbb{R} \to \mathbb{R}$ defined as

$$h(x) = (3x^2+2x+7)^{14}+32(3x^2+2x+7)^5-11(3x^2+2x+7)^3 \qquad \forall\, x \in \mathbb{R}.$$

- Break up the calculation of $z = h(x)$ into two pieces:
  1. Calculate $y = 3x^2 + 2x + 7$.
  2. Calculate $z = y^{14} + 32y^5 - 11y^3$.
- Write $y = f(x)$, where the $f\colon \mathbb{R} \to \mathbb{R}$ is defined as
$$f(x) = 3x^2 + 2x + 7 \qquad \forall\, x \in \mathbb{R}.$$
- Write $z = g(y)$, where the function $g\colon \mathbb{R} \to \mathbb{R}$ is defined as
$$g(y) = y^{14} + 32y^5 - 11y^3 \qquad \forall\, y \in \mathbb{R}.$$

  Then
$$h(x) = g\big(f(x)\big) \qquad \forall\, x \in \mathbb{R}.$$

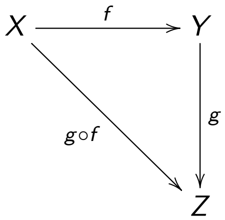
Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. The *composite function* $g \circ f\colon X \to Z$ is defined as

$$(g \circ f)(x) = g\big(f(x)\big) \qquad \forall\, x \in X.$$

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. The *composite function* $g \circ f\colon X \to Z$ is defined as

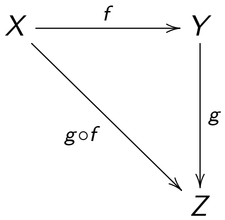
$$(g \circ f)(x) = g\big(f(x)\big) \qquad \forall x \in X.$$



Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. The *composite function* $g \circ f\colon X \to Z$ is defined as

$$(g \circ f)(x) = g\big(f(x)\big) \qquad \forall x \in X.$$



- Although we write $g \circ f$ and we read g before f when we say "g composed with f," we first calculate $y = f(x)$ and then $z = g(y)$ when we compute $z = g\big(f(x)\big)$.

Function composition (cont'd)

- The two functions must be compatible: Codomain of the first is (a subset of) domain of second.

Function composition (cont'd)

- The two functions must be compatible: Codomain of the first is (a subset of) domain of second.
- **Example:** Define $d\colon \mathbb{R} \to \mathbb{R}$ by

$$d(x) = 2x \qquad \forall\, x \in \mathbb{R}$$

and $p : \mathbb{Z} \to \mathbb{Z}$ by

$$p(x) = \begin{cases} 0 & \text{if } x \text{ is even,} \\ 1 & \text{if } x \text{ is odd.} \end{cases}$$

Function composition (cont'd)

- The two functions must be compatible: Codomain of the first is (a subset of) domain of second.
- **Example:** Define $d\colon \mathbb{R} \to \mathbb{R}$ by

$$d(x) = 2x \qquad \forall\, x \in \mathbb{R}$$

and $p : \mathbb{Z} \to \mathbb{Z}$ by

$$p(x) = \begin{cases} 0 & \text{if } x \text{ is even,} \\ 1 & \text{if } x \text{ is odd.} \end{cases}$$

Then $p \circ d$ is ill-defined—what's $(p \circ d)(\frac{1}{4})$?

Function composition (cont'd)

- The two functions must be compatible: Codomain of the first is (a subset of) domain of second.
- **Example:** Define $d\colon \mathbb{R} \to \mathbb{R}$ by

$$d(x) = 2x \qquad \forall\, x \in \mathbb{R}$$

and $p : \mathbb{Z} \to \mathbb{Z}$ by

$$p(x) = \begin{cases} 0 & \text{if } x \text{ is even,} \\ 1 & \text{if } x \text{ is odd.} \end{cases}$$

Then $p \circ d$ is ill-defined—what's $(p \circ d)(\frac{1}{4})$?
However $d \circ p\colon \mathbb{Z} \to \mathbb{R}$ *is* well-defined.

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

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

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

  Then $z = (g \circ f)(x)$.
- **Example:** Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x \qquad \text{and} \qquad g(x) = x + 1 \qquad \forall\, x \in \mathbb{R}.$$

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

  Then $z = (g \circ f)(x)$.
- **Example:** Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x \qquad \text{and} \qquad g(x) = x + 1 \qquad \forall\, x \in \mathbb{R}.$$

  We have

$$(f \circ g)(2) = f(g(2)) = f(2+1) = f(3) = 2 \times 3 = 6;$$

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

  Then $z = (g \circ f)(x)$.
- **Example:** Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x \qquad \text{and} \qquad g(x) = x + 1 \qquad \forall\, x \in \mathbb{R}.$$

We have

$$(f \circ g)(2) = f(g(2)) = f(2+1) = f(3) = 2 \times 3 = 6;$$

and

$$(g \circ f)(2) = g(f(2)) = f(2) + 1 = 2 \times 2 + 1 = 5;$$

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

  Then $z = (g \circ f)(x)$.
- **Example:** Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x \qquad \text{and} \qquad g(x) = x + 1 \qquad \forall\, x \in \mathbb{R}.$$

We have

$$(f \circ g)(2) = f(g(2)) = f(2+1) = f(3) = 2 \times 3 = 6;$$

and

$$(g \circ f)(2) = g(f(2)) = f(2) + 1 = 2 \times 2 + 1 = 5;$$

So $(f \circ g)(2) \neq (g \circ f)(2)$.

Function composition (cont'd)

- Let $f\colon X \to Y$ and $g\colon Y \to Z$. Computing the composite function $g \circ f$ at a point $x \in X$ is a two-step process:
  1. Compute $y = f(x)$.
  2. Compute $z = g(y)$.

  Then $z = (g \circ f)(x)$.
- **Example:** Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x \qquad \text{and} \qquad g(x) = x + 1 \qquad \forall\, x \in \mathbb{R}.$$

We have

$$(f \circ g)(2) = f(g(2)) = f(2+1) = f(3) = 2 \times 3 = 6;$$

and

$$(g \circ f)(2) = g(f(2)) = f(2) + 1 = 2 \times 2 + 1 = 5;$$

So $(f \circ g)(2) \neq (g \circ f)(2)$.
Function composition is not commutative!

Function composition (cont'd)

Example: Let P be the set of all people. Define functions $f\colon P \to P$ and $m\colon P \to P$ by

$$f(p) = \text{the (birth) father of } p \qquad \forall\, p \in P$$

and

$$m(p) = \text{the (birth) mother of } p \qquad \forall\, p \in P.$$

What is $m \circ m$? $m \circ f$? $f \circ m$? $f \circ f$?

Function composition (cont'd)

Example: Let P be the set of all people. Define functions $f\colon P \to P$ and $m\colon P \to P$ by

$$f(p) = \text{the (birth) father of } p \qquad \forall\, p \in P$$

and

$$m(p) = \text{the (birth) mother of } p \qquad \forall\, p \in P.$$

What is $m \circ m$? $m \circ f$? $f \circ m$? $f \circ f$?

