3 Relations

A predicate $P(x_1, \ldots, x_n)$ with more than one variable can describe a relation between n objects. In this section we will consider only binary relations, $P(x, y)$, which can be used e.g. to describe data in a database. We will consider the mathematical concepts underlying such relations, making use of set theoretical tools.

3.1 Basic Concepts

Consider the predicate

$$P(x, y) : \ x \text{ is a parent of } y,$$

where x and y range over the set H of all humans (this is the domain of discourse). $P(x, y)$ is a quintessential example of a binary relation, i.e. a relation between two objects. If we substitute particular humans for x and y we obtain a proposition, e.g. P(Ada Lovelace, Socrates), which can be true or false. (In this example it is false.) Note that $P(x, y)$ is fully determined by the truth values of $P(x, y)$ for all possible combinations of x and y.

A bit more generally, we will consider relations between two sets, A and B, with $x \in A$ and $y \in B$. Instead of considering a predicate $P(x, y)$, we will think of a relationship as the set of pairs $(x, y) \in A \times B$ for which $P(x, y)$ is true.

Definition 3.1 *A* binary relation R *from a set A to a set B is a subset $R \subseteq A \times B$. We say that $x \in A$ and $y \in B$ are related by the relation R if and only if $(x, y) \in R$. We call A the* domain *and B the* codomain *of the relation. If $B = A$ we call R a relation on A.*

Example 3.2 *The following are examples of relations:*

1. *Let S be the set of current DCU students and M the set of module currently offered. There is a relation $R \subseteq S \times M$ which describes exactly which students are currently registered for which modules. For every student and every module we can say whether the student is registered for the module or not.*

2. *Consider the relation between two copies of $\mathbb{R}$ given by the subset $R = \{(x, y) \in \mathbb{R}^2 |\ x \leq y\}$ of $\mathbb{R} \times \mathbb{R}$. The predicate corresponding to this relation is $P(x, y) : \ x \leq y$, because $(x, y) \in R$ if and only if $x \leq y$.*

Remark 3.3 *It is sometimes useful to write a relation using a different notation, namely xRy instead of $(x, y) \in R$. In particular, if we write $\leq$ instead of R for the last relation in Example 3.2, then $\leq$ is a funny name for a subset of $\mathbb{R} \times \mathbb{R}$, but the notation $x \leq y$ instead of $(x, y) \in \leq$ is in line with common usage.*

If A and B are finite sets, then $A \times B$ is also finite and hence so is $\mathcal{P}(A \times B)$. This means that there are only finitely many different relations between A and B. The number of such relations is $|\mathcal{P}(A \times B)| = 2^{|A \times B|} = 2^{|A| \cdot |B|}$. If $R = \varnothing$, then no elements of A and B are related. If $R = A \times B$, all elements of A and B are related.

Example 3.4 *Let $A = \{a, b\}$ and $B = \{1, 2, 3\}$. Then there are $2^6 = 64$ different relations. E.g., there are 6 relations in which exactly one element of A is related to exactly two elements of B: these are the relations $\{(a, 1), (a, 2)\}$, $\{(a, 1), (a, 3)\}$, $\{(a, 2), (a, 3)\}$, $\{(b, 1), (b, 2)\}$, $\{(b, 1), (b, 3)\}$ and $\{(b, 2), (b, 3)\}$.*

3.2 Representing Relations

When A and B are both finite sets we can represent a relation $R \subseteq A \times B$ using a *relation matrix*. For this we first order the elements of A and B, e.g. $A = \{x_1, x_2, \ldots, x_m\}$ for some $m \in \mathbb{N}$ and $B = \{y_1, x_2, \ldots, y_n\}$ for some $n \in \mathbb{N}$. The relation matrix is then a rectangular array of size $m \times n$ with entries T or F such that for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ the entry on the i^{th} row and in the j^{th} column is T exactly when $(x_i, y_j) \in R$.

