ECS 20 – Fall 2021 – Phillip Rogaway Relations & Functions

Def: With A and B sets, a **relation** R is subset of $A \times B$ (or write $X \times Y$?)

$$R \subseteq A \times B$$

Usually we prefer to write things in **infix** notation, so $x\ R\ y$ for $(x,y) \in R$.
And usually we use symbols, rather than letters, for relations: e.g., ~ or <

$$x \sim y \quad \text{if} \quad (x, y) \in \sim$$

Here are some common relations you know from arithmetic, for comparing numbers, where the underlying sets A=B are the sets of natural numbers, integers, or reals:

$$= \quad < \quad \leq \quad > \quad \geq$$

Another important one for integers:

$$|$$

where $d \mid a$ means that d divides a: there exists a number n such that $n\ d = a$.

What about our friends: **succ** (the successor function), +, *, ^ ?
No, these are **function symbols**, not relations.

In set theory we have the relation symbol

$$\in$$

What about $\emptyset$?
No, it's a **constant symbol**.

Often $A = B$ is the **same** set. That is the case for all of the following examples.

1. A = integers, $\leq$
2. A = set of strings over some alphabet; $x \leq y$ if is a substring of y
3. A = set of lines in the plane; $x \sim y$ if they are parallel
4. α and β are regular expressions; $\alpha \sim \beta$ if $L(\alpha) = L(\beta)$
5. x and y are strings of the same length
6. a and b are numbers and $n>0$ is a number and $a\ R_n\ b$ if $n \mid (a-b)$
7. a and b are real numbers and $a \sim b$ if $\lfloor a \rfloor = \lfloor b \rfloor$.

Equivalence relations – Are relations on $X \times X$ that enjoy three properties

Reflexive: $x \, R \, x$ for all x
Symmetric: $x \, R \, y \rightarrow y \, R \, x$ for all x, y
Transitive: $x \, R \, y \wedge y \, R \, z \rightarrow x \, R \, z$ for all x, y, z

Equivalence classes, quotients

If R is an equivalence relation on $A \times A$ then $[x]$ denotes the **set** of all elements related to x:

$$[x] = \{a: \; a \, R \, x\}$$

We call [x] the **equivalence class,** or **block**, of x.

Definition: The set of all equivalence classes of A with respect to a relation R is denoted A/R , which is read "**the quotient set of** A by R" or simply "A **mod** R".

I claim that every equivalence relation on a set **partitions** it into its blocks.

What does this mean? Let's define a **partition** of the set A:

Def: $\{A_i: i \in I \}$ is a **partition** of A if each A_i is nonempty set and (1) their union is A, $A = \cup A_i$, but (2) their pairwise intersection is empty, $A_i \cap A_j = \emptyset$ for all $i \neq j$.

Proposition: Let R be an equivalence relation on a set A.
Then the blocks of R are a partition of A.

Proof: -Every element x of A is in the claimed partition: $x \in [x]$, so the union of blocks covers A.

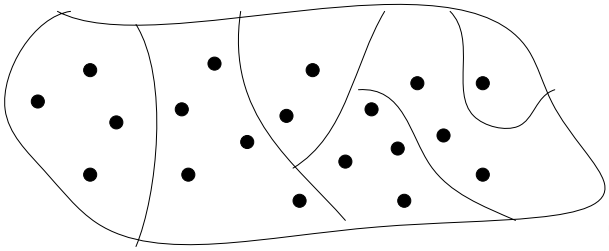
-Suppose that $[x]$ and $[y]$ intersect. I need to argue that they are identical. So suppose there exists a s.t. $a \in$ [x] and $a \in$ [y]. I must show that $[x] = [y]$. Let $b \in [x]$; must show $b \in [y]$. So given:
$a \, R \, x$ (so $x \, R \, a$) $a \, R \, y$ thus $x \, R \, y$, $y \, R \, x$
$b \, R \, x$ (so $x \, R \, b$) thus $y \, R \, b$ (or $b \, R \, y$).

In fact, the relation between equivalence relations and partitions **goes both ways:**

Given a partition $\{A_i: i \in I\}$ of a set A,

define a relation R by asserting that $x \, R \, y$ iff x and y are in the same block of the partition: there exists and i such that $x \in A_i$ and $y \in A_i$. Then R **is** an equivalence relation [prove this].

Note: you can talk about the **blocks** being related to one another by R, that is, $[x] \, R \, [y]$ iff $x \, R \, y$. This is well-defined.



The circles are the points in the base set A. Two points are in the same block if they are related to one another under the equivalence relation.

Now go back to prior examples and identify the blocks in each case.
Eg: strings x and y are equivalent if they have the same length: the blocks are $[\varepsilon]$, $[a]$, $[aa]$, … Here, we are using a nice **canonical name** for each block. It's good to choose such canonical names.

