Relations and Functions 2

Today:

- ☐ Properties of functions (1-to-1, onto, bijective)
- ☐ Sets of Functions
- ☐ Transforming functions into permutations (some modern crypto!)
- ☐ Comparing the sizes of sets (some infinites are bigger than others)

1 Properties of Functions

Last time we introduced *functions*, which we defined as relations $f \subseteq A \times B$ where each point $a \in A$ was related to one and only one point in B. We called A the *domain* of f and we called B its *target* (or *codomain*). We wrote $f\colon A \to B$ to denote a function named f with domain A and target B. We wrote $f(a) = b$ to indicate that $(a, b) \in f$.

Another word for a function is a *map.* If $f(x) = y$ we might say that x *maps to* y. We could also say that y is the *image* under f of x. And we could say that x is a *preimage* under f of y.

I emphasized that our functions are *total*, meaning that they are defined on every single point in the domain. Sometimes computer scientists like to consider *partial* functions, which have "holes" in their domains. But we won't do that.

I emphasized that functions needn't have "simple" domains, or targets, and they needn't have simple descriptions. How about a function that takes in a list of strings and sorts them in alphabetical order? So something like $s\colon (\Sigma^*)^* \to (\Sigma^*)^*$.

How about a function that takes in an arbitrary square matrix and returns its inverse? It might have a signature that looks like

$$\bigcup_{n=1}^{\infty} \mathbb{R}^{n\times n} \to \bigcup_{n=1}^{\infty} \mathbb{R}^{n\times n} \cup \{\perp\}.$$

How about the function that takes in all the sensory input of a cat and tells that cat what to do? Is it a function, too? For philosophical questions in this direction I love the essay "Why Philosophers Should Care About Computational Complexity" by Scott Aaronson.

Onto. I'd like to start looking at key properties of a function. Let's begin with this one. Let's call the *range* of a function $f\colon A \to B$ all the points that are the image of *something*: $\text{Range}(f) = f(A) = \{f(a)\colon a \in A\}$. (Note the "abuse" of notation when writing something like $f(A)$. I like to do that, as though extending the domain from points in A to sets of points in A—but you need to be clear that you're not literally applying f to A.) Is the range the target?

Definition. Let $f\colon A \to B$ be a function. If the range of f is exactly the target of f, $\{f(x)\colon x \in A\} = B$ then we say that f is **onto**, or **surjective**.

Let's make up some more functions. How about the function that maps everyone to their birthday, $b\colon P \to [1..12] \times [1..31]$. So $b(\mathsf{phil}) = (7, 31)$, $b(\mathsf{son}) = (5, 8)$. Is b onto? Not the way we described it, because nobody has a birthday of $(2, 31)$. Could we "clean up" the target to make it only have the 366 "valid" days? Sure.

How about the function that squares a number? Again, specify the domain and target to get a well-defined function. If we decide that that domain and target are $\mathbb{Z}_{10}$, say, then squaring is a function $s\colon \mathbb{Z}_{10} \to \mathbb{Z}_{10}$. What do the different points map to? Well, $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 9$, $4 \mapsto 6$, $5 \mapsto 5$, $6 \mapsto 6$, $7 \mapsto 9$, $8 \mapsto 4$, and $9 \mapsto 1$. Notice that I used a different kind of arrow to show the *image* of a point under f. It's $\to$ for indicating the domain and target of a function—$f\colon A \to B$, but it's this $\mapsto$ arrow to tell me what some specific point mapped to, $x \mapsto y$, with the function itself anonymous.

I see lots of "ad hoc" notation when it comes to function. Don't. If you're writing $f(x = a) : b$ or whatever, don't expect any credit. To be understood in English you need to speak in fairly grammatical sentences. To be understood in math you need to write or speak in grammatical ways, too.

I've told you one important property of a function—whether or not it's surjective (onto). You can express a function $f\colon A \to B$ as being surjective as the condition:

$$(\forall b \in B)(\exists a \in A)(f(a) = b).$$

I tend to think of the target of a function almost as a matter of opinion. If you've got a function $f\colon A \to B$ you can prune B down to the range of f and it doesn't really change the character of f. In the other direction, you can add in anything you like to B and it doesn't really change anything about the character of f, as you never even hit those points.

1-to-1. A second key property of a function $f\colon A \to B$ is whether or not it is *injective* (also called *1-to-1*). An injective function is one without *collisions*, which are distinct points $a, a' \in A$ such that $f(a) = f(a')$. In directed graph that represents a function, it's a target value y that has two *preimages*—points that map to it. Here's a logical definition for when a function $f\colon A \to B$ is injective:

$$(\forall a \in A)(\forall a' \in A)(f(a) = f(a') \to a = a')$$

Another word for a function being injective is it being *one-to-one* Let's memorialize all this:

Definition. A function $f\colon A \to B$ is *injective* (or *one-to-one*) if $f(a) = f(a')$ implies $a = a'$.

