# Summary last week

- model questions as problems on discrete structures
- various problems modelled as graph problems
- representing graphs as sets of vertices and edges, and by adjacency matrices
- Floyds shortest path algorithm, stepwise transforming adjacency matrix

# Summary last week

### Theorem

1

The following algorithm overwrites the matrix B with the matrix of distances

For r from 0 to n - 1 repeat: Set N = B. For i from 0 to n - 1 repeat: For j from 0 to n - 1 repeat: Set  $N_{ij} = \min(B_{ij}, B_{ir} + B_{rj})$ . Set B = N.

2

# Summary last week

#### Theorem

The following algorithm overwrites the matrix B with the matrix of distances

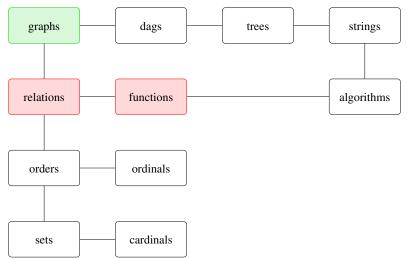
For r from 0 to 
$$n - 1$$
 repeat:  
Set  $N = B$ .  
For i from 0 to  $n - 1$  repeat:  
For j from 0 to  $n - 1$  repeat.  
Set  $N_{ij} = \min(B_{ij}, B_{ir} + B_{rj})$ .  
Set  $B = N$ .

# Course themes

- directed and undirected graphs
- relations and functions
- orders and induction
- trees and dags
- finite and infinite counting
- elementary number theory
- Turing machines, algorithms, and complexity
- decidable and undecidable problem

Proof. today

## Discrete structures



# Properties of Floyd's algorithm

- Does it work? What does that mean, exactly?
- In what language do we express that?
- How do we prove it?
- Why does the algorithm work?
- How fast is it? As a function of what?
- How much memory does it use?
- How do we express this in a computer-independent way?
- ...

3

# Floyd correctness

#### Theorem

Input: adjacency matrix of graph G Output: distance matrix of graph G

### Proof.

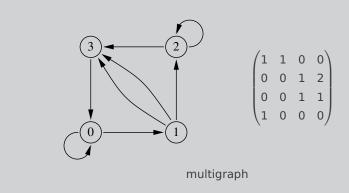
Idea: successively compute distances via subsets of nodes.

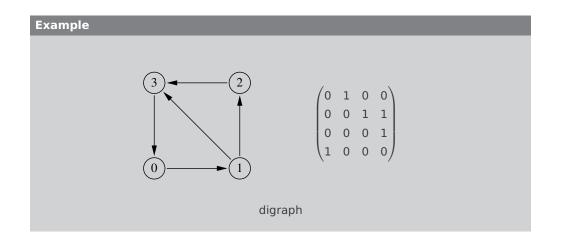
- **1** Pre: distance via empty subset  $\emptyset$  is
  - 0 from node to itself
  - edge weight if edge between distinct nodes
  - $\infty$  if no edge
- 2 (Outer) Loop invariant:

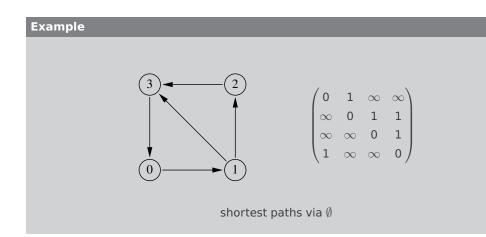
Input: matrix of distances in *G* via nodes  $\{v_0, \ldots, v_{r-1}\}$ Output: matrix of distances in *G* via nodes  $\{v_0, \ldots, v_{r-1}, v_r\}$ 

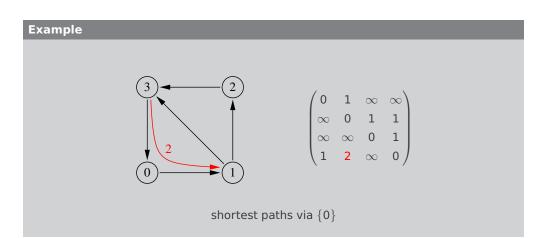
**3** Post: distance via **all** nodes is distance

