Notes 10

Lecture Notes 10

In last lecture we defined an important property of relations called antisimmetry. There is a similar property called "asymmetry". To avoid any confusion, we now repeat both definitions and compare them:

- relation R is antisimmetric if for all a and b, aRb and bRa imply $a = b$.
- relation R is asymmetric if for all a and b (possibly equal to a), aRb and bRa cannot both be true.

The difference is that in an antisimmetric relation we can have aRa, while for asymmetric relations this is not allowed.

Quiz 1 will be Wednesday March 19, from 7pm to 9pm in rooms 3-270 and 3-370.

There is a handout (H14) on proving correctness of programs summarizing all three techniques we have studied to prove algorithm correctness.

Homework: only 3 problems.

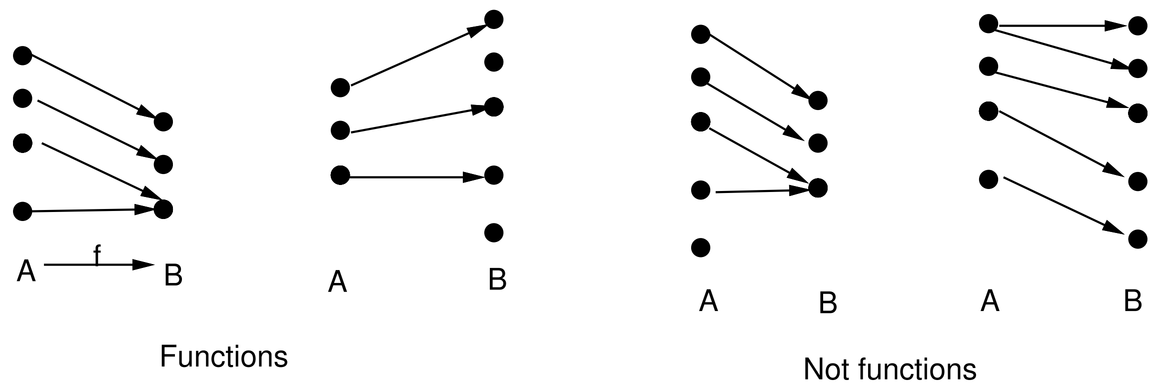
In this lecture we will talk about functions, which are a special kind of relations, their relation to counting and the Pigeonhole Principle.

12 Functions

A *function* is a way of relating *every* item in a set, A, with *precisely one* item in a (possibly different) set, B.

Definition 12.1 A *function* $f : A \to B$ is a relation R on $A \times B$ such that $(\forall a \in A)(\exists! b \in B)(a, b) \in R$. We write $f(a)$ for the unique element of B such that $(a, f(a)) \in R$.

The set A is called the *domain* of f, and the set B is called the *range* of f.



Why aren't the right-hand ones functions? Note they *are* relations.

To be a function, every item in A must be related to just one item in B. Note that every item in B need not be hit. The image of f is the set of points that are hit. Formally, the image of f, denoted by $f(A)$, is $\{b \in B | \exists a \in A \text{ s.t. } f(a) = b\}$.

You should be familiar with many functions such as $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = |x|$ and $g : \mathbb{R} \rightarrow \mathbb{Z}$ where $g(x) = \lfloor x \rfloor$.

An example of a non-function is $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \sqrt{x}$. This is not a function because $\sqrt{-1}$ is not a real. Even if we extend the range to the complex numbers, we still have the problem that $\sqrt{1} = \pm 1$. If we only take the positive root, then square root is no longer distributive over negative numbers (this is the source of our $1 = -1$ paradox from several lectures ago).

Functions can also be defined recursively. The Fibonacci function, $f : \mathbb{N} \rightarrow \mathbb{N}$ can be defined as

$$f(n) = \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ f(n-1) + f(n-2) & \text{if } n > 1. \end{cases}$$

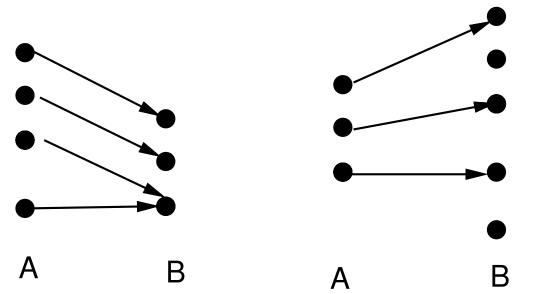
The factorial function can be similarly defined as

$$f(n) = \begin{cases} 1 & \text{if } n = 0, \\ n \cdot f(n-1) & \text{if } n > 0. \end{cases}$$

Three important special classes of functions are surjections, injections, and bijections.

