Relations and Functions

Magritte

Discrete Structures (CS 173)

Gul Agha

Slides based on Derek Hoiem, University of Illinois

Remarks on previous lectures

- Definition of divisibility:

$a \mid b$ *if* $b = a * n$ for some integer n

provided $a \neq 0$

Tautology

- A *tautology* is a logical formula that is true regardless of values assigned to the terms
  - In case of propositional logic, truth assignments (T, F) to the terms
  - In case of predicate logic, values assigned to the variables.

  Examples:

  if p then p

  $p \wedge \neg p = F$

  if $p \wedge \neg p$ then q

Satisfiability

- A logical formula is satisfied by an assignment of values to terms that results in the formula being true
- A logical formula is *satisfiable* if there exists an assignment of values to terms that makes it true.

Example:

if p then True

if p then False

Extended Euclidean Algorithm

gcd (81,57)

81 = 1 (57) + 24

57 = 2 (24) + 9

24 = 2 (9) + 6

9 = 1(6) + **3**

6 = 2(3) + 0

$\mathbf{3} = 9 - 1(6)$

$\mathbf{3} = 9 - (24 - 2(9))$

$= 3(9) - 1(24)$

$= 3(57 - 2(24)) - 1(24)$

$= 3(57) - 7(24)$

$= 3(57) - 7(81 - 1(57))$

$\mathbf{3} = 10(57) - 7(81)$

The gcd(a,b) can be expressed as a *linear combination* of a and b

Inverse in modular arithmetic

y is the inverse of x in $(\text{mod } n)$ if

$$x * y \equiv 1 \ (\text{mod } n)$$

Some crypto algorithms require finding this inverse.

An inverse of x in $(\text{mod } n)$ exists iff $\gcd(x, n) \equiv 1$ *(why?)*

Then: by Extended Euclid's algorithm, there exist p and s such that $p*x + s*n = 1$

So: $p*x = 1 + (-s)n$,

or p $(\text{mod } n)$ is the inverse of x $(\text{mod } n)$

Inverse of x in mod and gcd

Claim: An inverse of x in (mod n) exists iff $\gcd(x, n) = 1$.

Observe: $a \equiv b \pmod{n} \Rightarrow \gcd(a, n) = \gcd(b, n)$ *(why?)*

$xy \equiv 1 \pmod{n} \Rightarrow \gcd(xy, n) = \gcd(1, n)$

But $\gcd(1, n) = 1$, so $\gcd(xy, n) = 1$

Then $\gcd(x, n) = 1$ *(why?)*

GCD and mod

Claim (used on previous page):