Solution: We have $(m \circ m)(p) = m\bigl(m(p)\bigr)$, which is the mother of the mother of p, i.e.,

Function composition (cont'd)

Example: Let P be the set of all people. Define functions $f: P \to P$ and $m: P \to P$ by

$$f(p) = \text{the (birth) father of } p \qquad \forall\, p \in P$$

and

$$m(p) = \text{the (birth) mother of } p \qquad \forall\, p \in P.$$

What is $m \circ m$? $m \circ f$? $f \circ m$? $f \circ f$?

Solution: We have $(m \circ m)(p) = m\big(m(p)\big)$, which is the mother of the mother of p, i.e., the maternal grandmother of p.

Function composition (cont'd)

Example: Let P be the set of all people. Define functions $f\colon P \to P$ and $m\colon P \to P$ by

$$f(p) = \text{the (birth) father of } p \qquad \forall\, p \in P$$

and

$$m(p) = \text{the (birth) mother of } p \qquad \forall\, p \in P.$$

What is $m \circ m$? $m \circ f$? $f \circ m$? $f \circ f$?

Solution: We have $(m \circ m)(p) = m\bigl(m(p)\bigr)$, which is the mother of the mother of p, i.e., the maternal grandmother of p. Similarly, we find that

$$\begin{aligned} m \circ f &= \text{paternal grandmother}, \\ f \circ m &= \text{maternal grandfather}, \\ f \circ f &= \text{paternal grandfather}. \end{aligned}$$

Identity and inverse functions

- The *identity function* on a set A is the function $\mathrm{id}_A \colon A \to A$ defined by

$$\mathrm{id}_A(a) = a \qquad \forall\, a \in A$$

Identity and inverse functions

- The *identity function* on a set A is the function $\mathrm{id}_A \colon A \to A$ defined by
$$\mathrm{id}_A(a) = a \qquad \forall\, a \in A$$

- If $f \colon X \to Y$, then
$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$

Identity and inverse functions

- The *identity function* on a set A is the function $\mathrm{id}_A \colon A \to A$ defined by

$$\mathrm{id}_A(a) = a \qquad \forall\, a \in A$$

- If $f \colon X \to Y$, then

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$

- Why this name? Analogous to

$$a \times 1 = a = 1 \times a \qquad \forall\, a \in \mathbb{R}.$$

- **Example:** Let V be the set of all vowels. The identity function $\mathrm{id}_V \colon V \to V$ is given by

x	a	e	i	o	u
$\mathrm{id}_V(x)$	a	e	i	o	u

Identity and inverse functions (cont'd)

- **Example:** Let V be the set of all vowels. The identity function $\mathrm{id}_V \colon V \to V$ is given by

x	a	e	i	o	u
$\mathrm{id}_V(x)$	a	e	i	o	u

- **Example:** Let C be the set of all consonants. The identity function $\mathrm{id}_C \colon C \to C$ is similar:

x	b	c	d	f	...	z
$\mathrm{id}_C(x)$	b	c	d	f	...	z

- **Example:** Let V be the set of all vowels. The identity function $\mathrm{id}_V\colon V \to V$ is given by

x	a	e	i	o	u
$\mathrm{id}_V(x)$	a	e	i	o	u

- **Example:** Let C be the set of all consonants. The identity function $\mathrm{id}_C\colon C \to C$ is similar:

x	b	c	d	f	...	z
$\mathrm{id}_C(x)$	b	c	d	f	...	z

- Why do we care about a function that "does nothing"?

Identity and inverse functions (cont'd)

- The function $f\colon X \to Y$ is *invertible* if there exists another function $f^{-1}\colon Y \to X$ such that

$$f^{-1} \circ f = \mathrm{id}_X \qquad \text{and} \qquad f \circ f^{-1} = \mathrm{id}_Y,$$

i.e.,

$$\begin{aligned} f^{-1}\bigl(f(x)\bigr) &= x \qquad \forall\, x \in X \\ f\bigl(f^{-1}(y)\bigr) &= y \qquad \forall\, y \in Y. \end{aligned}$$

Identity and inverse functions (cont'd)

- The function $f\colon X \to Y$ is *invertible* if there exists another function $f^{-1}\colon Y \to X$ such that

$$f^{-1} \circ f = \mathrm{id}_X \qquad \text{and} \qquad f \circ f^{-1} = \mathrm{id}_Y,$$

  i.e.,

$$\begin{aligned} f^{-1}\big(f(x)\big) &= x \qquad \forall\, x \in X \\ f\big(f^{-1}(y)\big) &= y \qquad \forall\, y \in Y. \end{aligned}$$

- If f is invertible, then f^{-1} is the functional *inverse* of f.

Identity and inverse functions (cont'd)

- The function $f\colon X \to Y$ is *invertible* if there exists another function $f^{-1}\colon Y \to X$ such that

$$f^{-1} \circ f = \mathrm{id}_X \qquad \text{and} \qquad f \circ f^{-1} = \mathrm{id}_Y,$$

i.e.,

$$\begin{aligned} f^{-1}\big(f(x)\big) &= x \qquad \forall\, x \in X \\ f\big(f^{-1}(y)\big) &= y \qquad \forall\, y \in Y. \end{aligned}$$

- If f is invertible, then f^{-1} is the functional *inverse* of f.
- Don't confuse f^{-1} with a reciprocal $(1/f)$!

Identity and inverse functions (cont'd)

Example: Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by

$$g(x) = x - 7 \qquad \forall\, x \in \mathbb{Z}.$$

Show that $g^{-1}\colon \mathbb{Z} \to \mathbb{Z}$ is given by

$$g^{-1}(y) = y + 7 \qquad \forall\, y \in \mathbb{Z}.$$

Identity and inverse functions (cont'd)

Example: Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by

$$g(x) = x - 7 \qquad \forall\, x \in \mathbb{Z}.$$

Show that $g^{-1}\colon \mathbb{Z} \to \mathbb{Z}$ is given by

$$g^{-1}(y) = y + 7 \qquad \forall\, y \in \mathbb{Z}.$$

Solution: We have

$$\begin{aligned}(g \circ g^{-1})(y) &= g\big(g^{-1}(y)\big) = g(y+7) \\ &= (y+7) - 7 = y\end{aligned} \qquad \forall\, y \in \mathbb{Z}$$

Identity and inverse functions (cont'd)

Example: Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by

$$g(x) = x - 7 \qquad \forall\, x \in \mathbb{Z}.$$

Show that $g^{-1}\colon \mathbb{Z} \to \mathbb{Z}$ is given by

$$g^{-1}(y) = y + 7 \qquad \forall\, y \in \mathbb{Z}.$$

Solution: We have

$$\begin{aligned}(g \circ g^{-1})(y) &= g\big(g^{-1}(y)\big) = g(y+7) \\ &= (y+7) - 7 = y\end{aligned} \qquad \forall\, y \in \mathbb{Z}$$

and

$$\begin{aligned}(g^{-1} \circ g)(x) &= g^{-1}\big(g(x)\big) = g^{-1}(x-7) \\ &= (x-7) + 7 = x\end{aligned} \qquad \forall\, x \in \mathbb{Z}.$$

Identity and inverse functions (cont'd)

Example: Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by

$$g(x) = x - 7 \qquad \forall\, x \in \mathbb{Z}.$$

Show that $g^{-1}\colon \mathbb{Z} \to \mathbb{Z}$ is given by

$$g^{-1}(y) = y + 7 \qquad \forall\, y \in \mathbb{Z}.$$

Solution: We have

$$\begin{aligned}(g \circ g^{-1})(y) &= g\big(g^{-1}(y)\big) = g(y + 7) \\ &= (y + 7) - 7 = y\end{aligned} \qquad \forall\, y \in \mathbb{Z}$$

and

$$\begin{aligned}(g^{-1} \circ g)(x) &= g^{-1}\big(g(x)\big) = g^{-1}(x - 7) \\ &= (x - 7) + 7 = x\end{aligned} \qquad \forall\, x \in \mathbb{Z}.$$

So g^{-1} is the functional inverse of g, as claimed.

