Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Prof. Dr.-Ing. Sebastian Schlesinger
Department 2 - Dual Studies Economics & Tech

Exercises to the lecture

Security

HWR Berlin, winter term 2023/2024

Prof. Dr.-Ing. Sebastian Schlesinger
Blatt 1

Aufgabe 1.1 (Python for Relations and Functions) (15 Punkte)

Write a Python program that follows the following specification:

- It contains a class representing a relation,
- an inheriting class representing a function,
- and an inheriting class representing a relation that acts upon a single supporting set.
- The constructor of the base class should be able to consume the supporting sets and a list of pairs to form the relation.
- Methods to calculate the adjacency matrix,
- to check if they are reflexive,
- antisymmetric,
- symmetric,
- transitive,
- an order, or
- an equivelance relation should be provided.

Also based on the following definition, an operation should be added to compose two relations. The definition is as follows: For two Relations $R \subseteq M \times N$ and $S \subseteq N \times P$, the **composition** $R \circ S$ is a new relation defined as follows:

$$R \circ S := \{(x, z) \in M \times P | \exists y \in N : (x, y) \in R \wedge (y, z) \in S\}$$

Aufgabe 1.2 (Sieve of Eratosthenes) (5 Punkte)

Given a list of the first positive natural numbers > 1 up to a limit n, i.e., the list $[2, 3, 4, ..., n]$, the **Sieve of Eratosthenes** calculates the prime numbers in that interval.

It proceeds as follows: In each iteration, take the lowest number that has not been erased yet (in the first iteration it is simply the number 2), and erase all multiples of that number in the current list until you reach the end of the list. Do that until you have reached the end of the list. The remaining numbers, i.e., the numbers that have not been erased at the end of this process are the primes.

Implement that algorithm!

Aufgabe 1.3 (Adjacency Matrix) (3 Punkte)

Let $R = \{(1, 1), (2, 2), (1, 3), (2, 3), (2, 1), (3, 1)\}$ be a relation on the set $M = \{1, 2, 3\}$. Determine the adjacency matrix and decide if it is reflexive, antisymmetric, symmetric, or transitive.

Aufgabe 1.4 (Subset as Relation) (5 Punkte)

For a set M, the **power set** of M ist defined as $\mathcal{P}(M) = \{A \subseteq M\}$, i.e., the set of all sets that are a subset of M.

For example, if $M = \{1, 2\}$, then $\mathcal{P}(M) = \{emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Consider the subset relation on the power set of a set M, i.e., consider the relation $R \subseteq \mathcal{P}(M) \times \mathcal{P}(M)$ with $(A, B) \in R \Leftrightarrow A \subseteq B$.

Prove that this relation is an order and draw the Hasse diagram for R if $M = \{1, 2, 3\}$.

Aufgabe 1.5 (Transitive Hull) (10 Punkte)

For an arbitrary relation $R \subseteq M \times M$, the **transitive hull** is defined as the smallest relation containing R that is transitive. By *smallest*, we mean in the sense of the subset relation, i.e., the transitive hull is a relation R_{trans} such that there exists no other relation R' with $R \subseteq R' \subseteq R_{trans}$ and R' being transitive.

(i) Consider the relation $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (3, 2), (2, 4)\}$ on the set $M = \{1, 2, 3, 4\}$. Which pairs would need to be added to make it transitive, i.e., to form the transitive hull?

(ii) Visualise the relation and its transitive hull as graphs.

(iii) An algorithmic way to calculate the transitive hull is given via the equation $R_{trans} = \bigcup_{n \in \mathbb{N}} R^n$, where R^n is the composition of the relation R with itself (composition defined in the first exercise) executed n times. In other words: $R^0 = Id$, $R^{n+1} = R^n \circ R$, where Id is the identity relation. Extend your Python program from the first exercise by a function to calculate the transitive hull. *Note that in the formula, the unification is done over all natural numbers, while for finite relations like in our cases, the algorithm stops as soon as no changes occur in a step of the algorithm.*

Aufgabe 1.6 (Equivalance Relations, Partitions, Functions) (5 Punkte)

Let $X = \{1, 2, 3, 4, 5, 6, 7, 8\}, Y = \{a, b, c\}$, and $f : X \to Y$ be defined by: $f(1) = a$, $f(2) = a$, $f(3) = c$, $f(4) = b$, $f(5) = a$, $f(6) = b$, $f(7) = c$, $f(8) = a$.

(i) Write down $f^{-1}(\{a\})$, $f^{-1}(\{b\})$, $f^{-1}(\{c\})$. Observe that they realize a partition of X. *Note that for a function $f : M \to N$, then $f^{-1}(A) = \{x \in M | \exists y \in A : y = f(x)\}$*

(ii) Define $x_1 \sim x_2$ when $f(x_1) = f(x_2)$. Check that $\sim$ satisfies the conditions of an equivalence relation. What are the equivalence classes?

Aufgabe 1.7 (Factor Group) (5 Punkte)

Consider the factor group $(\mathbb{Z}/5\mathbb{Z})^* = \{[1], [2], [3], [4]\}$, which is (in this simplified context) the same as $\mathbb{Z}/5\mathbb{Z}$ without the $[0]$. Now, we consider the multiplication on $(\mathbb{Z}/5\mathbb{Z})^*$ as

$$[x] \cdot [y] := [x \cdot y]$$

Draw a number line (Zahlenstrahl) for the representatives of $(\mathbb{Z}/5\mathbb{Z})^* = \{[1], [2], [3], [4]\}$, calculate $[2]^i$ for $i = 0, 1, \ldots$ and highlight those steps on the number line.