# Functions

Joseph R. Mileti

January 30, 2015

## 1 Functions

We're all familiar with the concept of a function $f$ from Calculus, but often some . In that context, functions are often given by "formulas", such as $f(x) = x^4 - 4x^3 + 2x - 1$. However, we also encounter piecewise-defined functions like

$$f(x) = \begin{cases} x^2 + 1 & \text{if } x \geq 2, \\ x - 1 & \text{if } x < 2 \end{cases}$$

or functions like $f(x) = |x|$, which is really piecewise defined as

$$f(x) = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

For an more interesting example of a piecewise defined function, consider

$$f(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q}, \\ 0 & \text{if } x \notin \mathbb{Q}. \end{cases}$$

However, not all functions in Calculus are defined through formulas on pieces. For a simple example, the function $f(x) = \sin x$ is *not* given by a formula, and in fact it is difficult to compute values of this function with any accuracy using only basic operations like $+$ and $\cdot$. In fact, we give this function the strange new name of "sine" because we can not express it easily using more basic operations. The function $f(x) = 2^x$ is easy to compute for $x \in \mathbb{Z}$, but it's actually nontrivial to compute and even define in general (after all, do you remember the definition of $2^\pi$?). Even more fundamentally, the function $f(x) = \sqrt{x}$ is also not really given by a formula, because the definition, i.e. $f(x)$ is the unique positive $y$ with the property that $y^2 = x$, does not give us an easy way to compute it.

Beyond these fundamental functions that you encounter before Calculus, you learn more exotic ways to define functions in Calculus. Given a function $f$, you learn how to define a new function $f'$, called the derivative of $f$, using a certain limit operation. Now in many cases, you can compute $f'$ more easily using facts like the Product Rule and the Chain Rule, but these rules do not always apply. Moreover, given any continuous function $g$, we can define a new function $f$ by letting

$$f(x) = \int_0^x g(t)\ dt.$$

In other words, $f$ is defined as the "(signed) area of $g$ so far" function, in that $f(x)$ is defined to be the (signed) area between the graph of $g$ and the $x$-axis over the interval from 0 to $x$. Formally, $f$ is defined as a limit of Riemann sums. Again, in Calculus you learn ways to compute $f(x)$ more easily in many special cases using the Fundamental Theorem of Calculus. For example, if

$$f(x) = \int_0^x (3t^2 + t)\ dt$$

then we can also compute $f$ as

$$f(x) = x^3 + \frac{x^2}{2},$$

while if

$$f(x) = \int_0^x \sin t \; dt$$

then we can also compute $f$ as

$$f(x) = 1 - \cos x.$$

However, not all integrals can be evaluated so easily. In fact, it turns out that the perfectly well-defined function

$$f(x) = \int_0^x e^{-t^2} \; dt$$

can not be expressed through polynomials, exponentials, logs, and trigonometric functions using only operations like $+$, $\cdot$, and function composition. Of course, we can still approximate it using Riemann sums (or Simpson's Rule), and this is important for us to be able to do since this function represents the area under a normal curve, which is essential in statistics.

If we move away from functions whose inputs and outputs are real numbers, we can think about other interesting ways to define functions. For example, suppose we define a function whose inputs and outputs are elements of $\mathbb{R}^3$ by letting $f(\vec{u})$ be the result of rotating $\vec{u}$ by $27^o$ around the axis given by the line through the origin and $(1, 2, 3)$. This seems to be a well-defined function despite the fact that it is not clear how to compute it (though we will learn how to compute it in time).

Alternatively, consider a function whose inputs and outputs are natural numbers by letting $f(n)$ be the number of primes less than or equal to $n$. For example, we have $f(3) = 2$, $f(4) = 2$, $f(9) = 4$, and $f(30) = 10$. Although it is possible to compute this function, it's not clear whether we can compute it quickly. In other words, it's not obvious if we can compute something like $f(2^{50})$ without a huge amount of work.