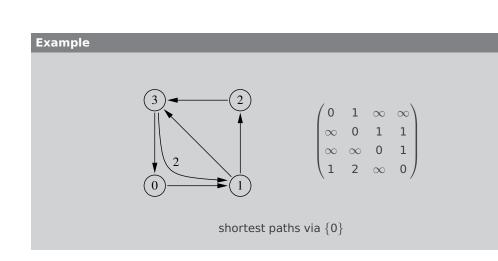
## Example

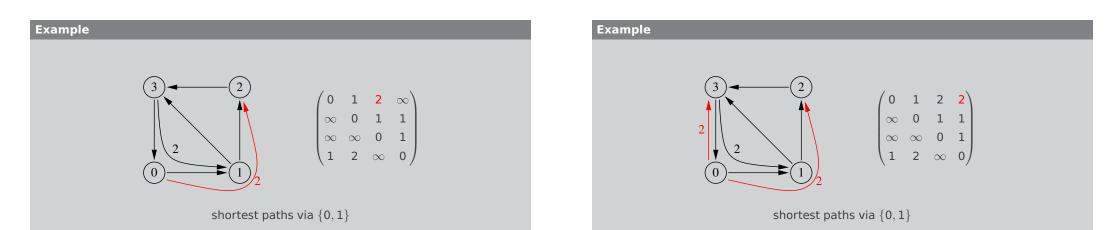


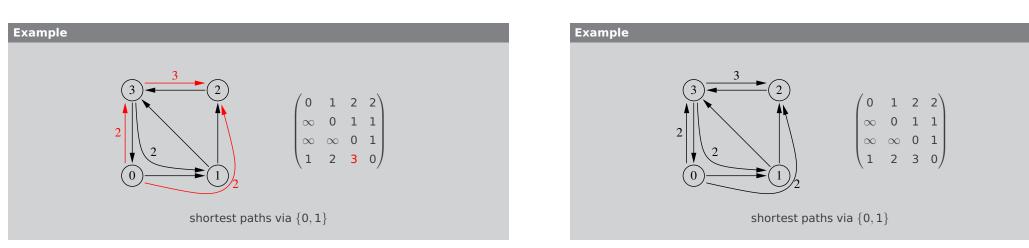


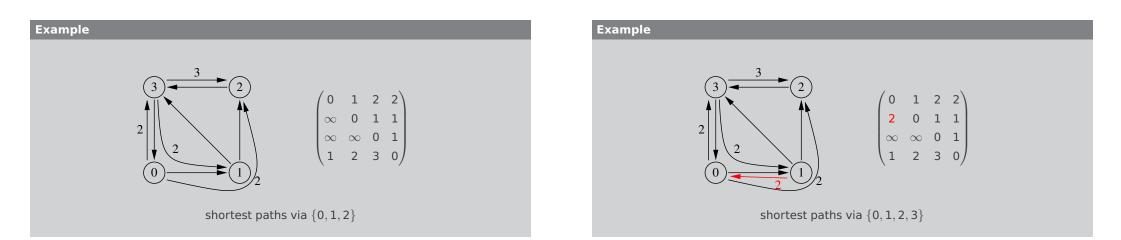


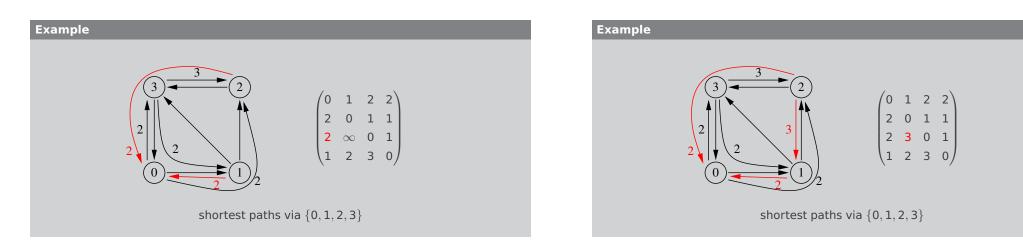


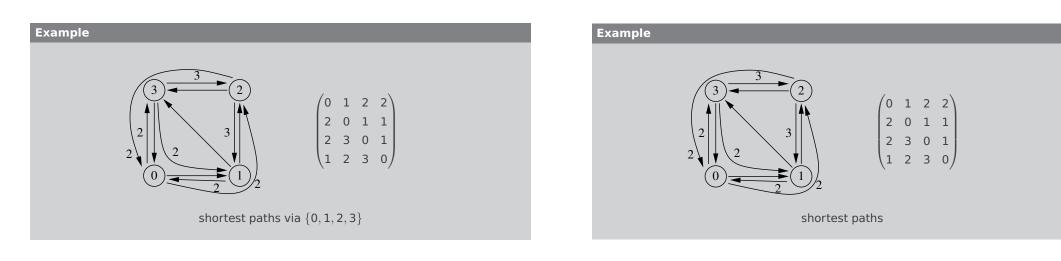












7

# Correctness of middle and inner loop

#### Lemma

Let G be a directed multigraph. If there is a non-empty path p from node c to node d, then there is a simple path from c to d, obtained by omitting edges

#### Observation

Shortest paths are simple

# Indirect proof resp. proof by contradiction

### Definition

- To show that a statement *A* holds, a proof by contradiction assumes that the negation of *A* holds.
- If from this assumption (that the negation of *A* holds, that is, that *A* is false) a contradiction can be deduced, then our assumption itself must have been false, hence *A* must hold.

# Indirect proof resp. proof by contradiction

### Definition

- To show that a statement *A* holds, a proof by contradiction assumes that the negation of *A* holds.
- If from this assumption (that the negation of *A* holds, that is, that *A* is false) a contradiction can be deduced, then our assumption itself must have been false, hence *A* must hold.

#### Example

#### The statement

?There are infinitely many natural numbers.?

true (and therefore a theorem). To show this, we assume the negation of the statement, that is

?There are only finitely many natural numbers.?

## Correctness of middle and inner loop

### **Auxiliary definition**

For  $r \in \{0, 1, ..., n\}$  let  $P_r$  be the set of all shortest paths in the graph of R that only have intermediate nodes in the set  $\{v_0, v_1, ..., v_{r-1}\}$ . Then

