15 151

Mathematical Foundations for Computer Science

Functions

$$f : U \to N$$

Outline

Question

Suppose we have a RNG $\mathscr{R}$ that will give us a random number in $[n]$ (each with equal probability). We'd really like a RNG f that will give us a random number in $\{0,1,\ldots,n-1\}$ instead. How can we get this?

Answer

Suppose R is a value that $\mathscr{R}$ has generated.There are a lot of possible answers. Here's two of them:

- $f(R) = R - 1$
- $f(R) = n - R$

Important Take-Aways

- The possible inputs and possible outputs are part of the function definition itself.
- A function is a "map" that assigns **a single output** to each input.

To define a function, we need to specify three things:

Domain	The set of possible inputs.
Co-Domain	The set of possible outputs.
Operation	The "rule" that maps the inputs to the outputs.

We can specify the first two of these by writing:

$$f : A \to B$$

("Define f as a function from A to B")

We have two options to define the operation: a rule and a program

One Rule to Define Them All

Defining a function via "a rule" is what you've seen before. For instance, to define the function f from the previous slide, we could do:

$$\begin{array}{rccc} f: & [n] & \to & [n-1] \cup \{0\} \\ & R & \mapsto & R-1 \end{array}$$

Note that $\to$ and $\mapsto$ are different arrows! The first defines the type of a function and the second defines the rule.

We can also define functions on the reals. Like...

$$\begin{array}{rccc} g: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & x^2+1 \end{array}$$

We can also define the "operation" part of the function by writing a program.

Define $f : \mathbb{N} \to \mathscr{P}(\mathbb{N})$ by

```
f(x) :=
    S := ∅
    for i → x:
        if even(i):
            S := S ∪ {i}
    return S
```

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

Definition (Image)

We define the **image of X under f** as

$$\text{img}_f(X) = \{f(x) \mid x \in X\}$$

That is, $\text{img}_f(X)$ is "the set of outputs pointed to by something in X."

So, since A is the domain, $\text{img}_f(A)$ is all of the achievable outputs of f.

Note that $\text{img}_f(A) \subseteq B$ is always true, but it is not necessarily the case that $\text{img}_f(A) = B$.

One more thing: you may have seen the term "range" before. Unfortunately, some high schools use "range" to mean codomain and others use it to mean $\text{img}_f(A)$. So, we will not use this term.

Let S be an arbitrary and fixed set. We give one more function definition:

Definition (Identity Function)

The Identity Function on the set S is defined as

$$\begin{aligned} I_S : \quad S &\to S \\ x &\mapsto x \end{aligned}$$

Outline

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

Definition (Totality)

We say f is **total** iff

$$\forall (x \in A).\, \exists (y \in B).\, y = f(x)$$

Informally, f is total if there is **at least** one output for each input.

Unless otherwise specified, we will assume that totality is a pre-requisite to being a function. That is, if f is not total, then it is not a function.

Definition (Single-valuedness)

We say that f is **single valued** iff

$$\forall (x \in A).\, \forall (y_1, y_2 \in B).\, ((f(x) = y_1 \wedge f(x) = y_2) \implies y_1 = y_2)$$

Informally, f is single valued if there is **at most** one output for each input.

If f is not single-valued, then f is not a function.

Question

Imagine we have a friend who has given us a function $g : \mathbb{N} \to \mathbb{N}$. He claims that if we give him $g(N)$ for some $N \in \mathbb{N}$, he can tell us what N originally was. Can he?

Answer

It depends on g.
This would fail if... g ever maps two numbers to the same output.

Definition (Injectivity)

Let $f : A \to B$ be a function. We say if is **injective** iff

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

Informally, f is injective if there is **at most** one input that maps to each output.

Question

We decide to be sneaky. Instead of actually choosing an N and giving our friend $g(N)$, we just randomly choose $X \in \mathbb{N}$ and give that. Can our friend still find an N?

Answer

It still depends on g. Now, in addition to g not being allowed to map two numbers to the same output, it must also be the case that g maps **some** input to every output.