You also have some exposure to the concept of a function as it is used in computer programming. From this perspective, a function is determined by a sequence of imperative statements or function compositions as defined by a precise programming language. Since a computer is doing the interpreting, of course all such functions can be computed in principle (or if your computations involve real numbers, then at least up to good approximations). However, if you take this perspective, an interesting question arises. If we write two different functions $f$ and $g$ that do not follow the same steps, and perhaps even act qualitatively differently in structure, but they always produce the same output on the same input, should we consider them to be the same function? We can even ask this question outside of the computer science paradigm. For example, if we define $f(x) = \sin^2 x + \cos^2 x$ and $g(x) = 1$, then should we consider $f$ and $g$ be the same function?

We need to make a choice about how to define a function in general. Intuitively, given two sets $A$ and $B$, a function $f \colon A \to B$ is an input-output "mechanism" that produces a *unique* output $b \in B$ for any given input $a \in A$. As we've seen, the vast majority of functions that we have encountered so far can be computed in principle, so up until this point, we could interpret "mechanism" in an algorithmic and computational sense. However, we want to allow as much freedom as possible in this definition so that we can consider new ways to define functions in time. In fact, as you might see in later courses (like Automata, Formal Languages, and Computational Complexity), there are some natural functions that are not computable even in theory. As a result, we choose to abandon the notion of computation in our definition. By making this choice, we will be able to sidestep some of the issues in the previous paragraph, but we still need to make a choice about whether to consider the functions $f(x) = \sin^2 x + \cos^2 x$ and $g(x) = 1$ to be equal.

With all of this background, we are now in a position to define functions as certain special types of sets. Thinking about functions from this more abstract point of view eliminates the vague "mechanism" concept because they will simply be sets. With this perspective, we'll see that functions can be defined in any way that a set can be defined. Our approach both clarifies the concept of a function and also provides us with some much needed flexibility in defining functions in more interesting ways. Here is the formal definition.

**Definition 1.1.** *Let $A$ and $B$ be sets. A* function *from $A$ to $B$ is a subset $f$ of $A \times B$ with the property that for all $a \in A$, there exists a unique $b \in B$ with $(a, b) \in f$. Also, instead of writing "$f$ is a function from $A$ to $B$", we typically use the shorthand notation "$f \colon A \to B$".*

For example, let $A = \{2, 3, 5, 7\}$ and let $B = \mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$. An example of a function $f \colon A \to B$ is the set

$$f = \{(2, 71), (3, 4), (5, 9382), (7, 4)\}.$$

Notice that in the definition of a function from $A$ to $B$, we know that for every $a \in A$, there is a unique $b \in B$ such that $(a, b) \in f$. However, as this example shows, it may not be the case that for every $b \in B$, there is a unique $a \in A$ with $(a, b) \in f$. Be careful with the order of quantifiers!

We can also convert the typical way of defining a function into this formal set theoretic way. For example, consider the function $f \colon \mathbb{R} \to \mathbb{R}$ by letting $f(x) = x^2$. We can instead define $f$ by the set

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}$$

or parametrically as

$$\{(x, x^2) : x \in \mathbb{R}\}$$

One side effect of our definition of a function is that we immediately obtain a nice definition for when two functions $f \colon A \to B$ and $g \colon A \to B$ are equal because we have defined when two sets are equal. Given two function $f \colon A \to B$ and $g \colon A \to B$, if we unwrap our definition of set equality, we see that $f = g$ exactly when $f$ and $g$ have the same elements, which is precisely the same thing as saying that $f(a) = g(a)$ for all $a \in A$. In particular, the *manner* in which we describe functions does not matter so long as the functions behave the same on all inputs. For example, if we define $f \colon \mathbb{R} \to \mathbb{R}$ and $g \colon \mathbb{R} \to \mathbb{R}$ by letting $f(x) = \sin^2 x + \cos^2 x$ and $g(x) = 1$, then we have that $f = g$ because $f(x) = g(x)$ for all $x \in \mathbb{R}$.

Thinking of functions as special types of sets is helpful to clarify definitions, but is often awkward to work with in practice. For example, writing $(2, 71) \in f$ to mean that $f$ sends 2 to 71 quickly becomes annoying. Thus, we introduce some new notation matching up with our old experience with functions.

