מתמטיקה בדידה
Discrete Math

Lecture 5

Last week: Functions

$$f : A \to B$$

Definition: A function, f, from set A to set B associates an element $f(a) \in B$ with an element $a \in A$.

We require that for every $a \in A$ there exists a single $b \in B$ so that $f(a) = b$

That is: $\forall a \in A, \forall b,b' \in B,$

$$(f(a)=b) \wedge (f(a)=b') \to b=b'$$

Last week: Summary

We say a function f: A → B is

Total if every $a \in A$ is assigned to some $b \in B$ (and partial otherwise).

Surjective if every $b \in B$ is mapped to *at least once*.

Injective if every $b \in B$ is mapped to *at most once*.

Bijective iff it is all of the above:

1. Total
2. Onto (על)
3. 1-1 (חד חד ערכית)

Formally

Definition: The domain of definition of f: A → B is the set A' ⊆ A defined as A' := {a ∈ A | ∃b ∈ B: [b=f(a)]}.

Definition: A function f: A → B is said to be partial if A' ⊂ A.

Definition: A function f: A → B is said to be total if A' = A.

Definition: A function f: A → B is onto iff for every b ∈ B, there exists a ∈ A such that b=f(a) (∀b ∈ B,∃a ∈ A : [b=f(a)]).

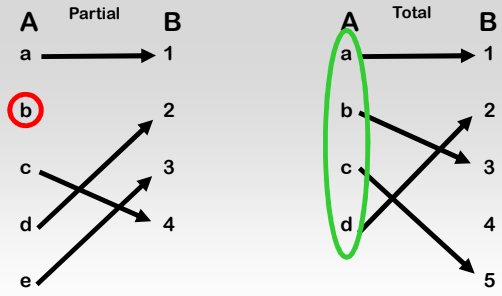
Definition: A function f: A → B is 1-1 iff for all x,y ∈ A, f(x) = f(y) implies x = y (∀x,y ∈ A : [f(x) = f(y) ⟶ x = y]).

The Mapping Rule

Lemma:

- If f: A → B is onto, then |A| ≥ |B|.
- If f: A → B is total and 1-1, then |A| ≤ |B|.
- If f: A → B is a bijection, then |A| = |B|.

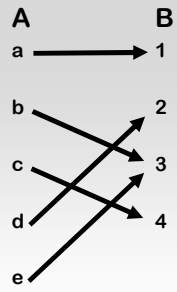
Partial vs. Total



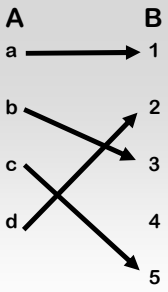
Total – exactly one arrow out of every element in A!

Onto vs. 1-1

Onto but not 1-1



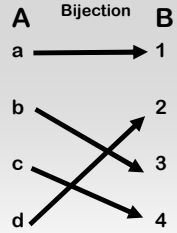
1-1 but not onto

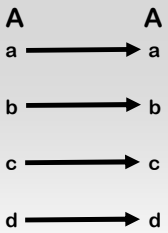


$f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ $f(x) = x^2$ $f : \mathbb{N} \to \mathbb{N}$ $f(x) = 2x$

Bijection (total, onto and 1-1)

Bijection





Identity function on A: $i_A: A \to A$ $i_A(x) = x$

The Graph of a Function

Everything about a function f is captured by 3 sets:

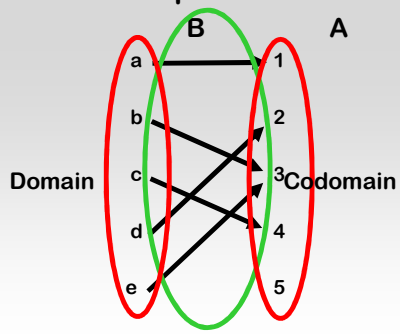
1. The domain A,
2. the codomain B,
3. the graph of f

$$\{(a,b) \mid f(a)=b\}$$

To tell if a function is

1. total we also need to know the domain
2. surjective we also need to know the codomain
3. 1-1 we need to know the graph

The Graph of a Function



The Graph corresponds to the arrows

Formal Definition of a Function

Definition: A function f from a set A to a set B is a set

$$f \subseteq A \times B$$

so that $\forall a \in A, \forall b,b' \in B$,

if $(a,b) \in f$ AND $(a,b') \in f$ then b=b'

(For every $a \in A$, there exists a *unique* $b \in B$ so that $(a,b) \in f$.)