Identity and inverse functions (cont'd)

Not all functions are invertible, and the difference between invertibility and non-invertibility may be subtle.

- **Example:** Define $m\colon \mathbb{Q} \to \mathbb{Q}$ by

$$m(x) = 2x \qquad \forall\, x \in \mathbb{Q}.$$

  Is m invertible? If so, what is its inverse function?

Identity and inverse functions (cont'd)

Not all functions are invertible, and the difference between invertibility and non-invertibility may be subtle.

- **Example:** Define $m\colon \mathbb{Q} \to \mathbb{Q}$ by
$$m(x) = 2x \qquad \forall\, x \in \mathbb{Q}.$$
Is m invertible? If so, what is its inverse function?
- **Solution:** We need to solve the equation
$$y = m(x) = 2x$$
for x in terms of y:

Identity and inverse functions (cont'd)

Not all functions are invertible, and the difference between invertibility and non-invertibility may be subtle.

- **Example:** Define $m\colon \mathbb{Q} \to \mathbb{Q}$ by

$$m(x) = 2x \qquad \forall\, x \in \mathbb{Q}.$$

  Is m invertible? If so, what is its inverse function?

- **Solution:** We need to solve the equation

$$y = m(x) = 2x$$

  for x in terms of y:

$$y = 2x \iff x = \tfrac{1}{2}y.$$

  Now $y \in \mathbb{Q} \implies x = \frac{1}{2}y \in \mathbb{Q}$. Thus m is invertible, with $m^{-1}\colon \mathbb{Q} \to \mathbb{Q}$ given by

$$m^{-1}(y) = \tfrac{1}{2}y \qquad \forall\, y \in \mathbb{Q}. \quad \square$$

Identity and inverse functions (cont'd)

- **Example:** Define $\widetilde{m}\colon \mathbb{N} \to \mathbb{N}$ by

$$\widetilde{m}(x) = 2x \qquad \forall\, x \in \mathbb{N}.$$

Is $\widetilde{m}$ invertible? If so, give its inverse function.

Identity and inverse functions (cont'd)

- **Example:** Define $\widetilde{m}\colon \mathbb{N} \to \mathbb{N}$ by

$$\widetilde{m}(x) = 2x \qquad \forall\, x \in \mathbb{N}.$$

  Is $\widetilde{m}$ invertible? If so, give its inverse function.

- **Solution:** We need to solve the equation

$$y = \widetilde{m}(x) = 2x$$

  for x in terms of y:

Identity and inverse functions (cont'd)

- **Example:** Define $\widetilde{m}\colon \mathbb{N} \to \mathbb{N}$ by

$$\widetilde{m}(x) = 2x \qquad \forall\, x \in \mathbb{N}.$$

  Is $\widetilde{m}$ invertible? If so, give its inverse function.

- **Solution:** We need to solve the equation

$$y = \widetilde{m}(x) = 2x$$

  for x in terms of y:

$$y = 2x \iff x = \tfrac{1}{2}y.$$

Identity and inverse functions (cont'd)

- **Example:** Define $\widetilde{m}\colon \mathbb{N} \to \mathbb{N}$ by

$$\widetilde{m}(x) = 2x \qquad \forall\, x \in \mathbb{N}.$$

  Is $\widetilde{m}$ invertible? If so, give its inverse function.

- **Solution:** We need to solve the equation

$$y = \widetilde{m}(x) = 2x$$

  for x in terms of y:

$$y = 2x \iff x = \tfrac{1}{2}y.$$

  Does $y \in \mathbb{N} \implies x = \frac{1}{2}y \in \mathbb{N}$?

- **Example:** Define $\widetilde{m}\colon \mathbb{N} \to \mathbb{N}$ by

$$\widetilde{m}(x) = 2x \qquad \forall\, x \in \mathbb{N}.$$

Is $\widetilde{m}$ invertible? If so, give its inverse function.

- **Solution:** We need to solve the equation

$$y = \widetilde{m}(x) = 2x$$

for x in terms of y:

$$y = 2x \iff x = \tfrac{1}{2}y.$$

Does $y \in \mathbb{N} \implies x = \frac{1}{2}y \in \mathbb{N}$?
No! For example, take $y = 1$, getting $x = \frac{1}{2}$.

Identity and inverse functions (cont'd)

- **Example:** Define $\widetilde{m} \colon \mathbb{N} \to \mathbb{N}$ by

$$\widetilde{m}(x) = 2x \qquad \forall\, x \in \mathbb{N}.$$

  Is $\widetilde{m}$ invertible? If so, give its inverse function.

- **Solution:** We need to solve the equation

$$y = \widetilde{m}(x) = 2x$$

  for x in terms of y:

$$y = 2x \iff x = \tfrac{1}{2}y.$$

  Does $y \in \mathbb{N} \implies x = \frac{1}{2}y \in \mathbb{N}$?
  No! For example, take $y = 1$, getting $x = \frac{1}{2}$.
  So $\widetilde{m}$ is *not* invertible.

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?
- **Fact:** The function $f\colon X \to Y$ is invertible if and only if f is a bijection.

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?
- **Fact:** The function $f\colon X \to Y$ is invertible if and only if f is a bijection.
- **Explanation:** Substitute $f(x) = y$ into $x = f^{-1}(f(x))$, finding

$$x = f^{-1}(y) \iff y = f(x).$$

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?
- **Fact:** The function $f\colon X \to Y$ is invertible if and only if f is a bijection.
- **Explanation:** Substitute $f(x) = y$ into $x = f^{-1}(f(x))$, finding

$$x = f^{-1}(y) \iff y = f(x).$$

  This gives a relation $f^{-1}\colon Y \to X$. Is it a function?

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?
- **Fact:** The function $f\colon X \to Y$ is invertible if and only if f is a bijection.
- **Explanation:** Substitute $f(x) = y$ into $x = f^{-1}(f(x))$, finding

$$x = f^{-1}(y) \iff y = f(x).$$

  This gives a relation $f^{-1}\colon Y \to X$. Is it a function?
- For any $y \in Y$, there must *exist* a *unique* $x \in X$ such that $x = f^{-1}(y)$, i.e., such that $y = f(x)$.
  - *Uniqueness* holds iff f is an injection.