Example 3.5 *If $A = \{2, 4\}$ and $B = \{1, 3, 5\}$ (with the given ordering), then $R = \{(x, y) \in A \times B |\ x \leq y\}$ has the relation matrix*

$$\begin{pmatrix} \mathrm{F} & \mathrm{T} & \mathrm{T} \\ \mathrm{F} & \mathrm{F} & \mathrm{T} \end{pmatrix}.$$

For large sets the relation matrix also gets very large, but they can be handled well by a computer.

Example 3.6 *If $A = B$ is the set of all web pages and R is the relation "web page x links to web page y", then a variation of the corresponding relation matrix is used to compute the pagerank of each web page. This is done regularly by Google in what is often called the largest matrix calculation in the world.*

When the sets A and B are small enough we can also represent a relation R between A and B graphically as follows. We draw a point for each element of $A \cup B$ and when $(x, y) \in R$ we draw an arrow from the point corresponding to x to the point corresponding to y. The result is a so-called *directed graph*.

Example 3.7 *The directed graph for the relation R of Example 3.5 is given in Figure 3.*

When $B = A$ we have $A \cup A = A$. In this case the directed graph of a relation may also have arrows from a point to itself.

Example 3.8 *Let $A = \{1, 2\}$ and let R be the relation on $\mathcal{P}(A)$ given by $R = \{(X, Y) \in \mathcal{P}(A) \| \ X \subseteq Y\}$. Then $\mathcal{P}(A)$ and R can be written down explicitly as*

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$$
$$R = \{(\varnothing, \varnothing), (\varnothing, \{1\}), (\varnothing, \{2\}), (\varnothing, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\})\}$$

and the directed graph for R is given in Figure 3.

3.3 Operations on Relations

In this section we will consider several ways to construct new relations from given ones. One option is to recall that a relation is a subset of $A \times B$, so we can use set operations like union, intersection or complement (in $A \times B$) to create new relations.

Example 3.9 *If H is the set of humans we can define a relation R on H by $(x, y) \in R$ if and only if x is older than y. We can also define a relation S on H by $(x, y) \in S$ if and only if x is a sibling of y. Then $R \cap S$ is the relation "x is an older sibling of y", because $(x, y) \in R \cap S$ if and only if x is older than y and x is a sibling of y.*

Apart from these set theoretic operations there are other operations that are often very useful.

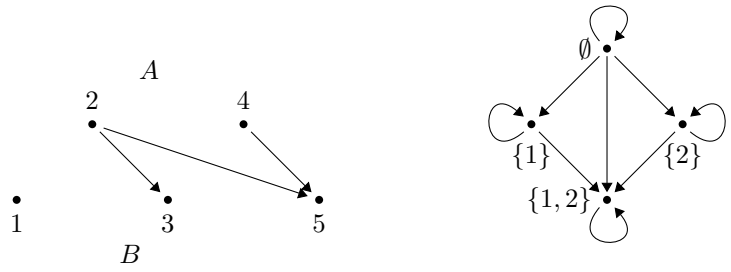

Figure 3: The directed graphs corresponding to the relations in Example 3.5 (on the left) and Example 3.8 (on the right).

3.3.1 The inverse relation

Definition 3.10 *If R is a relation from a set A to a set B, the* inverse relation R^{-1} *is the relation from B to A such that $(x, y) \in R^{-1}$ if and only if $(y, x) \in R$.*

Example 3.11 *On the set H of all humans, the inverse of the relation "x is a parent of y" is the relation "y is a child of x".*

Note that $(R^{-1})^{-1} = R$. The relation matrix of R^{-1} is obtained from the relation matrix of R by reflecting in the diagonal. (This turns an $m \times n$-matrix into an $n \times m$-matrix.) The directed graph of R^{-1} is obtained from the directed graph of R by reversing the direction of every arrow.