## Correctness of middle and inner loop

## Auxiliary definition

For  $r \in \{0, 1, ..., n\}$  let  $P_r$  be the set of all shortest paths in the graph of R that only have intermediate nodes in the set  $\{v_0, v_1, ..., v_{r-1}\}$ . Then

#### Lemma

**1**  $P_0$  is the set of all edges of G and empty paths;

## Correctness of middle and inner loop

### **Auxiliary definition**

For  $r \in \{0, 1, ..., n\}$  let  $P_r$  be the set of all shortest paths in the graph of R that only have intermediate nodes in the set  $\{v_0, v_1, ..., v_{r-1}\}$ . Then

#### Lemma

is

- **1**  $P_0$  is the set of all edges of G and empty paths;
- **2** Assume r < n. For a path p in  $P_{r+1}$  there are two cases:

# Correctness of middle and inner loop

## Auxiliary definition

For  $r \in \{0, 1, ..., n\}$  let  $P_r$  be the set of all shortest paths in the graph of R that only have intermediate nodes in the set  $\{v_0, v_1, ..., v_{r-1}\}$ . Then

#### Lemma

- **1**  $P_0$  is the set of all edges of G and empty paths;
- **2** Assume r < n. For a path p in  $P_{r+1}$  there are two cases:
  - $v_r$  is not an intermediate node of p. Then p in  $P_r$ .

## Correctness of middle and inner loop

### Auxiliary definition

For  $r \in \{0, 1, ..., n\}$  let  $P_r$  be the set of all shortest paths in the graph of R that only have intermediate nodes in the set  $\{v_0, v_1, ..., v_{r-1}\}$ . Then

#### Lemma

9

9

**1**  $P_0$  is the set of all edges of G and empty paths;

- **2** Assume r < n. For a path p in  $P_{r+1}$  there are two cases:
  - $v_r$  is not an intermediate node of p. Then p in  $P_r$ .
  - v<sub>r</sub> is an intermediate node of p. Then we can write the path p from e to d as the composition of a path u from e to v<sub>r</sub>, and a path v from v<sub>r</sub> to d, which are both in P<sub>r</sub>;