$$a \equiv b \pmod{n} \Rightarrow \gcd(a, n) = \gcd(b, n)$$

Proof: $a \equiv b \pmod{n}$

$\Rightarrow \exists m \in \mathbb{Z}\ (a = b + m*n)$ definition

$\Rightarrow \gcd(a, n) = \gcd(b, n)$ *(why?)*

Hint: $\gcd(a, n) \mid a$ and $\gcd(a, n) \mid n$

$\Rightarrow \gcd(a, n) \mid (a - m*n)$

$\Rightarrow \gcd(a, n) \mid b$

$\Rightarrow \gcd(a, n) \leq \gcd(b,n)$

Now apply the argument the other way round to get

$\gcd(b, n) \leq \gcd(a, n)$

Thus $\gcd(b, n) = \gcd(a, n)$

Last Class: Sets

A **set** is an unordered collection of objects

grandfather

Madonna

mother father

Beethoven

sister

my friend

me

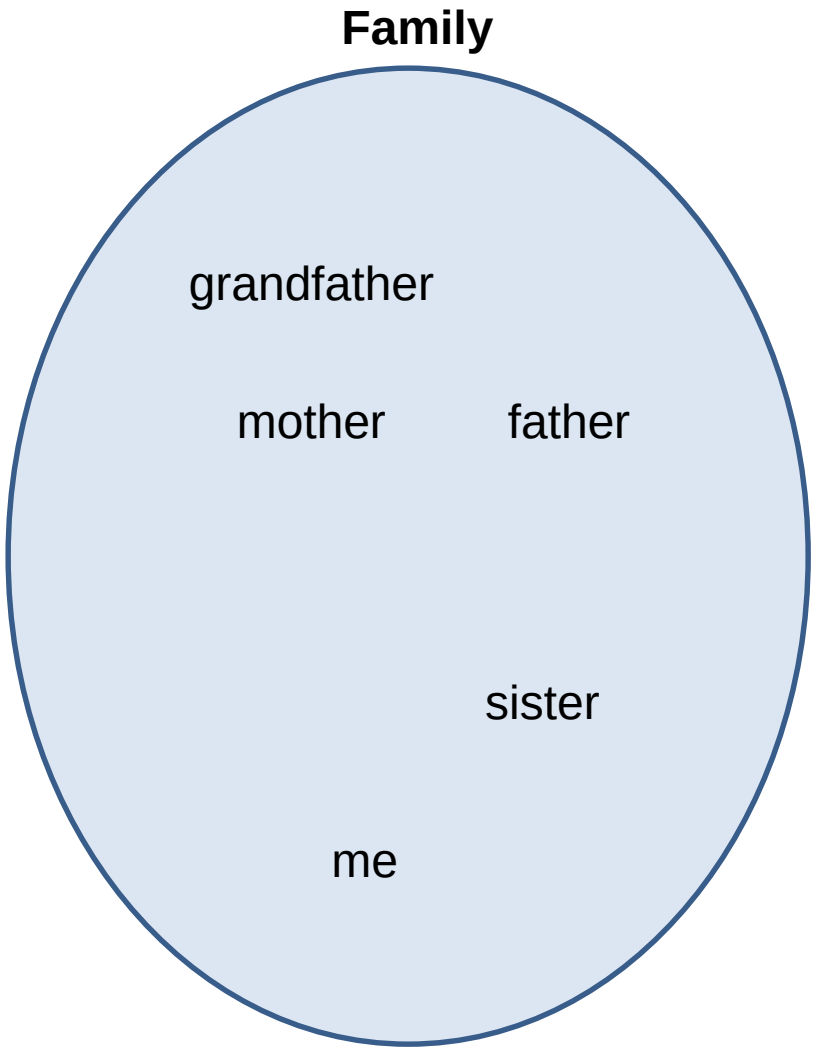
Powersets and Set Difference

A powerset of a set A is the set consisting of all the subsets of A:

$\mathcal{P}(\mathrm{A}) = \{\mathrm{B} \mid \mathrm{B} \subseteq \mathrm{A}\}$

$\mathrm{A} \backslash \mathrm{B}$ is an alternate notation for $\mathrm{A} - \mathrm{B}$

Last Class: Sets

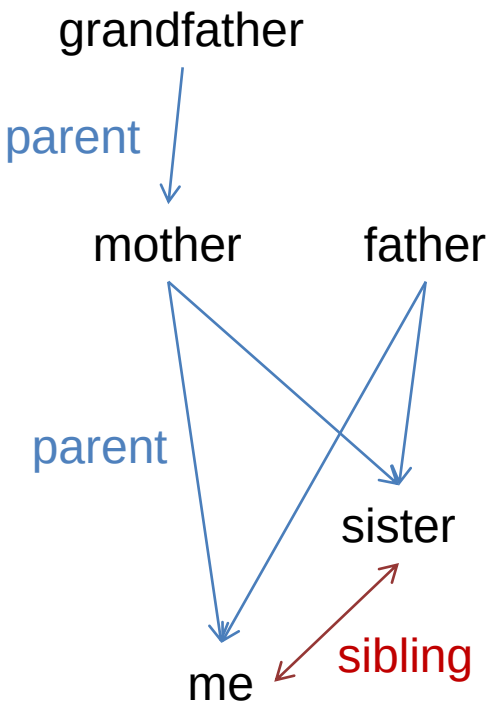


Madonna

Beethoven

my friend

Today's class: Relations



Madonna

Beethoven

my friend

Today's class

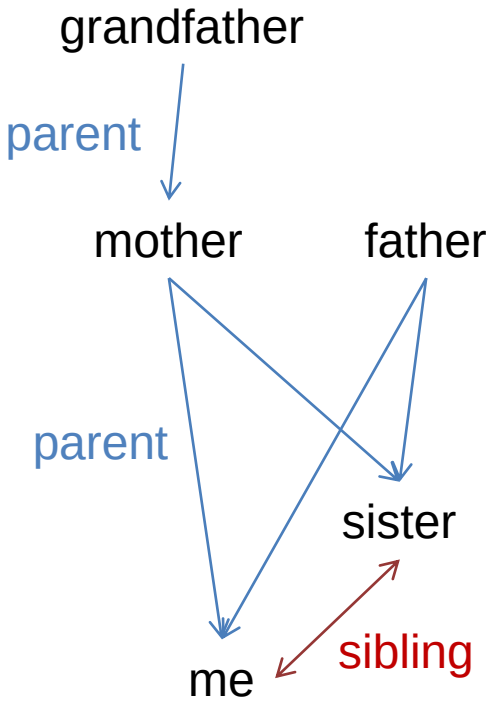
- How to represent relations
- Properties and types of relations: reflexive, symmetric, transitive, partial order, etc.
- Practice proofs with relations

Representing relations

A **relation** R on a set A is a set of ordered pairs of elements from A

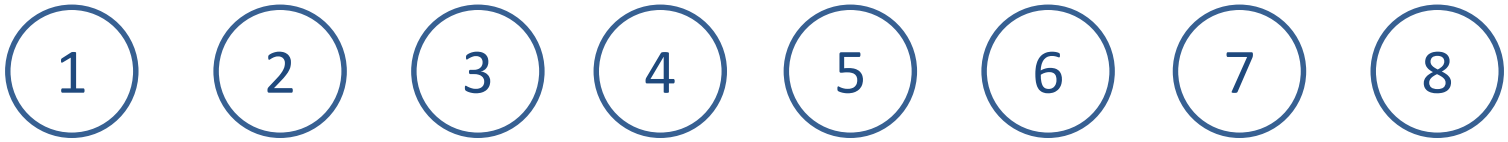
- Consider relation P to stand for "parent" on the set of people
  - mother P me
  - P = {(grandfather, mother), (mother, me), (father, me), (mother, sister), (father, sister)}