Example 3.12 *For $A = \{1, 2, 3\}$ and $B = \{a, b\}$ consider the relation $R = \{(1, a), (1, b), (3, b)\}$. Then $R^{-1} = \{(a, 1), (b, 1), (b, 3)\}$. The relation matrices are*

$$\begin{pmatrix} \mathrm{T} & \mathrm{T} \\ \mathrm{F} & \mathrm{F} \\ \mathrm{F} & \mathrm{T} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathrm{T} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{T} \end{pmatrix}$$

respectively. The directed graphs are shown in Figure 4.

Figure 4: The directed graphs corresponding to the relations R (on the left) and R^{-1} (on the right) of Example 3.12. Note that the two graphs are mirror images of each other, except for the direction of the arrows.

3.3.2 Composition of relations

Definition 3.13 *If R is a relation from a set A to a set B and S is a relation from B to a set C, then the* composition *of S with R, written as $S \circ R$, is the relation from A to C such that $(x, y) \in S \circ R$ if and only if there is a $z \in B$ such that $(x, z) \in R$ and $(z, y) \in S$.*

Example 3.14 *If H is the set of humans we can define a relation R on H by $(x, y) \in R$ if and only if x is a child of y. We can also define a relation S on H by $(x, y) \in S$ if and only if x is a sibling of y. Then $S \circ R$ is the relation "x is an aunt or uncle of y", because $(x, y) \in S \circ R$ if and only if there is a $z \in H$ such that $(x, z) \in R$ and $(z, y) \in S$, i.e. x is a child of z and z is a sibling of y.*

The directed graph of the composition $S \circ R$ can be constructed from the directed graphs of R and S by combining arrows as in the following example.

Example 3.15 *Let $A = \{1, 2, 3\}$, $B = \{a, b\}$ and $C = \{4, 5, 6\}$ and consider the relations $R = \{(1, a), (1, b), (3, b)\}$ from A to B and $S = \{(a, 4), (b, 6)\}$ from B to C. Then $S \circ R = \{(1, 4), (1, 6), (3, 6)\}$. The directed graphs of R, S and $S \circ R$ are given in Figure 5.*

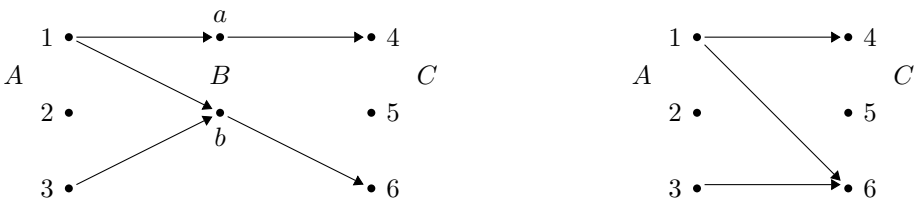

Figure 5: The directed graph of $S \circ R$ and the directed graphs of R and S.

3.4 Properties of Relations on a Single Set

Let R be a relation on a single set A, so $R \subseteq A \times A$ and the relation matrix is a square matrix. We can consider what happens to the truth value of $(x, y) \in R$ when $x = y$ or when we swap x and y. This leads to a number of additional properties that R may have and that we will now describe.

3.4.1 Reflexivity

Definition 3.16 *A relation R on a set A is called* reflexive *if and only if $(x, x) \in R$ for all $x \in A$. It is called* irreflexive *if and only if $(x, x) \notin R$ for all $x \in A$.*

The relation matrix of a reflexive relation has values T on the diagonal, whereas an irreflexive relation has values F on the diagonal. The directed graph of a reflexive relation has a loop at every element and the graph of an irreflexive relation has no loops. A relation cannot be both reflexive and irreflexive, except in the uninteresting case $A = \varnothing$ with $A \times A = \varnothing$ and $R = \varnothing$. However, a relation can be neither reflexive nor irreflexive.

