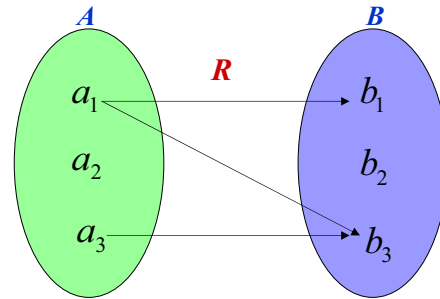




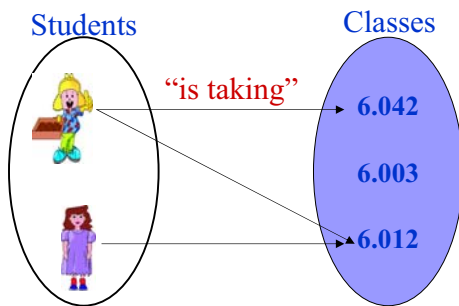
Relations



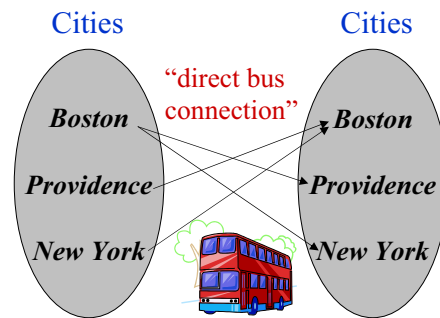
A Relation R



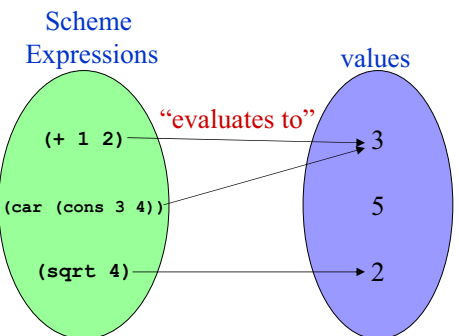
Example



Example



Example

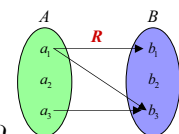


Relation Abstraction

A relation from set A to set B is a set $R \subseteq A \times B$

$$A \times B = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_2), (a_3, b_3)\}$$

$$R = \{(a_1, b_1), (a_1, b_3), (a_3, b_3)\}$$



Registrar

- Assign students to professors who they are not currently taking classes with

Q

Copyright © Radhika Nagpal, 2002. L3-1.7

Relation R

S C

R

students classes

6.042
6.012

Copyright © Radhika Nagpal, 2002. L3-1.8

Relation T

C P

T

classes professors

6.042
6.012

Copyright © Radhika Nagpal, 2002. L3-1.9

New Relation $T \circ R$

S C P

R T

students classes profs

Copyright © Radhika Nagpal, 2002. L3-1.10

New Relation $Q \subseteq S \times P$

S C P

students classes profs

S P

students profs

Q

students profs

Copyright © Radhika Nagpal, 2002. L3-1.11

Registrar Database

- Assign students to professors who they are not currently taking classes with.

$$Q = \overline{T \circ R}$$

$(Ben, Prof. X) \in Q$

Copyright © Radhika Nagpal, 2002. L3-1.12

6	9	13	7
12	10	8	
3	5	4	14
15	11	2	1

The Agenda

- Is it possible to get from any building connected to the infinite corridor to any other building **without crossing more than 5 other buildings**?
- How does Athena decide where to put your locker?
- **How many classes per term** do you need to take to graduate in course 6 in 3 years?
- **How many days** will it take the TAs to execute their evil plan of taking over MIT?

6	9	13	7
12	10	8	
3	5	4	14
15	11	2	1

Overview of Topics

- Representation (lists, matrices, digraphs)
- Operations (inverse, composition)
- Properties (reflexive, symmetric, transitive)
- Equivalence Relations
- Partial Orders

6	9	13	7
12	10	8	
3	5	4	14
15	11	2	1

Functions and Relations

Is a function a relation?

Yes!

$$f: A \rightarrow B$$

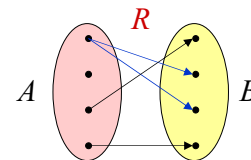
$$R = \{(a, b) \mid \text{where } b = f(a)\}$$

6	9	13	7
12	10	8	
3	5	4	14
15	11	2	1

Functions and Relations

Is a relation a function?

No



6	9	13	7
12	10	8	
3	5	4	14
15	11	2	1

Functions and Relations

But...

Can I represent a relation using a function?

$$R = \{(a_1, b_1), (a_1, b_2), (a_1, b_5)\}$$

$$f(a_1) = \{b_1, b_2, b_5\}$$

$$f: A \rightarrow \mathcal{P}(B)$$

6	9	13	7
12	10	8	
3	5	4	14
15	11	2	1

Relations and Functions

(define (f a)

.....

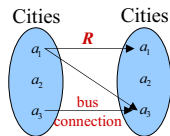
(list b_i))



Relational Properties

A relation on a set A

$$R \subseteq A \times A$$



Relational Properties

Let R be a relation on the set A

Reflexive: $\forall a \in A \ aRa$

Symmetric: $aRb \rightarrow bRa$

Transitive: $aRb \wedge bRc \rightarrow aRc$



Examples

$a R b ::= a$ is parent of b

- Reflexive **NO**
- Symmetric **NO**
- Transitive **NO**



Examples

$a R b ::=$ MIT building a is physically connected to building b

- Reflexive **NO**
- Symmetric **YES**
- Transitive **NO**



Examples

$a R b ::= a < b$ for $a, b \in$ integers

- Reflexive **NO**
- Symmetric **NO**
Actually is asymmetric
- Transitive **YES**



In-Class Problem 1



Relational Properties

R is a relation on the set A

Reflexive: $\forall a \in A \ aRa$

Symmetric: $aRb \rightarrow bRa$

Transitive: $aRb \wedge bRc \rightarrow aRc$



Problem 1

False Theorem:

Suppose R is a relation on A . If R is symmetric and transitive, then R is reflexive.