Definition 12.2 A function $f : A \rightarrow B$ is a *surjection* (aka onto) if $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

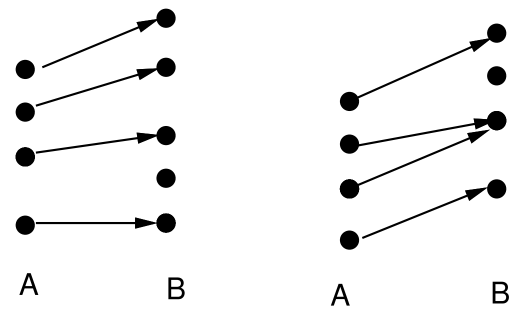
In a surjection, every element in B is hit by at least one element.



Surjection Not a surjection

Definition 12.3 A function $f : A \to B$ is an *injection* (aka as 1-1) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

In an injection, no two elements in A point to the same element.



Injection Not an injection

Definition 12.4 A function $f : A \to B$ is a *bijection* if it is both an injection and a surjection.

In a bijection, there is a one-to-one correspondence between elements in A and elements in B.

For example, $f : \mathbb{N} \to \mathbb{N}$ where $f(x) = 2x$ is one-to-one, but not onto, and thus not a bijection.

How do we prove this? We assume that $f(x) = f(y)$ and show that this implies $x = y$. If f is the function $f\colon x \mapsto 2x$ we have $2x = f(x) = f(y) = 2y$. Dividing both sides by 2 get $x = y$. So, f is injective. To prove that f is not surjective we just notice that $f(x) = 2x \neq y$ for any odd number y. In particular $f(x) \neq 1$ for any x and therefore f is not surjective.

However, if we modify the range, so $f : \mathbb{N} \to 2\mathbb{N}$("even numbers"), then we have a bijection.

There's something special relating the two sides of a bijection. What is it? If the domain and range of the bijection are finite, then they have the same size. This fact will be formally proved in a later section.

12.1 Composition

If $f : A \to B$ and $g : B \to C$ then $g \circ f : A \to C$ is defined by $(g \circ f)(a) = g(f(a))$.

This corresponds to relational definition:

$$S \circ R = \{(a, c) \mid (a, b) \in S, (b, c) \in R\}.$$

More precisely, if F is the function f regarded as a relation, and G is the function g regarded as a relation, then the relation composition $G \circ F$ is precisely the function $g \circ f$. In order to define function composition as a special case of relation composition when applied to functions, we need to prove the following theorem.

Theorem 12.5 Let f, g be two functions, and let F and G be the corresponding relations $aFb \leftrightarrow f(a) = b$ and $aGb \leftrightarrow g(a) = b$. Then, the composite relation $G \circ F$ is also a function and $a(G \circ F)b \leftrightarrow g(f(a)) = b$.

Proof. We have to prove that for all a there exists a unique b such that $(a, b) \in (G \circ F)$. Now, $(a, b) \in (G \circ F)$ iff there exists some c such that $(a, c) \in F$ and $(c, b) \in G$. Since F is a function, there exists a unique c such that $(a, c) \in F$, namely $c = f(a)$. Similarly, since G is a function there exists a unique b such that $(c, b) \in G$, namely $b = g(c) = g(f(a))$. Therefore, there is only a b such that $(a, b) \in (G \circ F)$ and this is precisely $g(f(a))$. ■

Lemma 12.6 Composition of two injections is an injection. Composition of two surjections is a surjection. Composition of two bijections is a bijection.