Example 3.17 *Let $A = \{1, 2, 3\}$, then*

- *the relation $R_0 = \varnothing$ is irreflexive, but not reflexive,*
- *the relation $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ is reflexive, but not irreflexive,*
- *the relation $R_2 = \{(1, 1), (2, 2)\}$ is neither reflexive, nor irreflexive.*

The graphs of these relations are in Figure 6. For any $S \subset \{(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}$ the relations $R_0 \cup S$, $R_1 \cup S$ and $R_2 \cup S$ have the same properties, because reflexivity and irreflexivity depend only on the question whether the elements $(1, 1)$, $(2, 2)$ and $(3, 3)$ are contained in the relation.

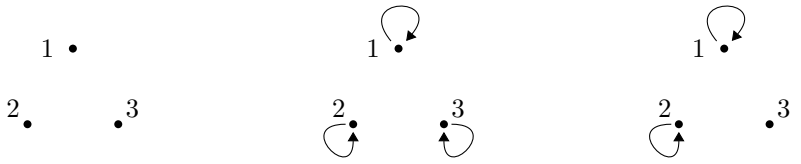

Figure 6: The directed graphs corresponding to the relations R_0, R_1 and R_2 in Example 3.17 from left to right.

Note that $(x,x) \in R^{-1}$ if and only if $(x,x) \in R$. It follows that R^{-1} is reflexive if and only if R is and that R^{-1} is irreflexive if and only if R is.

Definition 3.18 *The* reflexive closure *of a relation R on a set A is the relation $R \cup \{(x,x) | \ x \in A\}$ (as a union of sets).*

The reflexive closure of R is the smallest subset $R' \subseteq A \times A$ such that $R' \supseteq R$ and R' is a reflexive relation. If R is reflexive, then it is its own reflexive closure.

3.4.2 Symmetry

Definition 3.19 *A relation R on a set A is called* symmetric *if and only if for all $(x,y) \in A \times A$, $(x,y) \in R$ implies $(y,x) \in R$. It is called* anti-symmetric *if and only if for all $(x,y) \in A \times A$, $(x,y) \in R$ and $(y,x) \in R$ implies $x = y$.*

The relation matrix of a symmetric relation is a symmetric matrix under reflection in the diagonal. For an anti-symmetric relation the relation matrix is anti-symmetric in the sense that a T in an off-diagonal position turns into an F when we reflect in the diagonal (but we may have any values on the diagonal). The directed graph of a symmetric relation has an arriow from a to b if and only if there is an arrow from b to a. The directed graph of an anti-symmetric relation has no arrow from b to a if there is an arrow from a to b and $b \neq a$.

Example 3.20 *Let $A = \{1,2,3\}$, then*

- *the relation $S_0 = \varnothing$ is symmetric and anti-symmetric,*
- *the relation $S_1 = \{(1,2)\}$ is anti-symmetric, but not symmetric,*
- *the relation $S_2 = \{(1,2),(2,1)\}$ is symmetric, but not anti-symmetric,*
- *the relation $S_3 = \{(1,2),(2,1),(1,3)\}$ is neither symmetric nor anti-symmetric.*

Note that for any subset $R \subset \{(1,1),(2,2),(3,3)\}$ the relations $R \cup S_0$, $R \cup S_1$, $R \cup S_2$ and $R \cup S_3$ have the same properties, because symmetry and anti-symmetry is not changed by the elements $(1,1)$, $(2,2)$ and $(3,3)$.

It is not difficult to show that a relation R is symmetric if and only if $R = R^{-1}$. Also, R is anti-symmetric if and only if R^{-1} is anti-symmetric.

Definition 3.21 *The* symmetric closure closure *of a relation R on a set A is the relation $R \cup R^{-1}$ (as a union of sets).*

The symmetric closure of R is the smallest subset $R' \subseteq A \times A$ such that $R' \supseteq R$ and R' is a symmetric relation. If R is symmetric, then it is its own symmetric closure.

Figure 7: The directed graphs corresponding to the relations S_0, S_1, S_2 and S_3 in Example 3.20 from left to right.

3.4.3 Transitivity

Definition 3.22 *A relation R on a set A is called* transitive *if and only if for all $x, y, z \in A$, $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$.*

To recognise a transitive relation from its relation matrix is a bit cumbersome, but the directed graph of a transitive relation does have a nice property. If there is a path from a to b following the arrows in the graph, then there is a direct arrow from a to b.