(**Recall**: $A \times B = \{(a,b) \mid a \in A, b \in B\}$)

Functions: Composition

Definition: The composition of functions

$$g: A \to B \quad \text{and} \quad f: B \to C$$

is a new function $f \circ g$: $A \to C$ defined as:

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

Can be thought of as:

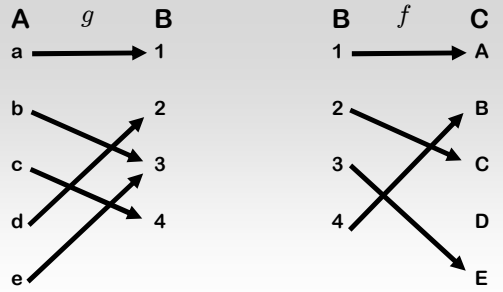
$$a \overset{g}{\mapsto} b \overset{f}{\mapsto} c$$

Note:

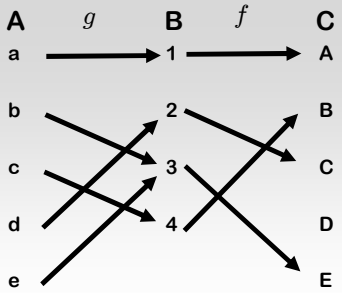
1. Defined only if Image(g) $\subseteq$ Domain of definition(f)
2. Very often, $f \circ g$ is defined, but $g \circ f$ is not

Composition הרכבה

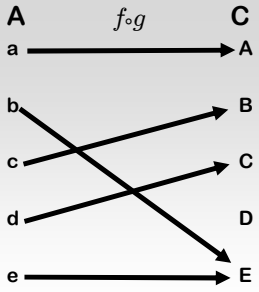
Function Composition



Function Composition



Function Composition



Function Composition: Example 1

g: $\mathbb{N} \to \mathbb{N}$ defined as $g(x) = x + 1$

f: $\mathbb{N} \to \mathbb{N}$ defined as $f(x) = x^2$

$f \circ g$: $\mathbb{N} \to \mathbb{N}$ is defined as $(f \circ g)(x) = f(g(x))$
$= f(x+1)$
$= (x+1)^2$

$g \circ f$: $\mathbb{N} \to \mathbb{N}$ is defined as $(g \circ f)(x) = g(f(x))$
$= g(x^2)$
$= x^2 + 1$

Function Composition: Example 2

g: $\mathtt{Evens} \to \mathbb{N}$ defined as $g(x) = x/2$

f: $\mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = x+1$

$f \circ g$: $\mathtt{Evens} \to \mathbb{Z}$ is defined as $(f \circ g)(x) = f(g(x))$
$= f(x/2)$
$= x/2+1$

$g \circ f$: $\mathbb{Z} \to \mathtt{Evens}$ is <u>not</u> defined! $(g \circ f)(x) = g(f(x))$
$= g(x+1)$
$= (x+1)/2$

x+1 is not necessarily even!

Function Composition: Properties

Let f: C $\to$ D, g: B $\to$ C, h: A $\to$ B

<u>Associativity</u>: $f \circ (g \circ h) = (f \circ g) \circ h$ (so we can write $f \circ g \circ h$)

<u>Commutativity</u>: <u>Not</u> always true that $f \circ g = g \circ f$

Some Special Cases

Associativity: when f: A $\to$ A,

- $f \circ f \circ \ldots \circ f = f^n$
- $f^0 = i_A$

Commutativity:

1. Let f: A $\to$ A, then for n,m$\in \mathbb{N}^+$

$$f^n \circ f^m = f^m \circ f^n$$

$$f^3 \circ f^4 = f \circ f \circ f \circ f \circ f \circ f \circ f$$

2. Let f: A $\to$ B, then $f \circ i_A = f$ and $i_B \circ f = f$

So if f: A $\to$ A, then $f \circ i_A = i_A \circ f = f$

Function Composition: Properties

Proposition: There exist two functions f: B $\to$ C, g: A $\to$ B such that $f \circ g \neq g \circ f$.