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?
- **Fact:** The function $f\colon X \to Y$ is invertible if and only if f is a bijection.
- **Explanation:** Substitute $f(x) = y$ into $x = f^{-1}(f(x))$, finding

$$x = f^{-1}(y) \iff y = f(x).$$

  This gives a relation $f^{-1}\colon Y \to X$. Is it a function?
- For any $y \in Y$, there must *exist* a *unique* $x \in X$ such that $x = f^{-1}(y)$, i.e., such that $y = f(x)$.
  - *Uniqueness* holds iff f is an injection.
    If $y = f(x)$ and also $y = f(x')$, we wouldn't know whether we should use x or x' as the value of $f^{-1}(y)$.

Identity and inverse functions (cont'd)

- So how can we determine whether a given function is invertible?
- **Fact:** The function $f\colon X \to Y$ is invertible if and only if f is a bijection.
- **Explanation:** Substitute $f(x) = y$ into $x = f^{-1}(f(x))$, finding

$$x = f^{-1}(y) \iff y = f(x).$$

  This gives a relation $f^{-1}\colon Y \to X$. Is it a function?
- For any $y \in Y$, there must *exist* a *unique* $x \in X$ such that $x = f^{-1}(y)$, i.e., such that $y = f(x)$.
  - *Uniqueness* holds iff f is an injection.
    If $y = f(x)$ and also $y = f(x')$, we wouldn't know whether we should use x or x' as the value of $f^{-1}(y)$.
  - *Existence* holds iff for any $y \in Y$, there exists some $x \in X$ such that $f(x) = y$, i.e., iff f is a surjection.

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- A function from the set $\{1, 2, 3, \ldots, 999\}$ to the set $\{1, 2, 3, \ldots, 999, 1000\}$.

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- A function from the set $\{1, 2, 3, \ldots, 999\}$ to the set $\{1, 2, 3, \ldots, 999, 1000\}$.
  No! (Pigeonhole principle: no such function is an surjection.)

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- A function from the set $\{1, 2, 3, \ldots, 999\}$ to the set $\{1, 2, 3, \ldots, 999, 1000\}$.
  No! (Pigeonhole principle: no such function is an surjection.)
- The function $q\colon \{1, 2, 3, 4\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ defined by

τ	1	2	3	4
$q(\tau)$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- A function from the set $\{1, 2, 3, \dots, 999\}$ to the set $\{1, 2, 3, \dots, 999, 1000\}$.
  No! (Pigeonhole principle: no such function is an surjection.)
- The function $q\colon \{1, 2, 3, 4\} \to \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ defined by

τ	1	2	3	4
$q(\tau)$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$

  Yes. q is a bijection. In fact its inverse is the function $q^{-1}\colon \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\} \to \{1, 2, 3, 4\}$ defined by

s	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
$q^{-1}(s)$	4	3	2	1

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- The function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- The function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not a surjection, since (e.g.) there is no $x \in \mathbb{R}$ such that $f(x) = -1$.

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- The function $f\colon \mathbb{R} \to \mathbb{R}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not a surjection, since (e.g.) there is no $x \in \mathbb{R}$ such that $f(x) = -1$.

- The function $f\colon \mathbb{R} \to \mathbb{R}^{\geq 0}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- The function $f \colon \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not a surjection, since (e.g.) there is no $x \in \mathbb{R}$ such that $f(x) = -1$.

- The function $f \colon \mathbb{R} \to \mathbb{R}^{\geq 0}$ defined by

$$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not an injection, since $f(1) = 1$ and $f(-1) = 1$.

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- The function $f\colon \mathbb{R} \to \mathbb{R}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not a surjection, since (e.g.) there is no $x \in \mathbb{R}$ such that $f(x) = -1$.
- The function $f\colon \mathbb{R} \to \mathbb{R}^{\geq 0}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not an injection, since $f(1) = 1$ and $f(-1) = 1$.
- The function $f\colon \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

Identity and inverse functions (cont'd)

Which of the following functions are invertible?

- The function $f\colon \mathbb{R} \to \mathbb{R}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not a surjection, since (e.g.) there is no $x \in \mathbb{R}$ such that $f(x) = -1$.

- The function $f\colon \mathbb{R} \to \mathbb{R}^{\geq 0}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  No. f is not an injection, since $f(1) = 1$ and $f(-1) = 1$.

- The function $f\colon \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ defined by

  $$f(x) = x^2 \qquad \forall\, x \in \mathbb{R}.$$

  Yes! Its inverse is the function $f^{-1}\colon \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ defined by

  $$f^{-1}(y) = \sqrt{y} \qquad \forall\, y \in \mathbb{R}^{\geq 0}.$$

Identity and inverse functions (cont'd)

One last example: Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by

$$g(s) = 4s - 3 \qquad \forall\, s \in \mathbb{R}\,.$$

Let's find an explicit formula for $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.

- By definition, we know that $s = g^{-1}(t)$ is equivalent to $t = g(s)$.

Identity and inverse functions (cont'd)

One last example: Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by

$$g(s) = 4s - 3 \qquad \forall\, s \in \mathbb{R}\,.$$

Let's find an explicit formula for $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.

- By definition, we know that $s = g^{-1}(t)$ is equivalent to $t = g(s)$.
- If we solve the equation

  $$t = g(s) = 4s - 3$$

  for s in terms of t, then $s = g^{-1}(t)$.

Identity and inverse functions (cont'd)

One last example: Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by

$$g(s) = 4s - 3 \qquad \forall\, s \in \mathbb{R}\,.$$

Let's find an explicit formula for $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.

- By definition, we know that $s = g^{-1}(t)$ is equivalent to $t = g(s)$.
- If we solve the equation

  $$t = g(s) = 4s - 3$$

  for s in terms of t, then $s = g^{-1}(t)$.
- Using simple algebra, we have

  $$t = 4s - 3$$

Identity and inverse functions (cont'd)

One last example: Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by

$$g(s) = 4s - 3 \qquad \forall\, s \in \mathbb{R}\,.$$

Let's find an explicit formula for $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.

- By definition, we know that $s = g^{-1}(t)$ is equivalent to $t = g(s)$.
- If we solve the equation

  $$t = g(s) = 4s - 3$$

  for s in terms of t, then $s = g^{-1}(t)$.
- Using simple algebra, we have

  $$t = 4s - 3 \iff t + 3 = 4s$$

Identity and inverse functions (cont'd)

One last example: Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by

$$g(s) = 4s - 3 \qquad \forall\, s \in \mathbb{R}\,.$$

Let's find an explicit formula for $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.

- By definition, we know that $s = g^{-1}(t)$ is equivalent to $t = g(s)$.
- If we solve the equation

  $$t = g(s) = 4s - 3$$

  for s in terms of t, then $s = g^{-1}(t)$.
- Using simple algebra, we have

  $$t = 4s - 3 \iff t + 3 = 4s \iff s = \tfrac{1}{4}(t + 3)\,.$$

Identity and inverse functions (cont'd)

One last example: Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by

$$g(s) = 4s - 3 \qquad \forall\, s \in \mathbb{R}\,.$$

Let's find an explicit formula for $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.

- By definition, we know that $s = g^{-1}(t)$ is equivalent to $t = g(s)$.
- If we solve the equation

  $$t = g(s) = 4s - 3$$

  for s in terms of t, then $s = g^{-1}(t)$.
- Using simple algebra, we have

  $$t = 4s - 3 \iff t + 3 = 4s \iff s = \tfrac{1}{4}(t+3)\,.$$

- Thus $g^{-1}\colon \mathbb{R} \to \mathbb{R}$ is given by the rule

  $$g^{-1}(t) = \tfrac{1}{4}(t+3) \qquad \forall\, t \in \mathbb{R}\,.$$

Identity and inverse functions (cont'd)

Suppose $f\colon X \to Y$ is invertible.
How to find $f^{-1}\colon Y \to X$?

