Functions

Magritte

Discrete Structures (CS 173)

Gul Agha

Slides based on Derek Hoiem, University of Illinois

REMARKS ON PREVIOUS LECTURES

Example Inverse

Definition: y is the *inverse of* x *in* $(mod\ n)$ iff

$$x * y \equiv 1\ (mod\ n)$$

number	0	1	2	3	4	5
inverse	--	1	--	--	--	5

-- inverse does not exist

1. *Does* 0 *have an inverse in* $(mod\ n)$ for any n?
2. *Is the inverse of* 1 *always* 1 in $(mod\ n)$ for any n?

GCD and mod

Claim: $a \equiv b \,(mod\ n) \Rightarrow \gcd(a,n) = \gcd(b,n)$

Proof: $a \equiv b \,(mod\ n)$

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

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

Hint: $\gcd(b,n) \mid b$ and $\gcd(b,n) \mid m * n$ …

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

Inverse in modular arithmetic

Definition: y is the *inverse of* x *in* $(mod\ n)$ iff

$$x * y \equiv 1\ (mod\ n)$$

Some crypto algorithms require finding this inverse.

If an inverse of x in $(mod\ n)$ exists then

$$\gcd(x, n) \equiv 1 \qquad \textit{(why?)}$$

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 $p\ (mod\ n)$ is the inverse of $x\ (mod\ n)$

Inverse of x in mod and gcd

Claim: If an inverse of x in $(mod\ n)$ exists then $\gcd(x, n) = 1$.
Observe: $a \equiv b\ (mod\ n) \Rightarrow \gcd(a, n) = \gcd(b, n)$

Suppose $x * y \equiv 1\ (mod\ n)$
Then $\gcd(x * y, n) = \gcd(1, n)$

Now $\gcd(1, n) = 1$, so $\gcd(x * y, n) = 1$
We can conclude: $\gcd(x, n) = 1$ *(why?)*

If an inverse of x in $(mod\ n)$ exists **then** $\gcd(x, n) = 1$
is equivalent to
An inverse of x in $(mod\ n)$ exists **only if** $\gcd(x, n) = 1$

Extended Euclidean Algorithm Example

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

Equivalent definitions of Antisymmetry

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

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

Suppose R is antisymmetric:

$$\forall x, y \in A\ (x \neq y \wedge xRy) \rightarrow y\not{R}x$$

Let $xRy \wedge yRx$ be true.

Now yRx implies $y\not{R}x$ is false. Thus $(x \neq y \wedge xRy)$ is false.

But xRy is true, so $x \neq y$ must be false. Thus: $x = y$.

So R antisymmetric implies $\forall x, y \in A,\ xRy \wedge yRx \rightarrow x = y$

Conversely suppose: $\forall x, y \in A,\ xRy \wedge yRx \rightarrow x = y$

Let $(x \neq y \wedge xRy)$.

Now if yRx is true, $xRy \wedge yRx$ is true. So $x = y$.

This contradicts $x \neq y$, so yRx must be false.

Thus: $(x \neq y \wedge xRy) \rightarrow y\not{R}x$ **QED**

Disproof of transitive

Claim: “is square of” is not transitive.

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

Proof by contradiction.

Suppose “is square of” is transitive.

We know: “81 is the square of 9” and “9 is the square of 3”,

By transitivity we can conclude: “81 is the square of 3”.

But 81 is not the square of 3, so the assumption that “is square of” is transitive is false. **QED**

overhead

Proof of antisymmetric

Claim: “is square of” is antisymmetric.

Definition: Relation R on set A is antisymmetric if $\forall x, y \in A,\ xRy \wedge yRx \rightarrow x = y$

Proof: Let R be “is square of”.

Suppose $xRy \wedge yRx$ holds.

Then $x = y^2$ and $y = x^2$

So $x = (x^2)^2$ or $x = x^4$

i.e., $1 = x^3$ or $x = 1$.

Now $y = x^2$ so $y = 12 = 1$.