Proof. Assume f and g are injections. We want to prove that $g \circ f$ is an injection. Assume for contradiction that there exists $a \neq b$ such that $g(f(a)) = g(f(b))$. Since f is an injection $f(a) \neq f(b)$, and since g is an injection this implies $g(f(a)) \neq g(f(b))$, contradiction.

Similarly, if f and g are surjections then for any b in the range of g there exists a c such that $g(c) = b$, and there exists an a such that $f(a) = b$. It follows from the definition of composition that $(g \circ f)(a) = b$, proving that $g \circ f$ is a surjection.

The fact that the composition of bijections is a bijection follows immediately from the previous parts. ■

12.2 Inverses

Let f be a function. The inverse function f^{-1} is defined by $f^{-1}(x) = y$ if $f(y) = x$. Is this a good definition? No: the f^{-1} so defined is not necessarily a function. There are two problems with the definition above:

- If f is not surjective, then f^{-1} doesn't have a mapping for some values.
- If f is not injective, then f^{-1} has more than one mapping for some values.

A more rigorous definition of *inverse* can be given for relations.

Let R be a binary relation over $A \times B$. The *inverse* relation R^{-1} is the relation over $B \times A$ defined by $R^{-1} = \{(b,a) \mid (a,b) \in R\}$. (The inverse relation R^{-1} is sometimes denoted also by R^T for analogy to the matrix transposition operation).
In particular we can apply the definition of inverse relation to a function, which is a relation with some special properties, but the result won't be a function in general, it will be a relation.

However we can prove the following theorem:

Theorem 12.7 Let f be a function and let F be the corresponding relation $aFb \leftrightarrow f(a) = b$. The inverse relation F^{-1} is a function from B to A iff f is a bijection from A to B.

Proof. F^{-1} is the set of pairs $(f(a), a)$. For this to be a function from B to A:

- every element of B must appear as a "first component" in F^{-1}. Means every $b \in B$ is $f(a)$ for some a, (f is a surjection).
- every $f(a)$ must have exactly one a. Means f is an injection.

So, if f is a bijection, then the inverse relation F^{-1} is a function corresponding to the usual definition $f^{-1}(x) = y$ iff $f(y) = x$. ∎

Notice that the definition of injectivity and surjectivity can be given for any relations, not just for functions. We say that a (binary) relation R is injective if for all a, b, c, aRb and cRb imply $a = b$. R is surjective if for all b there is some a such that aRb. Given this definition, the above theorem holds even if f is a relation: i.e., the inverse relation R^{-1} is a function if and only if the relation R is injective and surjective.

Theorem 12.8 Let R be a relation over $A \times B$. R is a function if and only if the relation R^{-1} is both injective and surjective.

The proof that the composition of injections is an injection and the composition of surjections is a surjections is then the same as the proof that the composition of functions is a function applied to the inverse relations. (notice that for any relations R and S we have $(R \circ S)^{-1} = (S^{-1} \circ R^{-1})$.

13 Cardinality

Bijections can be used to formally define the notion of cardinality of sets.

The idea is the following: "If there is a bijection between two sets, then the two sets have the same size."

Counting the elements of a sets can be viewed as assigning numbers $1, \ldots, n$ to the elements the set. In other words, counting is about creating a bijection between a set and the numbers $1, \ldots, n$.

Definition 13.1 $[n]$ is the set of numbers $\{1, \ldots, n\}$. (Recursive definition: $[0] = \emptyset$ and $[n+1] = [n] \cup \{n+1\}$).

We write $|A| = n$ if there is a bijection from A to $[n]$.

Counting lets us write set in a convenient way. We can write $A = \{a_1, \ldots, a_n\}$. Technically, this is defining a bijection $a : [n] \to A$; we just write a_i instead of $a(i)$.

Does this give a consistent notion of counting? In other words, is it true that $|[n]| = k$ if and only if $k = n$? Or, is it possible that $|A| = n$ and $|A| = k$ where $n \neq k$? We will answer this questions in the next theorems.

Theorem 13.2 There is no bijection from $[n]$ to $[k]$ if $n \neq k$.

Proof. Let n be smallest number for which exists bijection $f : [n] \to [k]$ for $k \neq n$ (note that this means $k > n$ because if f is a bijection from $[n]$ to $[k]$ then f^{-1} is a bijection from $[k]$ to $[n]$).