Identity and inverse functions (cont'd)

Suppose $f\colon X \to Y$ is invertible.
How to find $f^{-1}\colon Y \to X$?
Recall that

$$x = f^{-1}(y) \qquad \text{if and only if} \qquad y = f(x).$$

Identity and inverse functions (cont'd)

Suppose $f\colon X \to Y$ is invertible.
How to find $f^{-1}\colon Y \to X$?
Recall that

$$x = f^{-1}(y) \qquad \text{if and only if} \qquad y = f(x).$$

Follow these steps:

1. Write down the equation $y = f(x)$ or (equivalently) $f(x) = y$.

Identity and inverse functions (cont'd)

Suppose $f\colon X \to Y$ is invertible.
How to find $f^{-1}\colon Y \to X$?
Recall that

$$x = f^{-1}(y) \qquad \text{if and only if} \qquad y = f(x).$$

Follow these steps:

1. Write down the equation $y = f(x)$ or (equivalently) $f(x) = y$.
2. Solve the equation $f(x) = y$ for x in terms of y, checking that

   - there must be exactly one solution that gives x in terms of y, and
   - for any $y \in Y$, the resulting x value must be an element of X.

Identity and inverse functions (cont'd)

Suppose $f\colon X \to Y$ is invertible.
How to find $f^{-1}\colon Y \to X$?
Recall that

$$x = f^{-1}(y) \qquad \text{if and only if} \qquad y = f(x).$$

Follow these steps:

1. Write down the equation $y = f(x)$ or (equivalently) $f(x) = y$.
2. Solve the equation $f(x) = y$ for x in terms of y, checking that
    - there must be exactly one solution that gives x in terms of y, and
    - for any $y \in Y$, the resulting x value must be an element of X.

You'll now have something of the form

$$x = \text{some expression involving } y.$$

Identity and inverse functions (cont'd)

Suppose $f\colon X \to Y$ is invertible.
How to find $f^{-1}\colon Y \to X$?
Recall that

$$x = f^{-1}(y) \qquad \text{if and only if} \qquad y = f(x).$$

Follow these steps:

1. Write down the equation $y = f(x)$ or (equivalently) $f(x) = y$.
2. Solve the equation $f(x) = y$ for x in terms of y, checking that
   - there must be exactly one solution that gives x in terms of y, and
   - for any $y \in Y$, the resulting x value must be an element of X.

You'll now have something of the form

$$x = \text{some expression involving } y.$$

This expression on the right-hand side is precisely $f^{-1}(y)$.

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f)$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f$$

Inverse of composite functions

Fact: Let $f: A \to B$ and $g: B \to C$ be invertible functions. Then $g \circ f: A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1})$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1}$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_B \circ g^{-1}$$

Inverse of composite functions

Fact: Let $f: A \to B$ and $g: B \to C$ be invertible functions. Then $g \circ f: A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \text{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \text{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \text{id}_B \circ f = f^{-1} \circ f = \text{id}_A$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \text{id}_B \circ g^{-1} = g \circ g^{-1}$$

Inverse of composite functions

Fact: Let $f\colon A \to B$ and $g\colon B \to C$ be invertible functions. Then $g \circ f\colon A \to C$ is invertible, with

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Why? We need to show that

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A \qquad \text{and} \qquad (g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C\,.$$

But

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_B \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C\,. \quad \square$$

Inverse of composite functions (cont'd)

Example: Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x + 7 \text{ and } g(x) = x^3 - 8 \qquad \forall\, x \in \mathbb{R}.$$

Inverse of composite functions (cont'd)

Example: Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x + 7 \text{ and } g(x) = x^3 - 8 \qquad \forall\, x \in \mathbb{R}.$$

You may (should?) check that f and g are both invertible, with

$$f^{-1}(y) = \tfrac{1}{2}(y - 7) \text{ and } g^{-1}(y) = \sqrt[3]{y + 8} \qquad \forall\, y \in \mathbb{R}.$$

Inverse of composite functions (cont'd)

Example: Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x + 7 \text{ and } g(x) = x^3 - 8 \qquad \forall\, x \in \mathbb{R}.$$

You may (should?) check that f and g are both invertible, with

$$f^{-1}(y) = \tfrac{1}{2}(y - 7) \text{ and } g^{-1}(y) = \sqrt[3]{y + 8} \qquad \forall\, y \in \mathbb{R}.$$

Thus $g \circ f\colon \mathbb{R} \to \mathbb{R}$ is invertible, with

$$(g \circ f)^{-1}(y) = (f^{-1} \circ g^{-1})(y) = f^{-1}\big(g^{-1}(y)\big)$$

Example: Define $f, g \colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x + 7 \text{ and } g(x) = x^3 - 8 \qquad \forall\, x \in \mathbb{R}.$$

You may (should?) check that f and g are both invertible, with

$$f^{-1}(y) = \tfrac{1}{2}(y - 7) \text{ and } g^{-1}(y) = \sqrt[3]{y + 8} \qquad \forall\, y \in \mathbb{R}.$$

Thus $g \circ f \colon \mathbb{R} \to \mathbb{R}$ is invertible, with

$$\begin{aligned}(g \circ f)^{-1}(y) &= (f^{-1} \circ g^{-1})(y) = f^{-1}\bigl(g^{-1}(y)\bigr) \\ &= f^{-1}(\sqrt[3]{y + 8})\end{aligned}$$

Example: Define $f, g\colon \mathbb{R} \to \mathbb{R}$ by

$$f(x) = 2x + 7 \text{ and } g(x) = x^3 - 8 \qquad \forall\, x \in \mathbb{R}.$$

You may (should?) check that f and g are both invertible, with

$$f^{-1}(y) = \tfrac{1}{2}(y - 7) \text{ and } g^{-1}(y) = \sqrt[3]{y + 8} \qquad \forall\, y \in \mathbb{R}.$$

Thus $g \circ f\colon \mathbb{R} \to \mathbb{R}$ is invertible, with

$$\begin{aligned}(g \circ f)^{-1}(y) = (f^{-1} \circ g^{-1})(y) &= f^{-1}\big(g^{-1}(y)\big) \\ = f^{-1}(\sqrt[3]{y + 8}) &= \tfrac{1}{2}(\sqrt[3]{y + 8} - 7)\end{aligned}$$

Inverse of composite functions (cont'd)

- This extends to compositions of any number of functions, e.g.,

$$(f \circ g \circ h)^{-1} = h^{-1} \circ g^{-1} \circ f^{-1}.$$

Inverse of composite functions (cont'd)

- This extends to compositions of any number of functions, e.g.,

$$(f \circ g \circ h)^{-1} = h^{-1} \circ g^{-1} \circ f^{-1}.$$

- To undo a sequence of steps, undo all the steps, *but in reverse order*.