Another example: Consider the **tiles** we spoke of earlier in the course partition the plane (or the upper right quadrant) if you're careful at the *edges* of each tile to make sure that each point is in only one tile. If you define

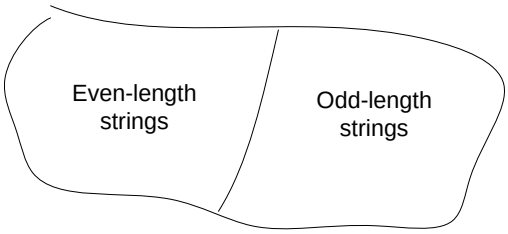
$$[a, b) = \{x \in \mathbb{R}: \; a \leq x < b)$$

So a tile with left endpoint at (i, j) is $[i, i+1) \times [j, j+1)$ and the plane is the disjoint union of tiles

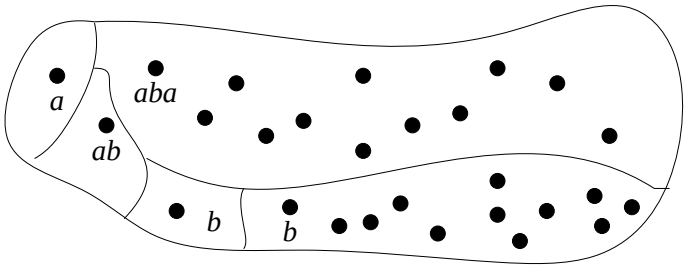
$T_{ij} = [i, i+1) \times [j, j+1)$ when $i, j \in \mathbb{N}\}$

An important example in **formal-language** theory: let L be a language and define from it the relation R_L by saying that $x \, R_L \, y$ if for all z, $x \, z \in L$ **iff** $y \, z \in L$.

Example: Figure out the blocks when $L = \{ \ x \in \{a,b\}^*: |x| \text{ is even}\}$



Example: Figure out the blocks when $L = \{ x \in \{a,b\}^*: x \text{ starts with 'aba'}\}$



Theorem [Myhill-Nerode]: A language L is regular [you can represent it with a regular expression] iff L/R_L has a finite number of blocks.

Back to: a and b are numbers and $n>0$ is a number and $a \ R_n \ b$ if $n \mid (a-b)$

Key example in computer science and mathematics.
"Ring of integers modulo n."
Many ways to understand this "thing".
Ring of integers modulo n, $\mathbf{Z}_n$
$\mathbf{Z}/R_n$ **More common notation** $\boldsymbol{Z}/n\boldsymbol{Z}$

Lots of variant notations
$a = b$ (a and b are point in Z_n)
$a \equiv b$ (a and b are congruent mod n)
$a \equiv b \pmod{n}$
$a \bmod n = b \bmod n$ (now 'mod' is a binary operator)

Functions

Definition: A function f is a relation on $A \times B$ such that there is one and only one $(a, b) \in R$ for every in $a \in A$.

When f is a function, we write $b = f(a)$ to mean that $(a,b) \in f$.

- We call A the domain of f, Dom(f).
- We call B the codomain of f.

Sometimes the codomain is called the range. More common, however, is that that the range of f is the set $\{b \in B: f(a)=b$ for some a in $A\} = f(A) = \cup a \in A \ \{f(a)\}$. A clearer term for this set is the target of f, or the = image of A under f. (The image of a point x under f is $f(x)$; a preimage of $f(x)$ is x.)

Example 1:
Domain={1,2,3}
$f(a) = a^2$.
Dom(f) = {1,2,3} f(A) = {1,4,9}
The co-domain: unclear – you have to specify it. It might be $\mathbb{N}$, might be $\mathbb{R}$, might be exactly the target.

Example 2:
Domain = students in this class, regarded as(month, day) pairs.
b(x) = birthdays, encoded as {1,..,12} x {1..31}.

b(phil) = (7,31)
b(ellen) = (4,1)

Example 3:
$f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$
I see lots of "ad hoc" notation. Don't.

$f: A \to B$. $f(a) = b$. If you're writing crazy things $f(x=a)$: b I'm likely to give no credit. It's like answering in a language you haven't learned to speak when the first requirement of communicating is to be able to speak the language.

Sometimes you might want to show that f takes x to y, a to $2a$, etc. Don't use a $\rightarrow$ symbol for that; write $x \mapsto y$, $a \mapsto 2a$. With surrounding English, this reads ok. But saying $a \rightarrow 2a$ definitely does not.

One-to-one and onto functions

Def: $f : A \rightarrow B$ is **injective** (or **one-to-one**) if $f(x)=f(y)$ implies $x=y$ "**no collisions**"

Def: $f: A \rightarrow B$ is **surjective** (or **onto**) if $(\forall b \in B)\ (\exists a \in A)\ f(a)=b$
"the codomain is the range"

Def: $f: A \rightarrow B$ is **bijective** if is injective and surjective.

A function that is bijective from A to A is called a **permutation**.

Func (A,B) = The set of **all** functions from A to

Perm (A) = The set of **all** permutation on A

Example:

- $f(n) = x^2$
  Ask if it's 1-1 and onto if the domain/co-domain is $\mathbb{Z}$

Sometimes it **can** be tricky to see if a function is 1-1, onto:

- $f(x) = 3x \bmod 90$ **bijective**
- $f(x) = 3x \bmod 91$ **not** bijective

Inverse of a function

If $f(x) = y$ we say that x is a **preimage** of y
Does every point in the codomain have a preimage?
No, only points in the image.
Does every point in the image have **one** preimage?

