Properties of functions

Lecture 13
ICOM 4075
Further concepts

Definition: Let $R$ be a relation that is a function.

Given a subset $C$ of $A$, the set

$$R(C) = \{b \in B: b = R(a) \text{ some } a \in C\}$$

is called **image of $C$ under $R$**

The set $R(A)$ is called **range** of $R$

Given a subset $D$ of $B$, the set

$$R^{-1}(D) = \{a \in A: (a, b) \in R \text{ for some } b \in D\}$$

is called **pre-image of $D$ under $R$**

$R$ is said to be **onto** if $B = R(A)$
Let’s illustrate image and pre-image with Venn diagrams

**Image \( R(\mathcal{C}) \):**

**Pre-image \( R^{-1}(\mathcal{D}) \):**
Illustration with sets

Let’s consider floor : Real $\rightarrow$ Integer

• Let $C = \{-1.2, 2.3, 4.01, 10.7\}$

  Then,

  $$\text{floor}(C) = \{-2, 2, 4, 10\}$$

  is the image of $C$ under floor.

• Let $D = \{1, 2\}$. Then,

  $$\text{floor}^{-1}(D) = \{x : x \text{ real and } 1 \leq x < 3\} = [1, 3).$$

• Since $\text{floor}(\text{Real}) = \text{Integers}$, floor is onto.
Let’s consider $R(n, 6) = n \mod 6$

- Let $C = \{0, 2, 4, 6, 8, 10, 12\}$
  
  Then,
  
  $R(C) = \{0, 2, 4\}$

  is the image of $C$.

- Let $D = \{0, 3\}$
  
  $R^{-1}(D) = \{x: x$ natural and $x = 6k$ or $x = 6k+3\}$

- $R(\text{natural}) = \{0, 1, 2, 3, 4, 5\}$ (not onto)
Properties of the composition of functions

The composition of two functions $f$ and $g$, when possible, is a function

The composition of functions is:

— Associative
This is, $(f \circ g) \circ h = f \circ (g \circ h)$

— Non-commutative
This is, in general, $f \circ g \neq g \circ f$
The identity function

Definition: Let $A$ be a set. The identity function over $A$ is defined as the function $id_A: A \to A$, $id_A(x) = x$.

The identity is always defined and composing a function with an identity returns the function.

—This is, if $f: A \to B$ is a function, then $f \circ id_A = id_B \circ f = f$
f: $A \rightarrow B$ and its two compositions with the identity:
Injections

**Definition:** A function $f : A \rightarrow B$ is said to be **injective** (or one-to-one) if it associates different elements in $A$ with different elements in $B$

More formally, $f$ is injective if and only if

$$a \neq b \text{ implies } f(a) \neq f(b)$$

**Observation:** Don’t confuse this property with property b) in the definition of function
In injective function, for all $a, b$: $f(a) \neq f(b)$.

In non-injective function, there is $a, b$ such that $f(a) = f(b)$. 
Examples

Injective
The mathematical formula \( f(x) = 5x + 3 \) is an injective function, with type
\[ f: \text{Real} \rightarrow \text{Real} \]
The graph of this function is a straight line with slope 5. Thus, each \( x \) is associated with a unique value \( y = 5x + 3 \)

Note: Any function whose graph is a straight line with slope different from zero, is injective

Not injective
The function floor is not injective
A counterexample is enough to prove this claim:
Let \( a = 3.5 \) and \( b = 3.7 \). Then \( a \neq b \) but
\[
\text{floor}(3.5) = \text{floor}(3.7) = 3
\]
**Bijections and inverses**

**Definition**: A function that is **injective and onto** is said to be a **bijection**

**Definition**: Let $f: A \rightarrow B$ be a function. Then, the relation $\text{Inv} = \{(y, x): y = f(x)\}$, is called **inverse relation** of $f$

**Property**: Let $f$ be a bijection. Then, the inverse relation of $f$ is also a function. This function is called **inverse of $f$** and it is denoted $f^{-1}$
Examples

The mathematical formula \( f(x) = 5x + 3 \) is a bijective function, since it is injective and onto (\( f(\text{Real}) = \text{Real} \))

The function floor is not bijective since it is not injective

Is onto because for each \( y \), there is always an \( x \) such that \( y = 5x + 3 \)
Tracing back an output

Given the **output** of a function, can you determine **what was the input**?

**An example:** The function is \( f(x) = 5x + 3 \). Assume that \( y=18 \) is an output. What is \( x \)? The answer is easy to compute:

\[
5x + 3 = 18, \\
5x = 15, \text{ and thus,} \\
x = 3
\]

**A counterexample:** \( \text{floor}(x) = 2 \), What is \( x \)? It is not possible to answer this question. There are infinitely many choices for \( x \). The input is not retrievable from the output (unless it has been stored separately).
Finding inverses

Finding the inverse of a mathematical function (this is, a formula) may be involved. The next example illustrate a generic method for computing the inverse of a function.