**Notation 1.2.** *Let $A$ and $B$ be sets. If $f \colon A \to B$ and $a \in A$, we write $f(a)$ to mean the unique $b \in B$ such that $(a, b) \in f$.*

For instance, in the above example of $f$, we can instead write

$$f(2) = 71, \qquad f(3) = 4, \qquad f(5) = 9382, \qquad \text{and} \qquad f(7) = 4$$

**Definition 1.3.** *Let $f \colon A \to B$ be a function.*

- *We call $A$ the* domain *of $f$.*
- *We call $B$ the* codomain *of $f$.*
- *We define range$(f) = \{b \in B :$ There exists $a \in A$ with $f(a) = b\}$.*

Notice that given a function $f \colon A \to B$, we have $\text{range}(f) \subseteq B$, but it is possible that $\text{range}(f) \neq B$. For example, in the above case, we have that the codomain of $f$ is $\mathbb{N}$, but $\text{range}(f) = \{4, 71, 9382\}$. In general, given a function $f \colon A \to B$, it may be very difficult to determine $\text{range}(f)$ because we may need to search through all $a \in A$.

For an interesting example of a function with a mysterious looking range, fix $n \in \mathbb{N}^+$ and define $f \colon \{0, 1, 2, \dots, n-1\} \to \{0, 1, 2, \dots, n-1\}$ by letting $f(a)$ be the remainder when dividing $a^2$ by $n$. For example, if $n = 10$, then we have

$$\begin{array}{lllll} f(0) = 0 & f(1) = 1 & f(2) = 4 & f(3) = 9 & f(4) = 6 \\ f(5) = 5 & f(6) = 6 & f(7) = 9 & f(8) = 4 & f(9) = 1 \end{array}$$

Thus, for $n = 10$, we have $\text{range}(f) = \{0, 1, 4, 5, 6, 9\}$. This simple but strange looking function has many interesting properties. Given a reasonably large number $n \in \mathbb{N}$, it looks potentially difficult to determine whether an element is in $\text{range}(f)$ because we might need to search through a huge number of inputs to see if a given output actually occurs. If $n$ is prime, then it turns out that there are much faster ways to determine if a given element is in $\text{range}(f)$ (see Number Theory). However, it is widely believed (although we do not currently have a proof!) that there is no efficient method to do this when $n$ is the product of two large primes, and this is the basis for some cryptosystems (Goldwasser-Micali) and pseudo-random number generators (Blum-Blum-Shub).

**Definition 1.4.** *Suppose that $f \colon A \to B$ and $g \colon B \to C$ are functions. The* composition *of $g$ and $f$, denoted $g \circ f$, is the function $g \circ f \colon A \to C$ defined by letting $(g \circ f)(a) = g(f(a))$ for all $a \in A$.*

Notice that in general we have $f \circ g \neq g \circ f$ even when both are defined! If $f \colon \mathbb{R} \to \mathbb{R}$ is $f(x) = x + 1$ and $g \colon \mathbb{R} \to \mathbb{R}$ is $g(x) = x^2$, then

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f(x^2) \\ &= x^2 + 1\end{aligned}$$

while

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(x + 1) \\ &= (x + 1)^2 \\ &= x^2 + 2x + 1.\end{aligned}$$

Notice then that $(f \circ g)(1) = 1^2 + 1 = 2$ while $(g \circ f)(1) = 1^2 + 2 \cdot 1 + 1 = 4$. Since we have found one example of an $x \in \mathbb{R}$ with $(f \circ g)(x) \neq (f \circ g)(x)$, we conclude that $f \circ g \neq g \circ f$. It does not matter that there do exist some values of $x$ with $(f \circ g)(x) = (f \circ g)(x)$ (for example, this is true when $x = 0$). Remember that two functions are equal precisely when they agree on *all* inputs, so to show that the two functions are not equal it suffices to find just one value where they disagree (again remember that the negation of a "for all" statement is a "there exists" statement).