Thus $x = y$

We have proved: if $xRy \wedge yRx$ holds then $x = y$.

i.e. R is antisymmetric. **QED**

overhead

Proof of equivalence

Claim: “congruent mod k” is an equivalence relation

Definitions: An equivalence relation is reflexive, symmetric, and transitive.

$$a \equiv b \,(mod\, n) \text{ if } \exists m \in \mathbb{Z}\,(a = b + m\, n)$$

Proof:

(1) Reflexive.

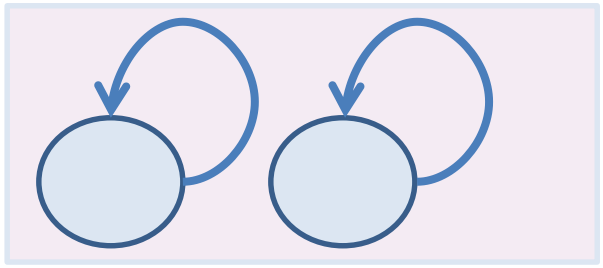
(1) Symmetric

(2) Transitive

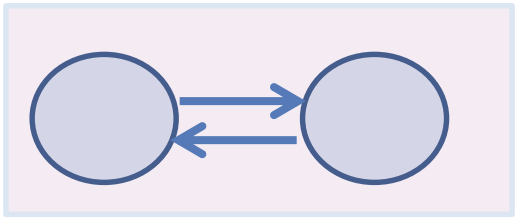
overhead

Relations

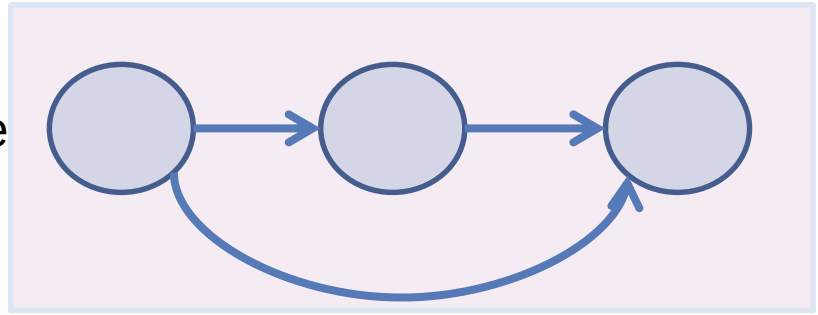
Reflexive

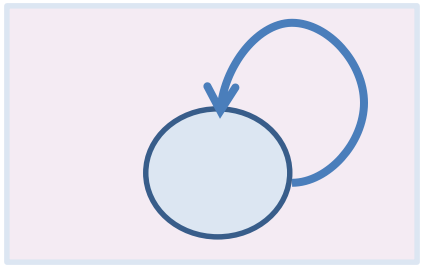


Symmetric



Transitive

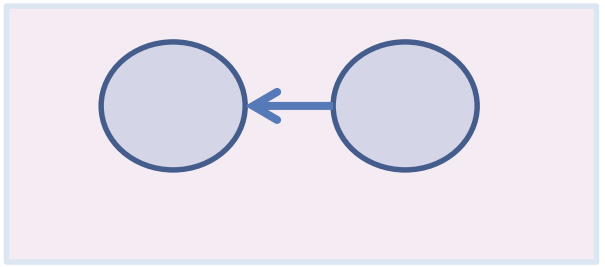




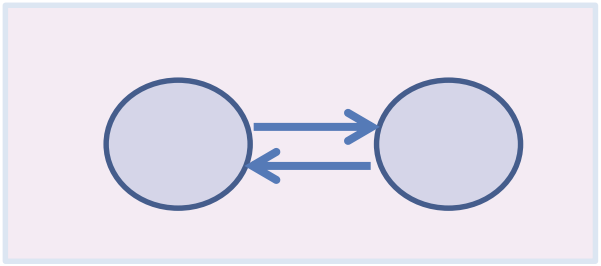
Vacuous truth

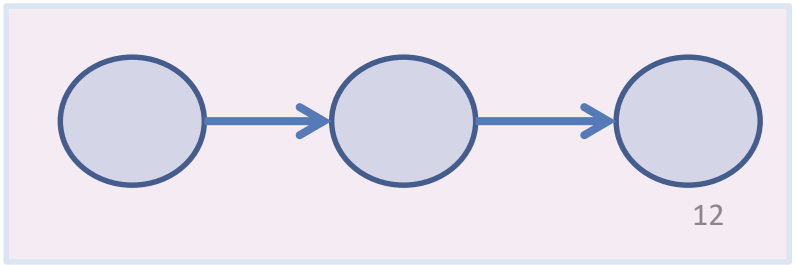
Reflexive, Symmetric and transitive

Irreflexive, Antisymmetric



Not Transitive





Homogeneous and (Heterogeneous) Relations

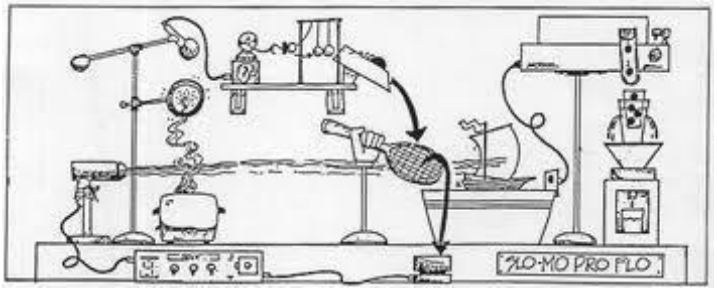
- We defined relations as *homogeneous* relations (i.e., as a subset of *A x A*)
- In general relations can be over any cross-products.
- For any two sets *A* and *B,* a *relation is a subset of A x B*

Some Things to Remember

- How to illustrate a relation graphically
- Be able to identify basic properties of relations: reflexivity, symmetry, transitivity
- Types of relations: partial order, strict partial order, linear order
- When proving (or disproving) a property of a relation, write down definition of relation and property

Functions

- What is a function, and what is not?
- Identify which functions are "*onto*" (or *surjective*)
- Nested quantifiers
  - Mixing "for all" and "there exists"
- Composing functions



What is a function?

Function: is a relation over $A \times B$ which maps each element of A to an element of B, so that an element maps to exactly one element and every element of A is mapped to something, i.e.:

1. $\forall \mathrm{a} \in A \; \exists b \in B, (\mathrm{a}, \mathrm{b}) \in f$
2. $\text{if } (a, b) \in f \text{ and } (a, c) \in f \text{ then } b = c.$

For functions: We write $f(a) = b$ or $f: a \mapsto b$

Functions terminology

$f: A \to B$ stands for f is a map $from\ A\ to$ B

A is the set of '*inputs*'
B is the set of '*outputs*'

Examples of functions

Concepts: mapping; bubbles, plots

Functions: age, t-shirt color, x^2

Functions may be *typed.* In this case, they have a *type signature.*

(In many programming languages, functions are typed).

overhead

What is not a function?

Not a valid function if

1. Some input is not mapped to an output
2. Some input is mapped to two outputs

overhead

When are functions equal?

Functions are equal if

1. They are over the same domain and range.
2. The mapping is the same.

$$f: A \to B \text{ and } g: A \to B \text{ are equal iff}$$
$$\forall a \in A, f(a) = b \text{ iff } g(a) = b$$

Image and Onto

The *image* of a function is the set of values produced when a function is applied to all "inputs"

$$\text{image}(f: A \to B) \subseteq B$$

A function is *onto* or *surjective* if the image is equal to the co-domain (every possible "output" is assigned to at least one input)

$$f: A \to B, \forall y \in B \; \exists x \in A \; f(x) = y$$

overhead

Example:

Claim: $f: R\backslash\{0\} \to R\backslash\{0\}$, $f(x) = 1/x$ is onto.

Recall: $R\ \backslash\{0\}$ is $R\ except\ 0$, i.e. the set of real numbers not including 0.

Definition:

$f: A \to B, f(x)$ is onto iff $\forall y \in B\ \exists x \in A\ f(x) = y$

overhead

Proof of onto

Claim: $f: N^2 \to Z$, $f(x, y) = x - y$ is onto.

Definition: $f: A \to B, f(x)$ is onto iff $\forall y \in B \; \exists x \in A \;\; f(x) = y$

Next Lecture..

- Functions and more functions