Example 3.23 *In family relations, the relation "x is a sibling of y" is transitive and so is the relation "x descends from y" if descendence is allowed to take multiple steps. The relation "x is a parent of y" is not transitive.*

Example 3.24 *Combining Examples 3.17 and 3.20 we get twelve relations of the form $R_i \cup S_j$ with $i \in \{0, 1, 2\}$ and $j \in \{0, 1, 2, 3\}$ which combine the properties of R_i and S_j. The relations $R_i \cup S_0 = R_i$ and $R_i \cup S_1$ are transitive for all $i \in \{0, 1, 2\}$. The relation $R_i \cup S_3$ is not transitive for any $i \in \{0, 1, 2\}$, because it does not contain $(2, 3)$. The relations $R_1 \cup S_2$ and $R_2 \cup S_2$ are also transitive, but $R_0 \cup S_2$ is not, because it does not contain $(1, 1)$. The directed graphs for $R_1 \cup S_1$, $R_0 \cup S_2$ and $R_2 \cup S_3$ are given in Figure 8.*

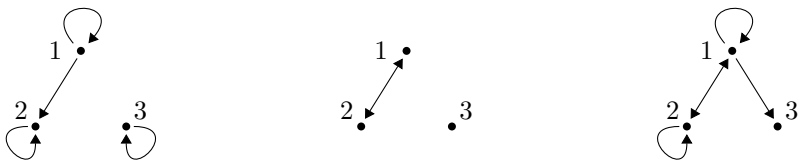

Figure 8: The directed graphs corresponding to the relations $R_1 \cup S_1$, $R_0 \cup S_2 = S_2$ and $R_2 \cup S_3$ in Example 3.24 from left to right.

It is not difficult to show that R is transitive if and only if R^{-1} is transitive.

Definition 3.25 *The* transitive closure *of a relation R on a set A is the relation R' on A such that $(x, y) \in R'$ if and only if there is a finite sequence of elements $x_1, x_2, \ldots, x_k$ in A for some $k \in \{0, 1, 2, \ldots\}$ such that $x_1 = x$, $x_k = y$ and $(x_i, x_{i+1}) \in R$ for all $i \in \{1, \ldots, k-1\}$.*

Example 3.26 *If A is the set of web pages and R the relation "x links to y", then the transitive closure of R is the relation "x connects to y by a sequence of links".*

There is an easy characterisation of transitivity using compositions.

Proposition 3.27 *A relation R on A is transitive if and only if $R \circ R \subseteq R$.*

Proof: If R is transitive, let $(x, y) \in R \circ R$ be arbitrary. Then there is a $z \in A$ such that $(x, z) \in R$ and $(z, y) \in R$. By transitivity this means that $(x, y) \in R$. Hence, $R \circ R \subseteq R$.
To prove the converse we assume that $R \circ R \subseteq R$. Let $(x, z) \in R$ and $(z, y) \in R$. Then $(x, y) \in R \circ R$ by definition of the composition and hence $(x, y) \in R$ by our assumption. Hence, R is transitive, as was to be shown. □

3.4.4 Further examples

Example 3.28 *Let us classify the following relations on $\mathbb{N}$ according to the properties of this section:*

1. *$x \leq y$:*
   This relation is reflexive: $n \leq n$ for all $n \in \mathbb{N}$. It is not irreflexive: $1 \leq 1$. It is also not symmetric: $1 \leq 2$, but $2 \not\leq 1$. It is anti-symmetric: $m \leq n$ and $n \leq m$ imply $m = n$ for all $m, n \in \mathbb{N}$. It is also transitive: $m \leq n$ and $n \leq k$ imply $m \leq k$ for all $m, n, k \in \mathbb{N}$.