Inverse of composite functions (cont'd)

- This extends to compositions of any number of functions, e.g.,

$$(f \circ g \circ h)^{-1} = h^{-1} \circ g^{-1} \circ f^{-1}.$$

- To undo a sequence of steps, undo all the steps, *but in reverse order*.
- Useful in Alice, Part III (unmelting the snow woman).

An example: cryptography

Consider the following scenarios:

- When you purchase an item from an e-business, you submit (among other things) a credit card number.
  If this information is intercepted when it is transmitted to the online store, you are a prime candidate for identity theft.

An example: cryptography

Consider the following scenarios:

- When you purchase an item from an e-business, you submit (among other things) a credit card number.
  If this information is intercepted when it is transmitted to the online store, you are a prime candidate for identity theft.
- A military officer needs to send battle plans to his troops.
  If the plans are intercepted and the enemy reads the plans, the battle (and perhaps the war) will be lost.

An example: cryptography

Consider the following scenarios:

- When you purchase an item from an e-business, you submit (among other things) a credit card number.
  If this information is intercepted when it is transmitted to the online store, you are a prime candidate for identity theft.
- A military officer needs to send battle plans to his troops.
  If the plans are intercepted and the enemy reads the plans, the battle (and perhaps the war) will be lost.

These are problems in computational cryptography, which deals with the problem of hiding information from people who shouldn't see it.

An example: cryptography (cont'd)

Julius Caesar needed to securely send military messages to his troops. Given the original *cleartext*, he created a *ciphertext* by replacing each letter by the one that comes three positions later in alphabetical order (*Caesar rotation*). This defines a encoding function $e\colon \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\}$, defined by the table

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

An example: cryptography (cont'd)

Julius Caesar needed to securely send military messages to his troops. Given the original *cleartext*, he created a *ciphertext* by replacing each letter by the one that comes three positions later in alphabetical order (*Caesar rotation*). This defines a encoding function $e\colon \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$, defined by the table

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Corresponding decoding function $d\colon \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$ is the inverse of the encoding function:

$$e\bigl(d(x)\bigr) = x \qquad \text{and} \qquad d\bigl(e(x)\bigr) = x$$

for any $x \in \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$. More succinctly,

$$e \circ d = \mathrm{id}_{\{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}} = d \circ e.$$

An example: cryptography (cont'd)

For Caesar rotation $e\colon \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\}$ is

An example: cryptography (cont'd)

For Caesar rotation $e\colon \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\}$ is

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$d(y)$	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

An example: cryptography (cont'd)

For Caesar rotation $e\colon \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$ is

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$d(y)$	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

("swap the rows").

For Caesar rotation $e\colon \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \to \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \to \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}$ is

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$d(y)$	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

("swap the rows").
For example, `ATTACK AT NOON` encodes as

An example: cryptography (cont'd)

For Caesar rotation $e\colon \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \to \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \to \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}$ is

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$d(y)$	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

("swap the rows").
For example, `ATTACK AT NOON` encodes as `DWWDFN DW QRRQ`.

An example: cryptography (cont'd)

For Caesar rotation $e\colon \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \to \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$ is

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$d(y)$	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

("swap the rows").
For example, `ATTACK AT NOON` encodes as `DWWDFN DW QRRQ`.

- If an enemy were to see this message and if he didn't know the secret, he'd simply dismiss it as gibberish.

An example: cryptography (cont'd)

For Caesar rotation $e\colon \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \to \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$e(x)$	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

decoding function $d\colon \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \to \{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\}$ is

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$d(y)$	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

("swap the rows").

For example, `ATTACK AT NOON` encodes as `DWWDFN DW QRRQ`.

- If an enemy were to see this message and if he didn't know the secret, he'd simply dismiss it as gibberish.
- But Caesar's forces (who had already been told what the encoding and decoding methods were), *would* be able to decode it!

An example: cryptography (cont'd)

- What about setting up e-commerce website?

An example: cryptography (cont'd)

- What about setting up e-commerce website?
- Sensitive information can be snooped if sent in plaintext. Must encrypt!

An example: cryptography (cont'd)

- What about setting up e-commerce website?
- Sensitive information can be snooped if sent in plaintext. Must encrypt!
- Let C_{plain} be the set of plaintext credit card numbers and C_{cipher} be the set of ciphertext credit card numbers.

An example: cryptography (cont'd)

- What about setting up e-commerce website?
- Sensitive information can be snooped if sent in plaintext. Must encrypt!
- Let C_{plain} be the set of plaintext credit card numbers and C_{cipher} be the set of ciphertext credit card numbers.
- We want an encoding function $\text{Enc}\colon C_{\text{plain}} \to C_{\text{cipher}}$ and a decoding function $\text{Dec}\colon C_{\text{cipher}} \to C_{\text{plain}}$, which is the inverse of Enc

An example: cryptography (cont'd)

- What about setting up e-commerce website?
- Sensitive information can be snooped if sent in plaintext. Must encrypt!
- Let C_{plain} be the set of plaintext credit card numbers and C_{cipher} be the set of ciphertext credit card numbers.
- We want an encoding function $\text{Enc}\colon C_{\text{plain}} \to C_{\text{cipher}}$ and a decoding function $\text{Dec}\colon C_{\text{cipher}} \to C_{\text{plain}}$, which is the inverse of Enc
- Security? Even if the details of computing Enc were to leak out, it must be hard for a Bad Guy to compute Dec.

An example: cryptography (cont'd)

- What about setting up e-commerce website?
- Sensitive information can be snooped if sent in plaintext. Must encrypt!
- Let C_{plain} be the set of plaintext credit card numbers and C_{cipher} be the set of ciphertext credit card numbers.
- We want an encoding function $\text{Enc}\colon C_{\text{plain}} \to C_{\text{cipher}}$ and a decoding function $\text{Dec}\colon C_{\text{cipher}} \to C_{\text{plain}}$, which is the inverse of Enc
- Security? Even if the details of computing Enc were to leak out, it must be hard for a Bad Guy to compute Dec.
- Can we do this?

An example: cryptography (cont'd)

- Good news: we know how to build an $(\mathsf{Enc}, \mathsf{Dec})$ pair that we believe is reasonably secure.

An example: cryptography (cont'd)

- Good news: we know how to build an (Enc, Dec) pair that we believe is reasonably secure.
- Based on simple idea:
  - Multiplication and factorization are (more-or-less) inverse operations.

An example: cryptography (cont'd)

- Good news: we know how to build an (Enc, Dec) pair that we believe is reasonably secure.
- Based on simple idea:
  - Multiplication and factorization are (more-or-less) inverse operations.
  - We know how to quickly multiply two large (e.g., 100-digit) numbers. Can multiply two n-digit numbers in time proportional to n^2.

An example: cryptography (cont'd)

- Good news: we know how to build an (Enc, Dec) pair that we believe is reasonably secure.
- Based on simple idea:
  - Multiplication and factorization are (more-or-less) inverse operations.
  - We know how to quickly multiply two large (e.g., 100-digit) numbers. Can multiply two n-digit numbers in time proportional to n^2.
  - Nobody knows how to quickly factor a large (e.g., 200-digit) number. All known algorithms require time that's exponential in the number of digits.