No, only if it's an injective function
Does every point the in the domain have an image?
Yes, that's required for being a function.
Might it have two images?
No, only one.

If you do have a bijective function $f: A \to B$ then the function $f^{-1}: B \to A$ is well defined: $f^{-1}(y)$ is the unique x such that $f(x) = y$.

Example: $f(x) = \exp(x) = e^x$
Draw picture.
What's the domain? $\mathbb{R}$
What's the range / image ? $(0, \infty)$
Is it 1-1 on this image? YES

What's it's inverse? $y \mapsto \ln(y)$

Some Counting Involving Functions

How many functions are there from 64 bits to 64 bits?
$|\text{Func}(\{0,1\}^{64},\{0,1\}^{64})|$

$$64\ 2^{64} \qquad\qquad 2^{70}$$
$$2 \qquad\qquad = \quad 2$$

How many permutations are there on 128 bits?

$$2^{128}\ !$$

How many on 8 bits?

$$256!$$

Stirling's formula is good for estimating such things:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

or

$$\ln(n!) = n\ln n - n + O(\ln n)$$

or

$$\log_2(n!) = n\log_2 n - n\log_2 e + O(\log_2 n).$$

Let's try to approximate:
How many functions are there on IEEE 64-bit floating points?

Counting above gives

$$2^{64\,2^{64}} = 2^{2^{70}} \qquad \text{(Big-1)}$$

But, realistically, any program that computes a function on the IEEE floating point numbers is going to be described by a program of at most 1 TB in length. How many such programs are there?

$$2^{8\,2^{40}} = 2^{2^{43}} \qquad \text{(Big-0)}$$

This is an infinitesimal fraction of Bug-1. To a pretty good approximation, virtually **none** of the programs we can imagine being computes from 64-bit values to 64-bit values are actually computable by a computer. That's kind of sobering, perhaps?

Composition of functions

Given a function f: $A \rightarrow B$ and a function g: $B \rightarrow C$ we can form the function $g \circ f$ that consists of first applying f and then applying g:

$$g \circ f\ (x) = g(\, f(\, x\,))$$

(There are arguments for writing this $f \circ g$ – we read left-to-right, after all, but then functions would be best written "operating on the left" instead of the more common convention of "operating on the right":

$$(x)\ \ f \circ g = ((x)\, f\,)\, g$$

This convention is common among algebraists, too. We'll use the other notation.)

Examples: Compose the increment function inc(n) on the natural with the squaring function sqr() on the natural.

Compose the increment function with itself.

Example: Let's fix a number *a* and define two function on the naturals:

D(*n*) = 2*n* // to double a number

A (*n*) = *n* + *a* // to add the constant *a* to a number

How could you compose these function to compute

M(*a*, *b*) = *a b* *// the product of a and b*

Solution: Let's regard the bits of *b* as instructions that we read left-to-right. When we see a 0 it means "multiply the current value by two". When we see a 1 it means "multiply the current value by two and then add *a*". Start with a constant of 0.

So if *b* = 1001101, say, and we want to multiply it by *a*, then we should compose the following sequence of operations (read from right-to-left, as per our convention) and apply the result to 0:

A ∘ D ∘ D ∘ A ∘ D ∘ A ∘ D ∘ D ∘ D ∘ A ∘ D

The add function itself can be regarded as a composition of operators drawn from A0, A1, A2, A3, .. where A*i* adds 2^i to the number. So, for example, if *a* = 1101110 then A = A1 ∘ A2 ∘ A3 ∘ A5 ∘ A6.

Example: The function *f* maps $1 \mapsto 2$, $2 \mapsto 3$, and $3 \mapsto 1$.

What is $f \circ f$? $f \circ f \circ f$? (These might be written f^2 and f^3, or sometimes $f^{(2)}$ and $f^{(3)}$.)

Describe alternative notations: pair-of-vectors stacked horizontally or vertically; product of cycles.

Permutations are the **products of disjoint cycles**. Explain. Write permutations in alternative notation.

S_n = all permutation on {1,2,…,*n*} = Perm({1,…,*n*}). The symmetric group on *n* letters (or numbers, or points).

Proposition S_n forms a **group** under composition.

We have three properties to check. Check them!

Comparing the size of sets

We can use the notions of injectivity and bijectivity to compare the sizes of sets, including infinite sets.

Def: Sets A and B are equicardinal if there exists a bijection $f: A \to B$. We write $|A| = |B|$.

Def: Set B is at least as large as set A if there exists an injection $f: A \to B$. We write $|A| \leq |B|$.

Proposition: Being equicardinal is an equivalence relation

Show:

1) $|\text{Evens}| = |\mathbb{N}|$
2) $|\mathbb{N}| = |\mathbb{Q}|$
3) $|\mathbb{N}| \neq |\mathbb{R}|$

Thm [Cantor-Schröder-Bernstein] If $|A| \leq |B|$ and $|B| \leq |A||$ then $|A| = |B|$.