**Proposition 1.5.** *Let $A, B, C, D$ be sets. Suppose that $f \colon A \to B$, that $g \colon B \to C$, and that $h \colon C \to D$ are functions. We then have that $(h \circ g) \circ f = h \circ (g \circ f)$. Stated more simply, function composition is associative whenever it is defined.*

*Proof.* Let $a \in A$ be arbitrary. We then have

$$\begin{aligned}((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) \\ &= h(g(f(a))) \\ &= h((g \circ f)(a)) \\ &= (h \circ (g \circ f))(a),\end{aligned}$$

where each step follows by definition of composition. Therefore $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$ for all $a \in A$. It follows that $(h \circ g) \circ f = h \circ (g \circ f)$. $\square$

**Definition 1.6.** *Let $A$ be a set. The function $id_A \colon A \to A$ defined by $id_A(a) = a$ for all $a \in A$ is called the* identity function *on $A$.*

We call this function the identity function because it leaves other functions alone when we compose with it. However, we have to be careful that we compose with the identity function on the correct set and the correct side.

**Proposition 1.7.** *For any function $f\colon A \to B$, we have $f \circ id_A = f$ and $id_B \circ f = f$.*

*Proof.* Let $f\colon A \to B$ be an arbitrary function.

- We first show that $f \circ id_A = f$. Let $a \in A$ be arbitrary. We have

$$\begin{aligned} (f \circ id_A)(a) &= f(id_A(a)) && \text{(by definition of composition)} \\ &= f(a) \end{aligned}$$

  Since $a \in A$ was arbitrary, it follows that $f \circ id_A = f$.

- We now show that $id_B \circ f = f$. Let $a \in A$ be arbitrary. We have

$$\begin{aligned} (id_B \circ f)(a) &= id_B(f(a)) && \text{(by definition of composition)} \\ &= f(a) && \text{(because } f(a) \in B\text{)} \end{aligned}$$

  Since $a \in A$ was arbitrary, it follows that $id_B \circ f = f$.

□

As we've mentioned, the key property of a function $f\colon A \to B$ is that every input element from $A$ produces a unique output element from $B$. However, this does not work in reverse. Given $b \in B$, it may be the case that $b$ is the output of zero, one, or many elements from $A$. We give special names to the types of functions where we have limitations for how often elements $b \in B$ actually occur as an output.

**Definition 1.8.** *Let $f\colon A \to B$ be a function.*

- *We say that $f$ is* injective *(or* one-to-one*) if whenever $a_1, a_2 \in A$ satisfy $f(a_1) = f(a_2)$, we have $a_1 = a_2$.*
- *We say that $f$ is* surjective *(or* onto*) if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.*
- *We say that $f$ is* bijective *if $f$ is both injective and surjective.*

Let's take a moment to unpack these definitions. First, saying that function $f\colon A \to B$ is surjective is simply saying that every $b \in B$ is hit at least once by an element $a \in A$. We can rephrase this using Definition 1.3 by saying that $f\colon A \to B$ is surjective exactly when $\text{range}(f) = B$.

The definition of injective is slightly more mysterious at first. Intuitively, a function $f\colon A \to B$ is injective if every $b \in B$ is hit by at most one $a \in A$. Now saying this precisely takes a little bit of thought. After all, how can we say "there exists at most one" because our "there exists" quantifier is used to mean that there is at least one! The idea is to turn this around and not directly talk about $b \in B$ at all. Instead, we want to say that we never have a situation where we have two distinct elements $a_1, a_2 \in A$ that go to the same place under $f$. Thus, we want to say

"**Not** (There exists $a_1, a_2 \in A$ with $a_1 \neq a_2$ and $f(a_1) = f(a_2)$)".

We can rewrite this statement as

"For all $a_1, a_2 \in A$, we have **Not**($a_1 \neq a_2$ and $f(a_1) = f(a_2)$)",

which is equivalent to

"For all $a_1, a_2 \in A$, we have either $a_1 = a_2$ or $f(a_1) \neq f(a_2)$"

(notice that the negation of the "and" statement turned into an "or" statement). Finally, we can rewrite this as the following "if...then..." statement:

"For all $a_1, a_2 \in A$, if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$".