# Correctness of middle and inner loop

## Auxiliary definition

For  $r \in \{0, 1, ..., n\}$  let  $P_r$  be the set of all shortest paths in the graph of R that only have intermediate nodes in the set  $\{v_0, v_1, ..., v_{r-1}\}$ . Then

#### Lemma

- **1**  $P_0$  is the set of all edges of G and empty paths;
- **2** Assume r < n. For a path p in  $P_{r+1}$  there are two cases:
  - *v<sub>r</sub>* is not an intermediate node of *p*. Then *p* in *P<sub>r</sub>*.
  - v<sub>r</sub> is an intermediate node of p. Then we can write the path p from e to d as the composition of a path u from e to v<sub>r</sub>, and a path v from v<sub>r</sub> to d, which are both in P<sub>r</sub>;
- $\square$   $P_n$  is the set of all shortest paths in G.

# Complexity of Floyd's algorithm

#### Parameter

#### number of nodes *n* of graph

# Complexity of Floyd's algorithm

### Parameter

number of nodes *n* of graph

### Time

a single operation: unit time 1

#### **1** Pre: initialisation $n^2$

#### 2 Loop:

- assignment (Set N<sub>i</sub>j): 1
- inner loop (j) n times assignment:  $n \cdot 1 = n$
- middle loop (i) n times inner loop:  $n \cdot n = n^2$
- outer loop (*r*) *n* times middle loop:  $n \cdot n^2 = n^3$

copy matrix twice:  $2n^2$ 

## 3 Post: –

total time:  $3n^2 + n^3 \in O(n^3)$  (detailed later) polynomial, cubic  $O(n^3)$ 

# Complexity of Floyd's algorithm

Number of paths by matrix multiplication

### Lemma

Let (V, E, src, tgt) be a directed multigraph having finitely many nodes- and edges with adjacency matrix  $A_{ij} := #(\{e \in E \mid src(e) = v_i \text{ and } tgt(e) = v_j)\}$  for nodes  $v_0, \ldots, v_{n-1}$ .

Number of paths by matrix multiplication

#### Lemma

Let (V, E, src, tgt) be a directed multigraph having finitely many nodes- and edges with adjacency matrix  $A_{ij} := #(\{e \in E \mid src(e) = v_i \text{ and } tgt(e) = v_j)\}$  for nodes  $v_0, \ldots, v_{n-1}$ .

For l ∈ N and i, j = 0, 1, ..., n − 1 is (A<sup>l</sup>)<sub>ij</sub> the number of paths from v<sub>i</sub> to v<sub>j</sub> of length l

10

# Number of paths by matrix multiplication

### Lemma

Let (V, E, src, tgt) be a directed multigraph having finitely many nodes- and edges with adjacency matrix  $A_{ij} := \#(\{e \in E \mid src(e) = v_i \text{ and } tgt(e) = v_j)\}$  for nodes  $v_0, \ldots, v_{n-1}$ .

• For  $\ell \in \mathbb{N}$  and i, j = 0, 1, ..., n - 1 is  $(A^{\ell})_{ij}$  the number of paths from  $v_i$  to  $v_j$  of length  $\ell$ 

## Proof.

How could we prove this?

# **Relations motivation**

#### **Mathematical relations**

used to model ... relations

Example		
• friend		
nemy		
<ul> <li>taller than</li> </ul>		
<ul> <li>sitting next to</li> </ul>		
<ul> <li>superclass</li> </ul>		
•		

# **Relations** definitions

### Definition

- $R \subseteq M \times M$  is a relation on *M*; *R* is
- reflexive, if for all  $x \in M$ ,  $(x, x) \in R$
- irreflexive, if for all  $x \in M$ ,  $(x, x) \notin R$
- symmetric, if for all  $x, y \in M$  $(x,y) \in R \Rightarrow (y,x) \in R$
- anti-symmetric, if for all  $x, y \in M$  $(x, y) \in R$  und  $(y, x) \in R \Rightarrow x = y$
- transitive, if for all  $x, y, z \in M$  $(x,y) \in R$  und  $(y,z) \in R \Rightarrow (x,z) \in R$