First suppose $n = 0$. Then our domain is $\emptyset$. So, if $f\colon [n] \to [k]$ is a bijection there exists a bijection from an empty to non-empty set. But this is impossible because $f(\emptyset) = \emptyset \neq [k]$ because $k > 0$, and f is not a surjection.

Suppose $f(n) = y$, and $f^{-1}(k) = x$. Then we define a new bijection $g : [n-1] \to [k-1]$ by setting $g(m) = f(m)$ except that $g(x) = y$.

We show this is a bijection from $[n-1]$ to $[k-1]$. Clearly g is a function. We prove that g is injective and surjective.

Let's do injective first. Assume for contradiction that $g(a) = g(b)$ for some $a, b \in [n-1]$ such that $a \neq b$. If $a = x$ (and therefore $b \neq x$) we have $f(b) = g(b) = g(a) = g(x) = y = f(n)$ and $b \neq n$, contradiction because f is injective. The case $b = x$ (and $a \neq x$) is analogous. Finally, if both $a, b \neq x$, we have $f(a) = g(a) = g(b) = f(b)$ and $a \neq b$, contradiction because f is injective.

We now show that g is surjective. Let b be in $[k-1]$. We want to prove that $g(a) = b$ for some $a \in [n-1]$. There are two cases. If $b = y$, then take $a = x$ and we have $g(x) = y$ by definition of g. Otherwise, $b \neq y$ and since f is surjective there exists an $a \in [n]$ such that $f(a) = b$. This a cannot be x because $f(x) = k > b$. Therefore $g(a) = f(a) = b$.

In conclusion, g is a bijection from $[n-1]$ to $[k-1]$ contradicting the claim that n is smallest. ∎

So bijection to $[n]$ captures the notion of counting.

We say A is *finite* if $|A| = n$ for some natural n. Can we have $|A| = n$ and $|A| = k$ for $n \neq k$? No, as we will now prove. Assume that $|A| = k$ and $|A| = n$ for $n \neq k$. There exist bijections $f\colon A \to [n]$ and $g\colon A \to [k]$. But the inverse of a function is a function and it is also a bijection, so $f^{-1}\colon [n] \to A$ is a bijection. Since the composition of bijections is a bijection, $g \circ f^{-1}$ is a bijection contradicting our previous theorem.

Theorem 13.3 If A and B are finite sets and $g : A \to B$ is a bijection, then $|A| = |B|$.

Proof. Suppose $|A| = n$. Then there is a bijection $f : [n] \to A$. There is also a bijection $g : A \to B$. Then $g \circ f : [n] \to B$ is a bijection from $[n]$ to B. ∎

This is a good trick if you are trying to count the elements of a set: set up a bijection with a set whose size you already know. Then you know they have the same size.

How did we use this last time? When counted the elements of the power set. Here's the formal proof:

Theorem 13.4 For finite A, $|2^A| = 2^{|A|}$.

Proof. By induction on $|A|$. In the base case $A = \emptyset$ and $2^A = \{\emptyset\}$, and therefore we have $|2^A| = 1 = 2^0 = 2^{|A|}$. Now assume $|A| > 0$ (i.e. A is not empty). Fix an element $a \in A$. Suppose the theorem is true for all A such that $|A| = n - 1$. Note that

$$A = \{S \subseteq A \mid a \notin S\} \cup \{S \subseteq A \mid a \in S\}$$

is union of two disjoint sets, and thus has size equal to the sum of their sizes (this can be proven giving a bijection: if $|A| = k$ and $|B| = n$, give a bijection from $A \cup B \to [k+n]$, but will spare you the details.)

The first is just $2^{(A-\{a\})}$, so has 2^{n-1} element by induction (notice that $|A - \{a\}| = n - 1$.

What about second? Well, we can biject it to the first: $f(S) = S - \{a\}$ can be easily verified to be a bijection from the second to the first set. So, the second set has also size 2^{n-1}.

So, since A is the disjoint union of two sets of size 2^{n-1}, is has size $2^{n-1} + 2^{n-1} = 2^n$. ∎

What can we say if there is a surjection/injection from A to B? The proof of theorem 13.2 can be split into two parts to yields the following two theorems.