Proof: Take $g: \mathbb{N} \to \mathbb{N}$ defined as $g(x) = x + 1$ and $f: \mathbb{N} \to \mathbb{N}$ defined as $f(x) = x^2$. Then $f \circ g(1) = 4$ is not equal to $g \circ f(1) = 2$. QED

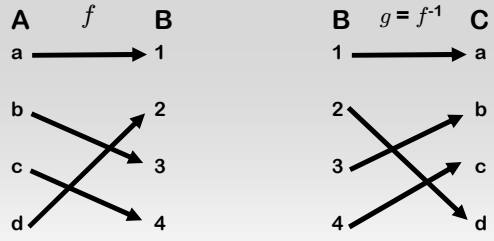
Proposition: For every three functions f: C $\to$ D, g: B $\to$ C, and h: A $\to$ B, it holds that $f \circ (g \circ h) = (f \circ g) \circ h$.

Proof: On the board.

Exercise: Let f: A $\to$ B and g: B $\to$ C and suppose that $g \circ f$ is onto. Then, g is also onto.

Proof: On the board.

Inverse function



Informally: An inverse for f:A$\to$B is a function g:B$\to$A such that if y = f (x) then x = g (y). It is denoted by $g = f^{-1}$

Inverse function הפונקציה ההפוכה

Inverse Function: Example

$f: \mathbb{N} \to \text{Evens}$ $f(x) = 2x$

$g: \text{Evens} \to \mathbb{N}$ $g(x) = x/2$

$f \circ g = i_{\text{Evens}}$

$g \circ f = i_{\mathbb{N}}$

Note: An inverse function does not always exist.

$f: \mathbb{R} \to \mathbb{R}$ $f(x) = x^2$

Does not have an inverse.

Left Inverse and Right Inverse

Let f: A $\to$ B be a function

- A left inverse for f is a function g: B $\to$ A such that

  $g \circ f = i_A$

  That is, if $f(x) = y$ then $g(y) = x$.

- A right inverse for f is a function h: B $\to$ A such that

  $f \circ h = i_B$

  That is, if $h(y) = x$ then $f(x) = y$.

Left inverse הופכי שמאלי
Right inverse הופכי ימני

Left Inverse and Right Inverse 2

Claim 1: A function f: A $\to$ B has a left inverse iff it is 1-1.

Claim 2: A function f: A $\to$ B has a right inverse iff it is onto.

Proofs: On the board.

To show that a function is 1-1: show that it has a left inverse.

To show that a function is onto: show that it has a right inverse.

Bijection and Inverse

Theorem: A function f: A → B is a bijection if and only if there exists a function g: B → A such that

$$f \circ g = i_B$$

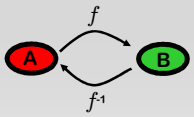
$$g \circ f = i_A$$

moreover, if such a function exists, it is unique.

Definition: If f: A → B is a bijection, then the unique function from above is called the inverse function of f. It is denoted by f^{-1}.

To show that a function is a bijection: show that it has an inverse

Bijection and Inverse 2



Facts: If f: A → B is a bijection then

1. f^{-1}: B → A.
2. $f \circ f^{-1} = i_B$ and $f^{-1} \circ f = i_A$
3. $\forall x \in A, \forall y \in B,\ y = f(x)$ if and only if $x = f^{-1}(y)$

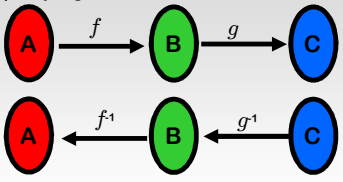
Claim: If f: A → B is a bijection then

1. f^{-1}: B → A is also a bijection
2. $(f^{-1})^{-1} = f$.