# **Relations** definitions

Definition
$R \subseteq M \times M$ is a relation on <i>M</i> ; <i>R</i> is
• reflexive, if for all $x \in M$ , $(x, x) \in R$
• irreflexive, if for all $x \in M$ , $(x, x) \notin R$
• symmetric, if for all $x, y \in M$
$(x,y) \in R \Rightarrow (y,x) \in R$
• anti-symmetric, if for all $x, y \in M$
$(x,y) \in R$ und $(y,x) \in R \Rightarrow x = y$

• transitive, if for all  $x, y, z \in M$  $(x, y) \in R$  und  $(y, z) \in R \Rightarrow (x, z) \in R$ 

### Remark

Homogeneous binary relations (heterogeneous *n*-ary relation  $\subseteq M_1 \times \ldots \times M_n$ )

11

- *R*<sub>1</sub> := friend on set of people
- R<sub>2</sub> := enemy on set of people
- *R*<sub>3</sub> := taller than on set of people
- *R*<sub>4</sub> := sitting next to on set of people in classroom
- $R_5 :=$  being superclass of in Java program  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
<i>R</i> <sub>1</sub>	√?	×?	√?	×	×
R <sub>2</sub>					
R <sub>3</sub>					
<i>R</i> <sub>4</sub>					
<i>R</i> <sub>5</sub>					

#### Example

- *R*<sub>1</sub> := friend on set of people
- $R_2 :=$  enemy on set of people
- *R*<sub>3</sub> := taller than on set of people
- *R*<sub>4</sub> := sitting next to on set of people in classroom
- $R_5 :=$  being superclass of in Java program  $\varnothing$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
$R_1$	√?	×?	√?	×	×
R <sub>2</sub>	×?	√?	√?	×	×
R <sub>3</sub>					
R <sub>4</sub>					
<i>R</i> <sub>5</sub>					

#### Example

- *R*<sub>1</sub> := friend on set of people
- *R*<sub>2</sub> := enemy on set of people
- $R_3 :=$  taller than on set of people
- *R*<sub>4</sub> := sitting next to on set of people in classroom
- $R_5 :=$  being superclass of in Java program  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
R <sub>1</sub>	√?	×?	√?	×	×
R <sub>2</sub>	×?	√?	√?	×	×
R <sub>3</sub>	×	$\checkmark$	×	$\checkmark$	$\checkmark$
R <sub>4</sub>					
<i>R</i> <sub>5</sub>					

#### Example

- *R*<sub>1</sub> := friend on set of people
- *R*<sub>2</sub> := enemy on set of people
- *R*<sub>3</sub> := taller than on set of people
- *R*<sub>4</sub> := sitting next to on set of people in classroom
- $R_5 :=$  being superclass of in Java program  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
<i>R</i> <sub>1</sub>	√?	×?	√?	×	×
R <sub>2</sub>	×?	√?	√?	×	×
<i>R</i> <sub>3</sub>	×	$\checkmark$	×	$\checkmark$	$\checkmark$
R <sub>4</sub>	×	$\checkmark$	×	×	×
<i>R</i> <sub>5</sub>					

14

- *R*<sub>1</sub> := friend on set of people
- $R_2 :=$  enemy on set of people
- *R*<sub>3</sub> := taller than on set of people
- $R_4 :=$  sitting next to on set of people in classroom
- $R_5 :=$  being superclass of in Java program  $\varnothing$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
R <sub>1</sub>	√?	×?	√?	×	×
R <sub>2</sub>	×?	√?	√?	×	×
R <sub>3</sub>	×	$\checkmark$	×	$\checkmark$	$\checkmark$
R <sub>4</sub>	×	$\checkmark$	×	×	×
<i>R</i> <sub>5</sub>	√?	×?	×	$\checkmark$	$\checkmark$

## Example

- $R_1 := \{(0,0), (1,1), (2,2)\}$  on  $\{0,1,2\}$
- $R_2 := \emptyset$  on  $\{0\}$
- $R_3 := \{(0,0), (2,1)\}$  on  $\{0,1,2\}$
- $R_4 := \{(0,0), (1,2), (2,1)\}$  on  $\{0,1,2\}$
- $R_5 := \emptyset$  on  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
$R_1$	$\checkmark$	×	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>2</sub>					
R <sub>3</sub>					
R <sub>4</sub>					
<i>R</i> <sub>5</sub>					