Here are some more examples. Let $f\colon \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = x^2$. Is it injective? Yes. Is it onto? No.

Let $f\colon \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$. Is it injective? No. Is it onto? No.

Let $f\colon \mathbb{R}^+ \to \mathbb{R}^+$, where $\mathbb{R}^+$ denotes the positive real numbers, defined by $f(x) = x^2$. Is it injective? Yes. Is it onto? Yes.

Whether or not a function is injective has nothing to do with whether or not it is onto. All four possibilities can easily occur (of being one-to-one or not; of being onto or not).

Sometimes it can be tricky to figure out if a function is one-to-one or onto. Let $f(x) = 3x \bmod 10$ on $\mathbb{Z}_{10}$. Not one-to-one and not onto. But how about $g(x) = 3x \bmod 11$ on $\mathbb{Z}_{11}$. Now it is both one-to-one and onto.

Bijections, permutations. Let us combine the two notions we've just given.

Definition. A function $f\colon A \to B$ that is both one-to-one and onto is called *bijective*.

You can also call the function a *bijection*. You can think of a bijection as a renaming of things: every point in domain has an alternative name in the target; every point in the target gets an alternative name in the domain.

A bijection $f\colon A \to A$ is called a *permutation*. It's again a renaming, but now you are renaming points within a set by points within that same set.

Here is a bijection. Points $\{A, B, C, D, E, F\}$ and $\{10, 11, 12, 13, 14, 15\}$ where $f(A) = 10$, $f(B) = 11$, $f(C) = 12$, $f(D) = 13$, $f(E) = 14$, $f(F) = 15$. Or: Even numbers and odd numbers by way of $f(n) = n + 1$.

I like to use π for permutations. How about $\pi_c\colon \{0,1\}^8 \to \{0,1\}^8$ by way of $\pi(x) = x \oplus c$ where the xor is done bitwise. (Do an example.) A nice bijection! How do you go backwards?

Similarly, in $\mathbb{Z}_n$, the function $f_c(a) = a + c$ (meaning $(a + b) \bmod n$). How do you go backwards now?

Inverses. This idea of going backwards is important in math.

Definition. Let $f\colon A \to B$. Then a function $g\colon B \to A$ is said to be an *inverse* of f if for all $x \in A$ we have that $g(f(x)) = x$

When will a function have an inverse? First, it has to be 1-to-1. Otherwise, you wouldn't know *which* inverse to use for some point $b \in B$. Second, it's got to be onto. Otherwise, some point in B wouldn't have *anywhere* to go to. In other words, the function $f\colon A \to B$ has an inverse if and only if f is bijective.

Or you could first throw out points outside of the range of f, so that $f\colon A \to C$ where $C = \text{Range}(f)$. Now f will have an inverse exactly when A is 1-to-1.

Let's think of more examples. Does the increment function in $\mathbb{Z}_n$ have an inverse? What is it.

How about adding two numbers in the integers? No way; lots of preimages.

What about "interleave the digits of two real numbers in $[0, 1]$"? If we're careful about it!

What about boolean negation? The function is its own inverse. And boolean conjunction? No, that's a map from $\mathbb{B}^2$ to $\mathbb{B}$, so the domain is bigger then the range and the function is not injective. For functions with a finite domain and range, you can only have a bijection between them if they have the same cardinality. That's important!

Composition Given a function $f\colon A \to B$ and a function $g\colon B \to C$ there is a function $g \circ f\colon A \to C$ defined by $(g \circ f)(x) = g(f(x))$.

2 Sets of Functions

I sometimes like to think about the set of *all* functions from A to B. I denote this $\text{Func}(A, B)$. It comes up a lot in cryptography. Can we count $|\text{Func}(A, B)|$ when $A = B = \{0, 1\}^{128}$. Thinking about the truth table, it's $2^{128 \cdot 2^{128}} = 2^{2^{135}}$.

Similarly, let's write $\text{Perm}(A)$ for the set of all permutation on A. How big is $\text{Perm}(\{\mathtt{0}, \mathtt{1}\}^{128})$? Again thinking about the truth table, that will be $2^{128}!$.

You can have other sets of functions. For example, how about

$$\text{Poly} = \{p\colon p \text{ is a polynomial with integer coefficients}\}.$$

Or

$$\mathcal{L} = \{x \mapsto ax + b\colon a \in \mathbb{R},\ b \in \mathbb{R}\}.$$

Does every $f \in \mathcal{L}$ have an inverse? What would you do to modify $\mathcal{L}$ so ensure that it did?

3 Transforming Functions into Permutations.

Permutations have some structure that functions lack. I mean, when filling out the truth table for a random permutation you have to observe some rule—that every answer is distinct. That structure is what lets you invert. Is it possible to convert a random function to a random permutation, giving the function the needed structure?