**Illustration**: Find the inverse of $f( x ) = 5x + 3$

**Method**: Make $y = 5x + 3$ and clear $y$. This yields

$$x = \frac{( y - 3 )}{5}$$

The inverse is $f^{-1}( y ) = \frac{( y - 3 )}{5}$
Property of inverse functions

**Property**: Let \( f : A \rightarrow B \) be a bijection. Then, the composition of \( f \) and its inverse is an identity function. This is,

\[
f \circ f^{-1} = \text{id}_B \quad \text{and} \quad f^{-1} \circ f = \text{id}_A
\]

This property may be used to check the correctness of the inverse formula. For example:

To verify that the inverse of \( f(x)=5x+3 \) is \( f^{-1}(y)=(y-3)/5 \) we do:

\[
\begin{align*}
  f \circ f^{-1}(y) &= f((y-3)/5) = 5((y-3)/5) + 3 = y = \text{id}_B \\
  f^{-1} \circ f(x) &= f^{-1}(5x + 3) = ((5x+3) - 3)/5 = x = \text{id}_A
\end{align*}
\]
Given natural numbers $n$, $a$ and $b$ we define:

$$f: \{0,1,\ldots,n-1\} \rightarrow \{0,1,\ldots,n-1\},$$

$$f(x) = ax + b \mod n$$

Is $f$ a bijection?

Let’s check a couple of examples:

- Let $n = 5$, $a = 2$ and $b = 3$. The table of values of $f(x) = 2x + 3 \mod 5$ is

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

As the table shows, the function $f(x) = 2x + 3 \mod 5$ is indeed a bijection.
More examples (cont.)

- Let \( n = 6, a = 2, \) and \( b = 3. \) The function is now \( f(x) = 2x + 3 \mod 6 \)

The table of values is

<table>
<thead>
<tr>
<th>( x )</th>
<th>( f(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

This function **is not a bijection**

**Theorem:** Given natural numbers \( n, a \) and \( b, \) the function

\[
f: \{0, \ldots, n-1\} \rightarrow \{0, \ldots, n-1\}
\]

\( f(x) = ax + b \mod n \)

is a bijection if and only if \( \gcd(a, n) = 1 \)

In the examples:
First example \( \gcd(2, 5) = 1 \)
Second example \( \gcd(2, 6) = 2 \)
Thus, given natural numbers $n$, $a$ and $b$ such that $\gcd(a, n) = 1$, the mapping $f(x) = ax + b$ is invertible. Let’s compute the inverse:

Let’s put $y = ax + b \mod n$

Step 1: $y - b = ax \mod n$

Step 2: ????????

Problem is we cannot divide by $a$. However, as we will see next, the condition $\gcd(a, n) = 1$ ensures the existence of a number $c$ in $\{1, \ldots, n-1\}$ such that $c \cdot a = 1 \mod n$
Compute the inverse of $f(x) = 2x + 3 \mod 5$

Step 1: $y = 2x + 3 \mod 5$

Step 2: $y - 3 = 2x \mod 5$

Step 3: Find $c$ in $\{1, 2, 3, 4\}$ such that

$$c \cdot 2 = 1 \mod 5$$

Let’s do this by exhaustion: $1 \cdot 2 = 2 \mod 5,$

$$2 \cdot 2 = 4 \mod 5, \quad 3 \cdot 2 = 1 \mod 5 \rightarrow \text{stop the search: } c = 3.$$  

Step 4: Multiply both sides by $c = 3$

$$2 \cdot (y - 3) = 2 \cdot 2x \mod 5 = x \mod 5$$

The inverse is $f^{-1}(y) = 2(y - 3) \mod 5$
Composition of injective and/or onto mappings

The injectivity and surjectivity of functions is preserved under composition. This is:

• If $f$ and $g$ are injective, then $g \circ f$ is injective

• If $f$ and $g$ are onto, then $g \circ f$ is onto

• If $f$ and $g$ are bijective, the $g \circ f$ is bijective
Summary

- Image, pre-image of sets
- Onto functions
- Composition of functions
- Identity map
- Injections, bijections and inverses
- Finding inverses
- Composition of injective, onto, and bijective mappings
Exercises

1. Find an inductive constructor for each of the following sets:
   a) \{x \text{ natural: } \text{ceil}(x/2) \text{ is even}\}
   b) \{x \text{ natural: } x \text{ mod } 6 = 1\}
Exercises

2. Let $T = (V, E)$ be a tree. Consider the function defined by $f(v) = \text{set of all descendents of } v$.
   a. Write the type of $f$
   b. Show that $f$ is a bijection
   c. Define the inverse of $f$. This is, give its type and formula.

3. Let $S$ be a nonempty set. Consider the function defined by $f(A) = \text{list of elements in } A$, where $A$ is a finite subset of $S$.
   a) Write the type of $f$.
   b) Show that $f$ is injective but not onto
   c) Show that if $f$ is defined as: $f(A) = \text{list of elements in } A$, where $A$ is a finite bag of elements in $S$, then $f$ is a bijection.
   d) Define the inverse of $f$, when $f$ is defined as in c)
Exercises

4. Let S be a set and A and B finite subsets of S. Consider the functions:
   I. \( \text{sum(numbers)} = \) sum of the numbers
   II. \( \text{count(A)} = \) number of elements in A
   III. \( \text{int(A, B)} = \) intersection of A and B
   IV. \( \text{uni(A, B)} = \) union of A and B
   V. \( \text{dif(A, B)} = \) difference of A and B

Then,

a) Write the type of each of the previous functions

b) Express each the counting rules for
   \( A \cup B, A \cup B \cup C, A - B, \) and \( A - (B \cap C) \)
   as compositions of the previous functions

c) For each of these compositions: are they injective? Are they onto?