#### Example

- $R_1 := \{(0,0), (1,1), (2,2)\}$  on  $\{0,1,2\}$
- $R_2 := \emptyset$  on  $\{0\}$
- $R_3 := \{(0,0), (2,1)\}$  on  $\{0,1,2\}$
- $R_4 := \{(0,0), (1,2), (2,1)\}$  on  $\{0,1,2\}$
- $R_5 := \emptyset$  on  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
R <sub>1</sub>	$\checkmark$	×	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>2</sub>	×	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>3</sub>					
R <sub>4</sub>					
R <sub>5</sub>					

### Example

- $R_1 := \{(0,0), (1,1), (2,2)\}$  on  $\{0,1,2\}$
- $R_2 := \emptyset$  on  $\{0\}$
- $R_3 := \{(0,0), (2,1)\}$  on  $\{0,1,2\}$
- $R_4 := \{(0,0), (1,2), (2,1)\}$  on  $\{0,1,2\}$
- $R_5 := \emptyset$  on  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
R <sub>1</sub>	$\checkmark$	×	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>2</sub>	×	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>3</sub>	×	×	×	$\checkmark$	$\checkmark$
<i>R</i> <sub>4</sub>					
<i>R</i> <sub>5</sub>					

14

- $R_1 := \{(0,0), (1,1), (2,2)\}$  on  $\{0,1,2\}$
- $R_2 := \emptyset$  on  $\{0\}$
- $R_3 := \{(0,0), (2,1)\}$  on  $\{0,1,2\}$
- $R_4 := \{(0,0), (1,2), (2,1)\}$  on  $\{0,1,2\}$
- $R_5 := \emptyset$  on  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
<i>R</i> <sub>1</sub>	$\checkmark$	×	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>2</sub>	×	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
<i>R</i> <sub>3</sub>	×	×	×	$\checkmark$	$\checkmark$
<i>R</i> <sub>4</sub>	×	×	$\checkmark$	×	×
<i>R</i> <sub>5</sub>					

#### Example

- $R_1 := \{(0,0), (1,1), (2,2)\}$  on  $\{0,1,2\}$
- $R_2 := \emptyset$  on  $\{0\}$
- $R_3 := \{(0,0), (2,1)\}$  on  $\{0,1,2\}$
- $R_4 := \{(0,0), (1,2), (2,1)\}$  on  $\{0,1,2\}$
- $R_5 := \emptyset$  on  $\emptyset$

	reflexive	irreflexive	symmetric	anti-symmetric	transitive
R <sub>1</sub>	$\checkmark$	×	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>2</sub>	×	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
R <sub>3</sub>	×	×	×	$\checkmark$	$\checkmark$
R <sub>4</sub>	×	×	$\checkmark$	×	×
R <sub>5</sub>	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$

15

# Closures

#### Definition

Let *P* be a property of relations. The *P*-closure of *R* is the least relation R' such that  $R \subseteq R'$  and R' has property *P*.

## Closures

## Definition

Let *P* be a property of relations. The *P*-closure of *R* is the least relation R' such that  $R \subseteq R'$  and R' has property *P*.

#### Remark

Only well-defined if it exists and is unique. E.g. if a relation is reflexive an irreflexive extension does not exist, and extending the empty relation on  $\{a, b\}$  such that a and b are related in some way is not *unique* (two choices).

# Closures

### Definition

Let *P* be a property of relations. The *P*-closure of *R* is the least relation R' such that  $R \subseteq R'$  and R' has property *P*.

## Notations

 $R^{=}$  is the reflexive closure of R,  $R^{+}$  its transitive closure,  $R^{*}$  its reflexive-transitive closure.

# Closures

### Definition

Let *P* be a property of relations. The *P*-closure of *R* is the least relation R' such that  $R \subseteq R'$  and R' has property *P*.

#### Notations

 $R^{=}$  is the reflexive closure of R,  $R^{+}$  its transitive closure,  $R^{*}$  its reflexive–transitive closure.