Definition (Surjectivity)

Let $f : A \to B$ be a function. We say if is **surjective** iff

$$\forall(y \in B).\ \exists(x \in A).\ y = f(x)$$

Informally, f is surjective if there is **at least** one input that maps to each output.

Question

Suppose we tried to replace $g : \mathbb{N} \to \mathbb{N}$ with

$$h : \mathscr{P}([15151]) \to \left[2^{15151}\right]$$

Could our friend find a function h that he can use to get back our input?

Answer

Yup. Consider the function that maps $S \mapsto 1 + \sum_{x \in S} 2^{x-1}$.

Important Take-Aways

- Since h allows us to get the input back, we have h is injective and surjective.(We would normally prove this! But we will assume it for now...)
- We can conclude that $|\mathscr{P}([15151])| = |\left[2^{15151}\right]|$ from the **existence** of such a function! Think about why.

Definition (Bijectivity)

Let $f : A \to B$ be a function. We say if is **bijective** iff it is injective and surjective.

Consider the following functions from $\mathbb{R} \to \mathbb{R}$.
Are they injective? surjective? bijective?

$x \mapsto x^2$	Injective? ✗	Surjective? ✗	Bijective? ✗
$x \mapsto x^3 - x$	Injective? ✗	Surjective? ✓	Bijective? ✗
$x \mapsto e^x$	Injective? ✓	Surjective? ✗	Bijective? ✗
$x \mapsto x^3$	Injective? ✓	Surjective? ✓	Bijective? ✓

Question

We don't remember how to convert between types of temperatures, but we do have two compiled C functions:

- $F2C$ which takes in a temperature in Fahrenheit and outputs the corresponding temperature in Celsius.
- $C2K$ which takes in a temperature in Celsius and outputs a temperature in Kelvin.

We need a function $F2K$ that takes in a Fahrenheit temperature and outputs a Kelvin one. If we were allowed to see the source code for **one** of these functions, could we write $F2K$?

Answer

Yes. We'd want the source code for $C2K$. Then, we can "reverse" it to get a function $K2C$ (this "reversal" process is the same one our friend used–the two properties we need **do** happen to be true here). Then, to construct $F2K(x)$, we'd just call $K2C(F2K(x))$.

Outline

Since functions just transform their input into some output, it's very common to chain them together.

With the temperature example, we combined several temperature transformations into one larger one.

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

Definition (Composition)

The **composition** of f and g is defined as

$$\begin{array}{rccc} g \circ f : & A & \to & C \\ & x & \mapsto & g(f(x)) \end{array}$$

We pronounce $g \circ f$ as "g after f".

We must have $\text{codomain}(f) = \text{domain}(g)$ for $g \circ f$ to make sense.
In particular, $g \circ f$ and $f \circ g$ are very different functions. The latter only makes sense when $A = C$.

Consider the functions:

- $S : \mathbb{N} \to \mathbb{N}$, where $S(x) = x^2$
- $D : \mathbb{N} \to \mathbb{N}$, where $D(x) = 2x$

What are each of the following?

- $S \circ D$ is $x \mapsto (2x)^2$ (or $x \mapsto 4x^2$)
- $D \circ S$ is $x \mapsto 2x^2$
- $S \circ S$ is $x \mapsto x^4$

Composition is Associative

Let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be three functions. Then,

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

That is, function composition is associative. This is an incredibly important fact that is often useful.

$f \circ g$ is a function

When working with composition, be very careful with notation. If we have functions $f : A \to B$ and $g : B \to C$...

- $f \circ g$ is probably not what you meant.
- $f(x) \in B$; so, $g \circ f(x)$ is gibberish!

When we talk about "reversing" a function $f : A \to B$, what we mean is "swapping the input and output". This is, of course, the idea of an inverse function which you may have seen before.

Definition (Inverse Function)

We say $g : B \to A$ is the **inverse** of $f : A \to B$ iff

- $\forall (a \in A).\ (g \circ f)(a) = a$
- $\forall (b \in B).\ (f \circ g)(b) = b$

If g is the inverse of f, we write $g = f^{-1}$.

Interestingly: f is bijective $\iff$ f is invertible. You will prove this later.

Some Related Material

$\vee$

Your Family Members