An example: cryptography (cont'd)

- Good news: we know how to build an (Enc, Dec) pair that we believe is reasonably secure.
- Based on simple idea:
  - Multiplication and factorization are (more-or-less) inverse operations.
  - We know how to quickly multiply two large (e.g., 100-digit) numbers. Can multiply two n-digit numbers in time proportional to n^2.
  - Nobody knows how to quickly factor a large (e.g., 200-digit) number. All known algorithms require time that's exponential in the number of digits.

No "security through obscurity"!

An example: cryptography (cont'd)

- Good news: we know how to build an (Enc, Dec) pair that we believe is reasonably secure.
- Based on simple idea:
  - Multiplication and factorization are (more-or-less) inverse operations.
  - We know how to quickly multiply two large (e.g., 100-digit) numbers. Can multiply two n-digit numbers in time proportional to n^2.
  - Nobody knows how to quickly factor a large (e.g., 200-digit) number. All known algorithms require time that's exponential in the number of digits.

  No "security through obscurity"!
- This does *not* mean that these techniques are provably secure!
  - Nobody knows how to do fast factorization.
  - Nobody has ever proved that fast factorization is impossible!

More about functions

Where else do functions crop up in computer science?

Standard mathematical functions Here's a partial list of functions you may have encountered:

math name	UNIX name	description
$\sqrt{\ }$	`sqrt`	square root
$\sin$	`sin`	trigonometric sine
$\cos$	`cos`	trigonometric cosine
$\tan$	`tan`	trigonometric tangent
$\sin^{-1}$	`asin`	trigonometric arc (inverse) sine
$\cos^{-1}$	`acos`	trigonometric arc cosine
$\tan^{-1}$	`atan`	trigonometric arc tangent
$\exp$	`exp`	exponential function
$\ln$	`log`	natural logarithm
$\lvert \cdot \rvert$	`fabs`	absolute value

More about functions (cont'd)

Standard mathematical functions (cont'd) You may be less familiar with the following:

- The max function. If x and y are numbers, then $\max(x, y)$ is the maximum of x and y. For example, $\max(2.3, -4.2) = 2.3$.

Standard mathematical functions (cont'd) You may be less familiar with the following:

- The max function. If x and y are numbers, then $\max(x, y)$ is the maximum of x and y. For example, $\max(2.3, -4.2) = 2.3$.
- The min function. If x and y are numbers, then $\min(x, y)$ is the minimum of x and y. For example, $\min(2.3, -4.2) = -4.2$.

More about functions (cont'd)

Standard mathematical functions (cont'd) You may be less familiar with the following:

- The max function. If x and y are numbers, then $\max(x, y)$ is the maximum of x and y. For example, $\max(2.3, -4.2) = 2.3$.
- The min function. If x and y are numbers, then $\min(x, y)$ is the minimum of x and y. For example, $\min(2.3, -4.2) = -4.2$.
- The ceiling function. If x is a number, then $\lceil x \rceil$ is the smallest integer that is greater than or equal to x. For example, $\lceil 4.001 \rceil = 5$.

More about functions (cont'd)

Standard mathematical functions (cont'd) You may be less familiar with the following:

- The max function. If x and y are numbers, then $\max(x, y)$ is the maximum of x and y. For example, $\max(2.3, -4.2) = 2.3$.
- The min function. If x and y are numbers, then $\min(x, y)$ is the minimum of x and y. For example, $\min(2.3, -4.2) = -4.2$.
- The ceiling function. If x is a number, then $\lceil x \rceil$ is the smallest integer that is greater than or equal to x. For example, $\lceil 4.001 \rceil = 5$.
- The floor function. If x is a number, then $\lfloor x \rfloor$ is the largest integer that is less than or equal to x. For example, $\lfloor 4.999 \rfloor = 4$.

More about functions (cont'd)

Standard mathematical functions (cont'd) You may be less familiar with the following:

- The max function. If x and y are numbers, then $\max(x, y)$ is the maximum of x and y. For example, $\max(2.3, -4.2) = 2.3$.
- The min function. If x and y are numbers, then $\min(x, y)$ is the minimum of x and y. For example, $\min(2.3, -4.2) = -4.2$.
- The ceiling function. If x is a number, then $\lceil x \rceil$ is the smallest integer that is greater than or equal to x. For example, $\lceil 4.001 \rceil = 5$.
- The floor function. If x is a number, then $\lfloor x \rfloor$ is the largest integer that is less than or equal to x. For example, $\lfloor 4.999 \rfloor = 4$.

The names of these functions, as found in the UNIX standard library, are `fmax`, `fmin`, `ceil`, and `floor`.

More about functions (cont'd)

Growth functions: Used to measure efficiency of algorithms.
Typically a function $f : \mathbb{Z} \to \mathbb{Z}$, with

$$f(n) = \text{cost of using algorithm to solve problem with input size } n$$

More about functions (cont'd)

Growth functions: Used to measure efficiency of algorithms.
Typically a function $f : \mathbb{Z} \to \mathbb{Z}$, with

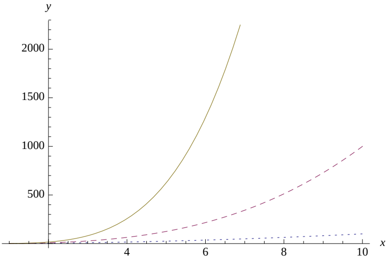
$$f(n) = \text{cost of using algorithm to solve problem with input size } n$$

Here are some standard growth functions:

function	name
$\log n$	logarithmic
n	linear
$n \log n$	(no commonly-accepted name)
n^2	quadratic
n^3	cubic
2^n	exponential
$n!$	factorial

Growth functions (cont'd):

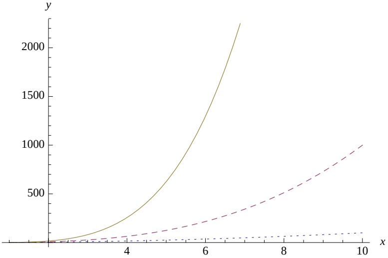
Let's do some graphing.

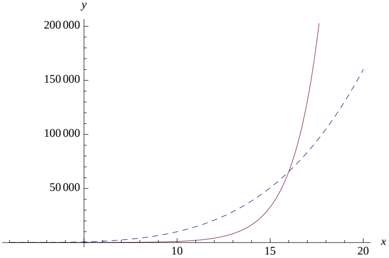


$y = x^2$ $y = x^3$ $y = x^4$

Growth functions (cont'd):

Let's do some graphing.



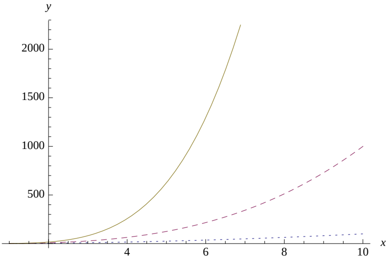


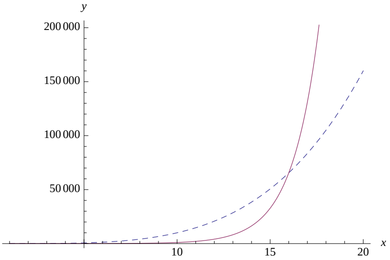
$y = x^2$ $y = x^3$ $y = x^4$

$y = x^4$ $y = 2^x$

Growth functions (cont'd):

Let's do some graphing.