## Example

The transitive closure of friendship and enemy relates everyone to everyone?, of being taller than and superclass are the relation themselves, and of sitting next to is sitting in the same row.

# Algorithm of Warshall, transitive closure

#### Theorem

- **1** Let R be a relation on a set M with n elements and let A be its adjacency matrix
- **2** The following algorithm with  $O(n^3)$  bit operations overwrites A with the adjacency matrix of the transitive closure of R

For r from 0 to 
$$n - 1$$
 repeat:  
Set  $N = A$ .  
For i from 0 to  $n - 1$  repeat:  
For j from 0 to  $n - 1$  repeat:  
Set  $N_{ij} = max(A_{ij}, A_{ir} \cdot A_{rj})$   
Set  $A = N$ .

### Example

The transitive closure of the relation  $R = \{(0,2), (1,0), (2,1)\}$  on the set  $\{0,1,2\}$  is  $T = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$ 

16

The transitive closure of the relation  $R = \{(0,2), (1,0), (2,1)\}$  on the set  $\{0,1,2\}$  is  $T = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$ 

Adjacency matrix and first iteration (r = 0)

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \qquad A_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Second (r = 1) and third (r = 2) iteration

$$A_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad \qquad A_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

# Relations as digraphs

#### Definition

Let R be a relation on a set M. Then the digraph of R is given by:

- the set of nodes M
- the set of edges R
- the functions src((x, y)) = x and tgt((x, y)) = y

## Graph notions apply to relation

Notions for graphs apply to a relation *R* via its graph.

# Relations as digraphs

## Graph notions apply to relation

Notions for graphs apply to a relation R via its graph.

#### Example

Let G be the graph of the relation R

- *R* is reflexive iff all nodes of *G* have a loop
- *R* is reflexive and transitive iff for every path from *a* to *b* there is an edge from *a* to *b* in *G*
- *R* is symmetric iff for every edge from *a* to *b* in *G* there is an edge from *b* to *a*

• ...

# Relations as digraphs, Warshall as Floyd

## Graph notions apply to relation

Notions for graphs apply to a relation *R* via its graph.

### Theorem

Let R be a relation. R\* can be obtained from the distance matrix of R by mapping  $\infty$  to 0 and natural numbers to 1.

## Proof.

The correspondence holds for every stage of Warshall's algorithm applied to  $R^{=}$  and Floyd's algorithm applied to the adjacency matrix of R.

18

# Functions as relations

### Definition

A function on *M* is a relation *R* on *M* such that

for all  $x \in M$ , there exists y such that x R y (totality)

**2** for all  $x, y, y' \in M$  if x R y and x R y' then y = y', i.e. R relates uniquely.

we then write R(x) to denote y.

# Functions as relations

#### Definition

A function on *M* is a relation *R* on *M* such that

**1** for all  $x \in M$ , there exists y such that x R y (totality)

**2** for all  $x, y, y' \in M$  if x R y and x R y' then y = y', i.e. R relates uniquely.

we then write R(x) to denote y.

#### Example

20

- The squaring function on natural numbers is the relation {(0,0), (1,1), (2,4), (3,9), (4,16), ...}.
- Taking the square root is not a function on natural numbers, since, e.g., the square root of 2 is not a natural number (existence fails)
- Taking the square root is not a function on the real numbers either, since, e.g., both -2 and 2 are square roots of 4 (uniqueness (also) fails)

# Functions as relations

#### Definition

A function on *M* is a relation *R* on *M* such that

**1** for all  $x \in M$ , there exists y such that x R y (totality)

**2** for all  $x, y, y' \in M$  if x R y and x R y' then y = y', i.e. R relates uniquely.

we then write R(x) to denote y.

### Specification of functions

A function is said to be **defined** by some specification this expresses that there **exists** a **unique** relation satisfying the specification and the relation is a **function**.

## Example

The function *f* on natural numbers defined by

• 
$$f(n) = n? \checkmark \text{or } f(n) = -1? \times \text{or } f(n) = f(n)? \times$$

• 
$$f(0) = 10$$
 and  $f(1) = 2? \times \text{or } f(0) = 0$  and  $f(n+1) = f(n)? \checkmark ...$