ECS 20 — Lecture 10 — Fall 2013 —29 Oct 2013
Phil Rogaway

Today:

- o Relations
- o Functions
- o Comparing the size of infinite sets

Reminder: MT on Thursday

Relations

Recall:
DEF: With A and B sets, a **relation** R is subset of $A \times B$.

$R \subseteq A \times B$

Usually we prefer to write things in **infix** notation: $x\,R\,y$ for $(x,y) \in R$

Often we use symbols, rather than letters, for relations: eg, $\sim$ or $<$

$x \sim y$ if $(x, y) \in \sim$

Here are some common relations from arithmetic, where A=B are the set of natural number (or the set of reals):

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

Another important one for integers:

$|$ divides

What about our friends: **succ**, +, * ?
NO, these are **function symbols**, not **relations**

In set theory we have the relation symbol
$\in$
What about $\varnothing$?
NO, it's a **constant symbol**

More examples:
Often $X = Y$ is the **same** set
Relations on natural numbers, real numbers, strings, etc.

1. *X = integers, $\leq$*
2. X = set of strings over some alphabet; $x \leq y$ if is a substring of y

3. X = 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 and y R z $\rightarrow$ x R z for all x, y, z

Equivalence classes, quotients

If R is an equivalence relation on A x A then [x] denotes the setof all elements related to x:

$$[x] = \{a\colon\ a\ R\ x\}$$

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

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 "A mod R".

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

What does this mean?
Define a **partitioning** of the set A:

Def: $\{A_i\colon i\ I\}$ 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, $A_i \cap A_j = \varnothing$ for all $i \neq j$.

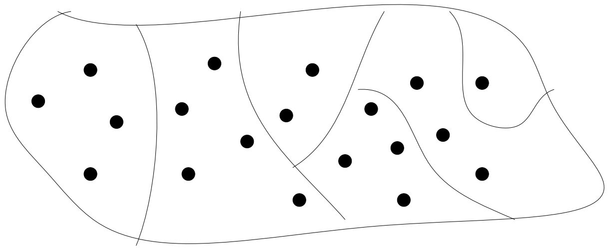
Proposition: Let R be an equivalence relation on a set A.
Then the blocks of R are a partition of A.

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:
aRx (so xRa) aRy thus xRy, yRx
bRx (so xRb) thus yRb (or bRy).

The relation between equivalence relations and partitions **goes both ways:**
Given a partition $\{A_i\colon i \in I\}$ 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].

Notation: A/R the blocks of A relative to equivalence relation R.

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: blocks $[\varepsilon]$, $[a]$, $[aa]$, …
Here, using a nice **canonical name** for each block

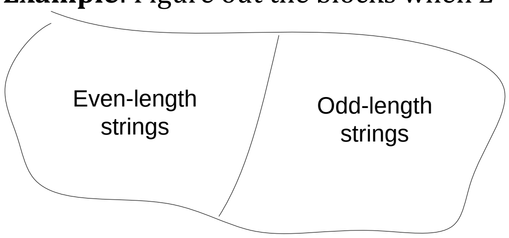
Another example: Consider the **tiles** we spoke of earlier partition the plane (upper right quadrant) if you're careful at the *edges* of each tile to make sure that each point is in only one tile. We defined

$[a, b) = \{x \in \mathbf{R}:\ a \le x < b)$

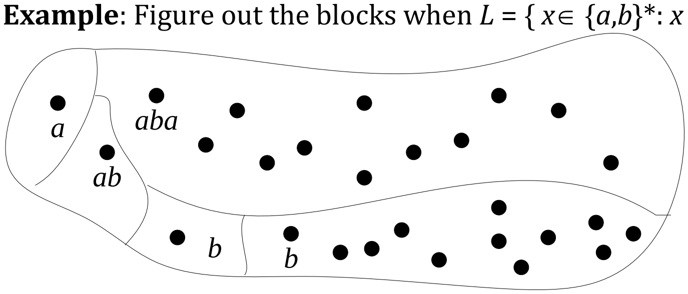
So a tile with left endpoint at (i, j) is $[i, i+1) \times [j, j+1)$ and the plane is the disjoint union of tiles
$T_{ij} = [i, i+1) \times [j, j+1)$ when $i,j \in \mathbf{N}\}$

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, $xz \in L$ **iff** $yz \in L$.

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



Example: Figure out the blocks when $L = \{\, x \in \{a,b\}^*\!: x$ 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 $n \mid (a\text{-}b)$ ***
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 $\boldsymbol{Z}_\mathrm{n}$)
$a \equiv b$ (a and b are congruent mod n)
$a \equiv b \pmod{n}$
a mod n = b mod 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** (or **target**) 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 $A\} = f(A) = \bigcup_{a\in A} \{f(a)\}$

Also called the **image** of A under f.

Example 1:
Domain={1,2,3}
f(a) = a^2.
Dom(f) = {1,2,3}
f(A) = {1,4,9}
co-domain: unclear, might be **N**, might be **R**, ...

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: **R** $\rightarrow$ **R** defined by f(x) = x^2
I see lots of **"ad hoc" notation**. **Don't.**

$f: A \rightarrow B$. $f(a) = b$. 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) $\rightarrow$ 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 (image is the domain)

Def: $f: A \rightarrow$ is **bijective** if is injective and surjective (one-to-one and onto).

Example:

- $f(n) = x^2$

  ask if it's 1-1 and onto if the domain/co-domain is **Z**, **N**

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

- `f(x) = 3x mod 90` **bijective**
- `f(x) = 3x mod 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 $f: A \rightarrow B$ then the function $f^{-1}: B \rightarrow A$ is well defined:

$f^{-1}(y)$ = the unique x such that $f(x) = y$.

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

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