- Relation S stands for "sibling"
  - S ={(sister, me), (me, sister)}

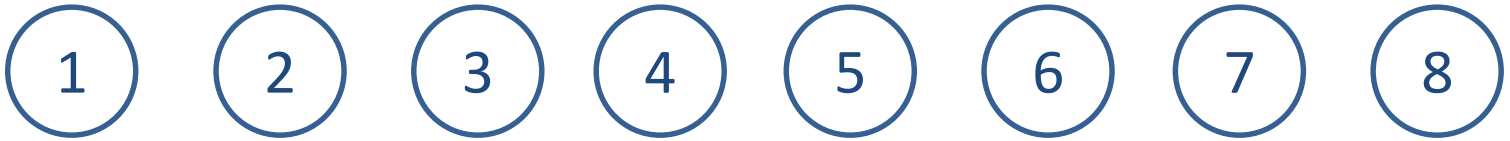


Relations with numbers

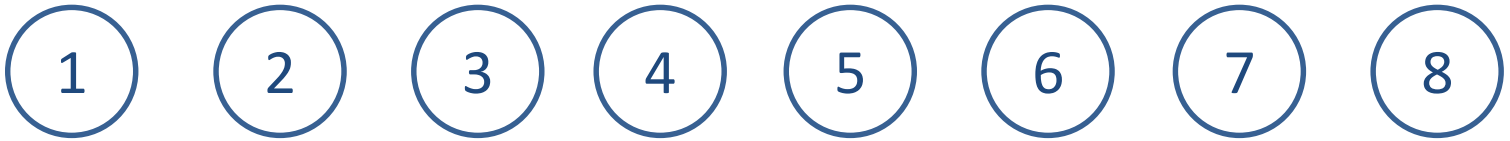
"less than"



"divides"



"congruent mod 3"



overhead

Reflexivity

Reflexive: each element relates to itself

$$For\ all\ x \in A,\ xRx$$

Irreflexive: no element relates to itself

$$For\ all\ x \in A,\ x\not{R}x$$

$\not{R}$ means "R does not hold", i.e. $\neg(xRx)$

1. Is irreflexive the negation of reflexive?
2. What is an example of a reflexive familial relation?
3. Is it irreflexive?
4. What is an example of a number relation that is neither?

Symmetry

Symmetric: $\forall x, y \in A,\ xRy \rightarrow yRx$

Antisymmetric: $\forall x, y \in A$ with $x \neq y,\ \ xRy \rightarrow y\not{R}x$ [1]

or equivalently: $\forall x, y \in A,\ xRy \wedge yRx \rightarrow\ x = y$ [2]

(show that the definition [1] holds iff [2] holds)

What is an example of a symmetric familial relation?

Antisymmetric?

Neither?

Transitivity

Transitive: $\forall x, y, z \in A, xRy \wedge yRz \rightarrow xRz$

What is an example of a familial relation that is transitive? Not transitive?

Practice identifying relation properties

All to self

None to self

If one way then both

Never both ways if not same

if x->y->z, x->z

	Reflexive	Irreflexive	Symmetric	Antisymmetric	Transitive
"less than"					
"divides"					
"congruent mod k"					
"is square of"					

overhead

Disproof of transitive

Claim: “is square of” is not transitive.

Definition: Relation R on set A is transitive iff $\forall x, y, z \in A, xRy \wedge yRz \rightarrow xRz$

overhead

Proof of antisymmetric

Claim: “is square of” is antisymmetric.

Definition: Relation R on set A is antisymmetric if $\forall x, y \in A$ with $x \neq y,\ xRy \rightarrow y\not{R}x$, or equivalently $\forall x, y \in A,\ xRy \wedge yRx \rightarrow x = y$

overhead

Types of relations

Partial order: reflexive, antisymmetric, transitive

Linear order: partial order in which every pair of elements is comparable: $\forall x, y \in A, xRy \text{ x or } yRx$

Strict partial order: irreflexive, antisymmetric, transitive

Equivalence relation: reflexive, symmetric, transitive

Equivalence example

Relation C on R^2: $(x, y)C(a, b)$ iff $x^2 + y^2 = a^2 + b^2$

$[(0,1)]_C$ contains all points on the unit circle

overhead

Proof of equivalence

Claim: “congruent mod k” is an equivalence relation

Definition: An equivalence relation is reflexive, symmetric, and transitive

overhead

Next Lecture..

- Final remarks on relations
- Functions and more functions