Counter-example

$R ::= \{(a,a), (a,b), (b,a), (b,b)\}$
on the set $A ::= \{a, b, c\}$

- Symmetric and Transitive
- But **Not Reflexive** since $(c,c) \notin R$



False Proof

1. Let x be an arbitrary element of A .
 $A = \{a, b, c\}$, so $x = a, b$ or c .
2. Let y be any element of A such that xRy .
BUG: $R = \{(a,a), (a,b), (b,a), (b,b)\}$, so **no such y exists** for $x = c$!
3. Since R is symmetric, this implies yRx .
4. Now xRy and yRx , so by transitivity xRx .
5. **Since x was arbitrary**, $\forall x \in A \ xRx$, which proves that R is reflexive. QED.



Types of Relations

Equivalence

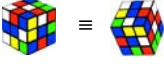
- Reflexive, Transitive, Symmetric.

Partial Orders

- Reflexive, Transitive, Antisymmetric.



Equivalence Relations

- Two names are equivalent if they start with the same letter **Ben \equiv Bob**
- Propositional equivalence $\overline{P \wedge Q} \equiv \overline{P} \vee \overline{Q}$
- Modulo equivalence **$1 \equiv 5 \pmod{4}$**
- Rubik's cube equivalence  \equiv
- Equivalent code (compilers)



Equivalence

$R ::= \{(x,y) \in N \times N \mid \text{the names } x \text{ and } y \text{ start with the same letter}\}$ where N is the set of all names in the 6.042 class

- Reflexive **YES**
- Symmetric **YES**
- Transitive **YES**



Partitions

Theorem:

An equivalence relation on a set A partitions A into disjoint sets



Equivalence Classes

$R ::= \{(x,y) \in N \times N \mid \text{the names } x \text{ and } y \text{ start with the same letter}\}$ where N is the set of all names in the 6.042 class

- {Ackermann, Ada, Alyssa} = [Ackermann]
- {Dijkstra, DeMorgan} = [Dijkstra]
- {Euler, Erdős} = [Euler]



Application: Athena

Example: Athena partitions the filesystem into directories based on the **first two letters of a username**.

```

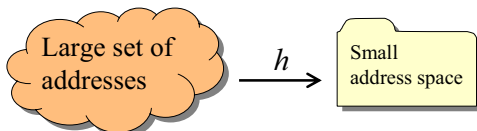
delhi:~$ ssh athena.dialup.mit.edu
Warning: Permanently added host key for IP address '18.7.16.69' to the list of k
nown hosts.
~$ pwd
~/afs/athena.mit.edu/user/r/a/radhi
~$ ls
index.html  raeburn/  raise/    rallen63/  ranib/    raul/
rab/        raj/      raisang/  ralmeida/  ranthony/ raulm/
rabatin/   raf/     raj/      rajph/     rangins/  raup/
rabbaul/   rafaelm/ rajajay/  rajphons/  raul/     ravel/
rabbib/    rafaeln/ raja/     rajphs/    rapa/     raparker/
rabi/      rafal/   rajappa/  rama/      raparkar/ raven/
rabiul/    rafawit/ rajas/    ramanurt/  rapwat/   ravicz/
rabin/     rafel/   rajbansh/ raman/     raposo/   ravir/
rabino/    raffib/  rajdeep/  rameshs/   rappley/  ravr/
rabraff/   raffik/  rajeev/   rameson/   rapson/   ravsegal/
rabrooks/  rafikid/ rajesh/   ramesoni/  rasquel/  rawsis/
irac/      rafiah/  raiestur/ ravin/     raulmea/  raw/

```



Hash Functions

General CS Problem: How do you map a large address space into a smaller address space



So that no collisions occur?

$$\overbrace{h(\langle name1 \rangle)} = \overbrace{h(\langle name2 \rangle)}$$



Equivalence Relation

$$a R b ::= a \equiv b \pmod{4}$$

Reminder:

$$a \equiv b \pmod{4} \leftrightarrow (a - b) = 4k$$

$$(1 - 5) = 4 \times 1 \rightarrow 1 \equiv 5 \pmod{4}$$



Modulo 4

Reflexive: Yes

Symmetric: Yes

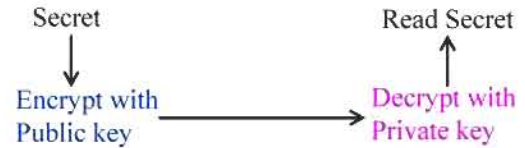
Transitive: Yes

If $(a - b) = 4k$ and $(b - c) = 4l$,
then

$$(a - c) = a - b + b - c = 4(k+l)$$



Application: RSA Cryptography



RSA Cryptography

Compute $M^a \pmod{b}$

- If $x \equiv y \pmod{b}$
- then $x^2 \equiv y^2 \pmod{b}$
– e.g. $1 \equiv 5 \pmod{4}$, $1 \equiv 25 \pmod{4}$

If x is a large number, then can
replace it with any y in the same
equivalence class



In-Class Problems 2 and 3



RSA Cryptography

Public Key $P = (e, n)$

Secret Key $S = (d, n)$

n, d & e are very large ($\gg 128$ bits)

Encrypt: $P(M) = M^e \pmod{n} = C$

Decrypt: $S(C) = C^d \pmod{n} = M$