$y = x^2$ $\quad$ $y = x^3$ $\quad$ $y = x^4$ $\qquad$ $y = x^4$ $\quad$ $y = 2^x$

Breakpoint (between tractable and intractable problems): polynomial vs. exponential

More about functions (cont'd)

Functions in program construction
Functions are ubiquitous in the design and implementation of computer programs. For starters, functions are the main building block for many computer programming languages. For instance, every executable C or C++ program will have a function named `main`, which is the starting point for program execution.

More about functions (cont'd)

Functions in program construction

Functions are ubiquitous in the design and implementation of computer programs. For starters, functions are the main building block for many computer programming languages. For instance, every executable C or C++ program will have a function named `main`, which is the starting point for program execution.

An example in C++:

```
#include <iostream>

int main()
{
   std::cout << "Hello, world!\n";
}
```

Functions in program construction (cont'd):

Look at the following:

```
int main()
{
   do_initialization();
   do {
      data = get_input_data();
      result = process_data(data);
      put_result(result);
      still_working = more_to_process();
   } while (still_working);
   do_cleanup();
}
```

More about functions (cont'd)

Functions in program construction (cont'd): This particular `main` function involves other functions. Note the following points:

- This is a syntactically correct C++ (or C) `main` function.
- This could be the `main` function for almost *any* text-based task.
- `main` involves other functions. These can be written by other programmers. In fact, they themselves can involve (sub)functions, and so on. Can use this "functional decomposition" to split the work amongst a team of programmers.
- At each stage, we have a working system (without all the features).
- When functions are fully fleshed out, we have a complete working system.
- This approach can make testing a lot easier.

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.
- Key ingredient: An *encryption function* $f : S \to S$, where S is the set of all possible character strings.

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.
- Key ingredient: An *encryption function* $f : S \to S$, where S is the set of all possible character strings.
- Properties of f?

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.
- Key ingredient: An *encryption function* $f : S \to S$, where S is the set of all possible character strings.
- Properties of f?
  - f must be an injection.

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.
- Key ingredient: An *encryption function* $f : S \to S$, where S is the set of all possible character strings.
- Properties of f?
  - f must be an injection.
  - f must be easy to compute.

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.
- Key ingredient: An *encryption function* $f : S \to S$, where S is the set of all possible character strings.
- Properties of f?
  - f must be an injection.
  - f must be easy to compute.
  - $f : S \to \text{Range}(S)$ must be hard to invert. That is, given an encrypted password e, computing the plaintext password $f^{-1}(e)$ must be prohibitively expensive.

An application: secure storage of passwords

- UNIX uses an encryption scheme to store passwords.
- Key ingredient: An *encryption function* $f : S \to S$, where S is the set of all possible character strings.
- Properties of f?
  - f must be an injection.
  - f must be easy to compute.
  - $f : S \to \text{Range}(S)$ must be hard to invert. That is, given an encrypted password e, computing the plaintext password $f^{-1}(e)$ must be prohibitively expensive.
- System stores each user's encrypted password in a world-readable file.

An application: secure storage of passwords (cont'd)

- When trying to log in, user presents login ID and purported password $\tilde{p}$.

An application: secure storage of passwords (cont'd)

- When trying to log in, user presents login ID and purported password $\tilde{p}$.
- System computes $\tilde{e} = f(\tilde{p})$.

An application: secure storage of passwords (cont'd)

- When trying to log in, user presents login ID and purported password $\tilde{p}$.
- System computes $\tilde{e} = f(\tilde{p})$.
- System compares $\tilde{e}$ with actual encrypted password e.

An application: secure storage of passwords (cont'd)

- When trying to log in, user presents login ID and purported password $\tilde{p}$.
- System computes $\tilde{e} = f(\tilde{p})$.
- System compares $\tilde{e}$ with actual encrypted password e.
- User is allowed in if and only if $\tilde{e} = e$.

An application: secure storage of passwords (cont'd)

- If f isn't injective, user might be admitted upon presenting an incorrect password (a "synonym").

An application: secure storage of passwords (cont'd)

- If f isn't injective, user might be admitted upon presenting an incorrect password (a "synonym").
- If f cannot be computed quickly, login process takes too long.

An application: secure storage of passwords (cont'd)

- If f isn't injective, user might be admitted upon presenting an incorrect password (a "synonym").
- If f cannot be computed quickly, login process takes too long.
- If f^{-1} can be computed quickly, then a Bad Guy could compute plaintext password, given the encrypted password.

An application: secure storage of passwords (cont'd)

Note the following:

An application: secure storage of passwords (cont'd)

Note the following:

- Exhaustive search isn't an option for Bad Guys, since search space is too big. For instance, if using a password of length from 4 through 8 in the standard 95-character ASCII character set, there are

$$\sum_{j=4}^{8} 95^j = 6{,}704{,}780{,}953{,}650{,}625$$

  possible passwords; if you could check one billion per second, this would take about 78 days to check.

An application: secure storage of passwords (cont'd)

Note the following:

- Exhaustive search isn't an option for Bad Guys, since search space is too big. For instance, if using a password of length from 4 through 8 in the standard 95-character ASCII character set, there are

$$\sum_{j=4}^{8} 95^j = 6{,}704{,}780{,}953{,}650{,}625$$

  possible passwords; if you could check one billion per second, this would take about 78 days to check.
- Exhaustive search over a subspace *is* an option.

An application: secure storage of passwords (cont'd)

Note the following:

- Exhaustive search isn't an option for Bad Guys, since search space is too big. For instance, if using a password of length from 4 through 8 in the standard 95-character ASCII character set, there are

$$\sum_{j=4}^{8} 95^j = 6{,}704{,}780{,}953{,}650{,}625$$

  possible passwords; if you could check one billion per second, this would take about 78 days to check.
- Exhaustive search over a subspace *is* an option.
  - If you only use lower-case letters, there are only 217,180,128,880 passwords, which we could check in about 200 seconds.

An application: secure storage of passwords (cont'd)

Note the following:

- Exhaustive search isn't an option for Bad Guys, since search space is too big. For instance, if using a password of length from 4 through 8 in the standard 95-character ASCII character set, there are

$$\sum_{j=4}^{8} 95^j = 6{,}704{,}780{,}953{,}650{,}625$$

  possible passwords; if you could check one billion per second, this would take about 78 days to check.
- Exhaustive search over a subspace *is* an option.
  - If you only use lower-case letters, there are only 217,180,128,880 passwords, which we could check in about 200 seconds.
  - A *dictionary attack* can break passwords in (e.g.) English (or French or Urdu).

An application: secure storage of passwords (cont'd)

Note the following:

- Exhaustive search isn't an option for Bad Guys, since search space is too big. For instance, if using a password of length from 4 through 8 in the standard 95-character ASCII character set, there are

$$\sum_{j=4}^{8} 95^j = 6{,}704{,}780{,}953{,}650{,}625$$

  possible passwords; if you could check one billion per second, this would take about 78 days to check.
- Exhaustive search over a subspace *is* an option.
  - If you only use lower-case letters, there are only 217,180,128,880 passwords, which we could check in about 200 seconds.
  - A *dictionary attack* can break passwords in (e.g.) English (or French or Urdu).

The moral of the story: choose good passwords!