Bijection and Inverse 3

Claim: If f: A → B and g: B → C are bijections, then

1. $g \circ f$ is a bijection
2. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.



Corollary: If f: A → A is a bijection, then $(f^{-1})^n = (f^n)^{-1}$.

Counting

0)20480135385502964448038	31710048321735013941130 17	57632573310834796474093 98	82473310000429953116460 21
48944599186691567624099 2	32082344215973686470192 65	58009491235489891226286 63	84962439971234759227663 10
10826620324303796513709 81	34372546563551578648691 13	60429008011992802180260 01	85183991406760026607474 77
11784808947697061789949 93	35748833939305865392371 1365	61161717891373738967014 05	85436912834701914523337 63
12531273516832396938513 27	36449099460404801899691 49	61448689730015823697235 12	86753092583741370924613 52
13015051292340778110690 11	37900441327370840944172 46	62473145938511692347461 52	86943211123639968672966 65
13115671111438664338821 94	38703321274379713553228 15	68144289442668749634882 74	87723212036084772458511 54
14700294527212035876862 14	40805058045778014513631 00	68708529455438868491478 81	87914221617225825463410 91
15782710472862574994338 86	41672834610257023481249 20	69149555081209500937323 97	90626280245921262839732 85
16382439218521762431923 54	42359968311237778821124 9	69496324513659871524235 41	91378455669255263498977 94
17635802191319859631023 65	46709394457494390421112 20	71282111436136198284156 50	91537629668031892919344 19
18262277956018422310296 94	48153793518653842796134 27	71739200836518623079253 94	92708801940776364069842 49
18439718626751020372012 20	48370529482129226044421 90	72156548742117556762205 87	93243014807221034903792 04
23969511937221345261772 37	51063894238550185506715 30	72569328471643910402330 50	94360908321466951471405 81
27813945682685998019963 54	51423681920047692180699 10	73328226570752354316203 17	94753081597345382490132 38
27966051967136104054080 19	51812340961301440840418 56	74264418295415734449641 39	94923766239174869749232 02
29310163947619752631903 47	51982673981256179943913 48	76321981265318093271863 21	95119725587798802882529 79
29334580582944051551972 96	53175929403162312197583 72	77121544322119128823105 11	96024134246191871125522 64
30755144104909759203153 48	53843581267717941283569 47	78589186642402623566100 10	96312171149061292194611 11
31114749852527934528600 17	54392117122489019955423 441	78981567867632129631786 79	99081898531027533359813 19
31456215879361201184387 01	56103798260928381927604 58	81475910170375733378486 16	99132374763417642998139 87
31489012556288811031985 49	56323175554652286776760 44	81494367168713711619320 35	
31576931053251112843219 93	56921683746370196174237 12	81760638316825365713067 91	

90 numbers – A = $\{a_1, a_2, \ldots, a_{90}\}$
25 digits each - $a_i \in \{0,\ldots,9\}^{25}$

Q: Are there two subsets of the numbers that have the same sum?
For example, is sum of numbers in 1st column equal to sum of numbers in 2nd column?

The Subset Sum Problem

Q: Are there two subsets that have the same sum?

That is, are there $S_1, S_2 \subseteq \{1,\ldots,90\}$ so that

$$\sum_{i \in S_1} a_i = \sum_{i \in S_2} a_i$$

Why is the problem interesting?

1. Optimization - packing boxes in shipping containers.
2. Cryptography - decoding secret messages.
3. and much more...

Finding two such subsets seems to be very hard.*
Counting helps us decide if there *is* such a pair.

*Note: # subsets of A = 2^{90}

Why Count?

Very useful in computer science:

1. How much time/storage is required to solve a problem.
2. Counting is the basis for probability theory.
3. Useful proof techniques (e.g., pigeonhole principle).

Examples:

1. How many comparisons are needed to sort n numbers?
2. How many multiplications to compute d^n?
3. How many configurations to Rubik's cube?
4. How many different chess positions after n moves?
5. How many ways to select 12 balls w/ 5 different colors?
6. How many 16-bit numbers with exactly 4 ones?