Theorem 13.5 If there is an injection from $[n]$ to $[k]$ then $n \leq k$.

Theorem 13.6 If there is a surjection from $[n]$ to $[k]$ then $n \geq k$.

A seemingly immediate result is that any set A with more items than another set B cannot have a bijection between the two. This is true for finite sets. However, it is not true for *infinite* sets.

Consider $f : \mathbb{N} \to \{0, 2, 4, 6, 8, \dots\}$ where $f(n) = 2n$. This is a bijection, yet the natural numbers contain more elements than the evens. Infinite sets have special properities. In the next lecture, we will discuss them further.

14 Pigeonhole principle

Above, we saw that two (finite) sets of the same size have a bijection. What if A is bigger than B? We know that there is no bijection between the two sets. We said something more precise. If A and B are finite sets with A bigger then B, then there is no injection from A to B.

The principle can be simply stated as: "If $n+1$ pigeons are put in n holes, then at least one hole has two or more pigeons." One easy way to see this is that if each hole only had one or zero pigeons, then there are at most n pigeons. This simple fact allows us to prove many things. An immediate result is that if three people are in a room, then at least two have the same sex.

Theorem 14.1 If A and B are (finite) sets with $|A| > |B|$, then there is no injection from A to B.

Proof. Suppose $|A| = k$ and $|B| = n$ for some $k > n$. Suppose there exists an injection $f\colon A \to B$. We know from before there are bijection $g\colon [k] \to A$ and $h\colon B \to [n]$. Composition of injections $h \circ f \circ g$ is an injection from $[k]$ to $[n]$ with $k > n$. But this is impossible from above. ∎

Wait a minute, we assumed something. What? Finiteness. Pigonehole only applies to finite sets.

Here's a slightly more complicated example (killed people on final exam a couple years ago).

Theorem 14.2 $\forall m < n$, every set with n numbers must contain two numbers whose difference is a multiple of m. (e.g., every set with 1000 numbers must contain two whose difference is a multiple of 573.)

Proof. The proof is easy once you see how to apply the pigeonhole principle.

Let the n numbers be the pigeons. The holes are congruencies mod m (i.e. 0 mod m, 1 mod m, 2 mod m, ... , $m-1$ mod m). Thus, we can map pigeons into holes. Every pigeon will get mapped to some hole. Since there are more pigeons than holes, two pigeons get mapped to the same hole.

If two pigeons (say x and y) are in the same hole, they are congruent mod m. Thus, $x \equiv y \pmod{m}$ and therefore $m|x-y$. ■

Another example is the following.

Theorem 14.3 Let "friendship" be a reflexive and symmetric relation. Then, any set of n people has two people with the same number of friends.

Proof. We again use the pigeonhole principle. Let the pigeons be the n people. Now, we want to choose the holes so that there are $n-1$ holes, and every person gets mapped to a hole. The number of possible friends is 1 to n, which is n possibilites. Apparently, we can't directly apply the pigeonhole principle. However, if we do a little extra work, we can. If a person has n friends, then every person has at least two friends – himself and the very friendly person. Thus, the set of possible friendships is either $[1, n-1]$ or $[2, n]$. Each of these sets has $n-1$ elements, so we can apply the pigeonhole in either situation. Therefore, two people must have the same number of friends. ■

If you ever have a problem that says "show there are two things with the same property" and you don't know what to do, try pigeonhole. But remember, this principle only applies to finite sets.

14.1 Strong Pigeonhole

The *Strong Pigeonhole Principle* is as follows. If $n(r-1)+1$ pigeons are put in n holes, then there is at least one hole with r or more pigeons.

We can prove this by contradiction. Assume all holes have $r-1$ or fewer pigeons, Then, the total number of pigeons is at most $n(r-1)$, which is a contradiction. Note the simple pigeonhole priciple is a special case when $r=2$.

We can use the strong pigeonhole principle to prove some interesting facts. We estimate that any person has at most one million hairs on his head. In China there are oven one billion people. By the strong pigeonhole principle, there are more than one thousand people in China with exactly the same number of hairs on their heads.