Fisher-Yates Shuffle, 1938/1964 Traditionally called the Knuth Shuffle. To shuffle an array a of n elements indexed 0 to $n-1$:

```
for $i$ from $n-1$ downto 1 do
    $j \twoheadleftarrow [0..i]$
    swap $a[j]$ and $a[i]$
```

The notation $j \twoheadleftarrow S$ means to choose an element uniformly at random from the finite set S and assign that value to the variable named j.

Can you see why this construction gives a uniformly random permutation (just using an informal understanding of that term)?

Very pretty, that shuffle. Now seen as the natural way to implement a card-shuffle on a computer. But not obivious, if you had to invent it on your own.

Swap-or-not shuffle, Morris-Rogaway, 2012 The following algorithm, known as *swap-or-not*, shuffles an array a of n elements indexed 0 to $n-1$:

```
for $r$ from 1 to $R$ do
    $K \twoheadleftarrow [0..n-1]$
    for each $\{i, j\}$ s.t. $i + j = K$ do
        if $b \twoheadleftarrow \{0,1\}$ then swap $a[i]$ and $a[j]$
```

A cool thing about this shuffle is that it is *oblivious*: you can track the trajectory of each card without worrying about the trajectory of all the rest. Also, Morris and I prove that it mixes the deck of cards very quickly. While you need to spend n rounds to (perfectly) mix the cards with the first shuffle, it only takes about $c \lg n$ round to mix the cards well in the second shuffle. It makes a pretty good way to shuffle a deck of cards that has, say, 10^9 cards, and where you just want to know where some particular card goes to. And this problem is actually quite proactical. I mean, if you wanted anonymize someone's social security number, which is a 9-decimal-digit string, doin this in a way that you can reverse if you need to, is that not shuffling a deck of 10^9 cards where you only aim to follow some particular one of them?

4 Comparing the sizes of sets

Are there more integers or even integers?

It's tempting to say that there are more integers because the even integers are a proper subset of the integers. But this isn't a very "robust" view of size—in particular, it's not the view of size that extends when you would say that two *finite* sets have the same size. There, it is natural to say that two sets A and B have the same size, or are *equinumerous*, if there is a bijection $\pi\colon A \to B$.

Example: $\{A, B, C, D, E\}$ and $\{1, 2, 3, 4, 5\}$ are equinumerous. But so are $\mathbb{N}$ and $2\mathbb{N} = \{2i\colon i \in \mathbb{N}\}$. The bijection from $N \to 2\mathbb{N}$ is just $x \mapsto 2x$.

Are there more strings over $\{0, 1\}$ or natural numbers? Again, there are the same. Enumerate them in lexicographic order, $\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$. The bijection from $\mathbb{N}$ to $\{\mathtt{0}, \mathtt{1}\}^*$ maps the number n to the nth string that would list in lexicographic order.

Are there more real numbers in $[0, 1]$ or pairs of real numbers in $[0, 1] \times [0, 1]$? Again the are the same. Each real number $x \in [0, 1]$ can specify a pair of real numbers by taking the odd and even digits. But there is a technicality insofar as some real numbers have two representations. So always used the "smaller" representation (according to the first digit of difference). Can we really specify any pair (x_1, x_2)?

Definition. Sets A and B are said to be *equinumerous*, written $|A| = |B|$, if there exists a *bijection* $\pi\colon A \to B$. We say that $|A| \le |B|$ if there exists an *injection* $f\colon A \to B$.

Proposition. Equicardinality is an equivalence relation. (Well, maybe better not ask $\sim$ is a subset of!).

Definition. A set A is *countable* if it is finite or equicardinal with $\mathbb{N}$. A set is *uncountable* otherwise.

Proposition. $\mathbb{Z} \times \mathbb{Z}$ is countable. So is $\mathbb{Q}$. So is Σ^*.

Theorem. [Cantor-Schröder-Bernstein, circa 1896.] If $|A| \le |B|$ and $|B| \le |A|$ then $|A| = |B|$. We won't prove this, but I encourage you to read a proof of it!

Theorem. There are uncountable sets. In particular, the set of all languages over the alphabet $\Sigma = \{0, 1\}$ is uncountable.

Proof: Suppose for contradiction that the languages over Σ were countable. Let $L_1, L_2, \ldots$ be an enumeration of them. Let $x_1, x_2, \ldots,$ be an enumeration of the strings in Σ^*. Define a new language $D \subseteq \{\mathtt{0}, \mathtt{1}\}^*$ by asserting that

$$D = \{x_i\colon x_i \notin L_i\}.$$

I claim that $D \notin \{L_1, L_2, \ldots\}$. After all, if $D = L_k$ for some particular k, then is x_k in D or is it not? By definition, $x_k \in D$ if and only if $x_i \notin L_k = D$, a contradiction.