Looking at our statement here, it captures what we want to express perfectly because it says that distinct inputs always go to distinct outputs, which exactly says no element of $B$ is hit by 2 or more elements, and hence that every element of $B$ is hit by at most 1 element. Thus, we could indeed take this as our definition of injective. The problem is that this definition is difficult to use in practice. To see why, think about how we would argue that a given function $f \colon A \to B$ is injective. It appears that we would want to take arbitrary $a_1, a_2 \in A$ with $a_1 \neq a_2$, and argue that under this assumption we must have that $f(a_1) \neq f(a_2)$. Now the problem with this is that is very difficult to work with an expression involving $\neq$ in ways that preserve truth. For example, we have that $-1 \neq 1$, but $(-1)^2 = 1^2$, so we can not square both sides and preserve non-equality. To get around this problem, we instead take the contrapositive of the statement in question, which turns into our formal definition of injective:

"For all $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$, then $a_1 = a_2$".

Notice that in our definition above, we simply replace the "for all... if... then..." construct with a "whenever...we have..." for clarity, but these are saying precisely the same thing, i.e. that whenever we have two elements of $A$ that happen to be sent to the same element of $B$, then in fact those two elements of $A$ must be the same. Although our official definition is slightly harder to wrap one's mind around, it is *much* easier to work with in practice. To prove that a given $f \colon A \to B$ is injective, we take arbitrary $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, and use this equality to derive the conclusion that $a_1 = a_2$.

To recap the colloquial ways to understand these concepts, a function $f \colon A \to B$ is injective if every $b \in B$ is hit by at most one $a \in A$, and is surjective if every $b \in B$ is hit by at least one $a \in A$. It follows that a function $f \colon A \to B$ is bijective if every $b \in B$ is hit by exactly one $a \in A$. These ways of thinking about injective and surjective are great, but we need to be careful when proving that a function is injective or surjective. Given a function $f \colon A \to B$, here is the general process for proving that it has one or both of these properties:

- In order to prove that $f$ is injective, you should start by taking arbitrary $a_1, a_2 \in A$ that satisfy $f(a_1) = f(a_2)$, and then work forward to derive that $a_1 = a_2$. In this way, you show that whenever two elements of $A$ happen to go to the same output, then they must have been the same element all along.

- In order to prove that $f$ is surjective, you should start by taking an arbitrary $b \in B$, and then show how to build an $a \in A$ with $f(a) = b$. In other words, you want to take an arbitrary $b \in B$ and fill in the blank in $f(\underline{\quad\quad}) = b$ with an element of $A$.

Here is an example.

**Proposition 1.9.** *The function $f \colon \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is bijective.*

*Proof.* We need to show that $f$ is both injective and surjective.

- We first show that $f$ is injective. Let $x_1, x_2 \in \mathbb{R}$ be arbitrary with $f(x_1) = f(x_2)$. We then have that $2x_1 = 2x_2$. Dividing both sides by 2, we conclude that $x_1 = x_2$. Since $x_1, x_2 \in \mathbb{R}$ were arbitrary with $f(x_1) = f(x_2)$, it follows that $f$ is injective.

- We next show that $f$ is surjective. Let $y \in \mathbb{R}$ be arbitrary. Notice that $\frac{y}{2} \in \mathbb{R}$ and that

  $$f\left(\frac{y}{2}\right) = 2 \cdot \frac{y}{2} = y$$

  Thus, we have shown the existence of an $x \in \mathbb{R}$ with $f(x) = y$. Since $y \in \mathbb{R}$ was arbitrary, it follows that $f$ is surjective

Since $f$ is both injective and surjective, it follows that $f$ is bijective. □

Notice that if we define $g\colon \mathbb{Z} \to \mathbb{Z}$ by letting $g(x) = 2x$, then $g$ is injective by the same proof, but $g$ is not surjective because there does not exist $m \in \mathbb{Z}$ with $f(m) = 1$ (since this would imply that $2m = 1$, so 1 would be even, a contradiction). Thus, changing the domain or codomain of a function can change the properties of that function. We will have much more to say about injective and surjective functions in time.