2. *$x < y$:*
   This relation is not reflexive: $1 \not< 1$. It is irreflexive: $n \not< n$ for all $n \in \mathbb{N}$. It is not symmetric: $1 < 2$, but $2 \not< 1$. It is anti-symmetric in a trivial way: there are no $m, n \in \mathbb{N}$ such that $m < n$ and $n < m$. It is transitive: $m < n$ and $n < k$ imply $m < k$ for all $m, n, k \in \mathbb{N}$.

3. *x has the same parity (even/odd) as y:*
   This relation is reflexive, not irreflexive, symmetric, but not anti-symmetric, and transitive. We leave the verifications to the reader.

4. *$x = y$:*
   This relation is reflexive, not irreflexive, symmetric and anti-symmetric and also transitive. We leave the verifications to the reader.

Example 3.29 *Let $A = \{a, b, c\}$ and let R be the relation $R = \{(a, a), (a, b), (b, c), (c, a)\}$. We consider the various closures of this relation.*

- *The reflexive closure is the relation $\{(a, a), (a, b), (b, b), (b, c), (c, a), (c, c)\}$, where we added the elements (b, b) and (c, c).*

- *The symmetric closure is the relation $\{(a, a), (a, b), (a, c), (b, a), (b, c), (c, a), (c, b)\}$, where we added the elements (a, c), (b, a) and (c, b).*

- *The transitive closure is the relation $A \times A$. To see this we note that the transitive closure must contain (a, c), because it contains (a, b) and (b, c). Similarly, it must contain (b, a) and (c, b). Next we note that the transitive closure must also contain (b, b), because it contains (b, a) and (a, b). Similarly it must contain (c, c) and it already contains (a, a).*

3.5 Equivalence Relations

Some relations are used to formulate the idea that one thing is "the same as" something else in some sense (which depends on the context). E.g., x and y are siblings exactly when they have the same parents. Such special relations are called equivalence relations. More precisely, we make the following definition.

Definition 3.30 *A relation R on a set A is called an* equivalence relation *if and only if it is reflexive, symmetric and transitive.*

Example 3.31 *Here are two examples of equivalence relations. The verification of reflexivity, symmetry and transitivity is left as an exercise.*

1. *Let A be the set of DCU academic staff and define the relation R on A by $(x, y) \in R$ if and only if x works in the same faculty as y. Then R is an equivalence relation.*
2. *Let $A = \{1, 2, 3, 4, 5, 6\}$ and consider the subsets $A_1 = \{1\}$, $A_2 = \{2, 3\}$ and $A_3 = \{4, 5, 6\}$. Then $\{A_1, A_2, A_3\}$ is a partition of A. Define the relation R on A by $(x, y) \in R$ if and only if x is in the same subset A_i as y, with $i \in \{1, 2, 3\}$. Then R is an equivalence relation.*
3. *More generally, let A be a set with a partitioning $\{A_1, A_2, \ldots, A_k\}$. Define the relation R on A by $(x, y) \in R$ if and only if x is in the same subset A_i in the partition as y.*

The directed graph and the relation matrix of an equivalence relation have special properties. We illustrate this for the second item in Example 3.31, whose directed graph is given in Figure 9 and whose relation matrix is

$$\left(\begin{array}{c|cc|ccc} \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \hline \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \hline \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{T} \\ \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{T} \\ \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{T} \end{array}\right).$$

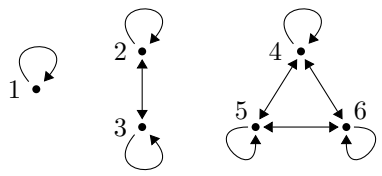

Figure 9: The directed graph corresponding to the second item in Example 3.31.

Definition 3.32 *Given an equivalence relation R on a set A we define the* equivalence class *of an element $x \in A$ to be the set of all elements to which it is related by R,*

$$E_x := \{y \in A |\ (y, x) \in R\}.$$

A representative *of the equivalence class E_x is any element $y \in E_x$.*

Note that x is always a representative of its own equivalence class E_x.

Example 3.33 *Returning to the second example in 3.31, the equivalence class of the number* 3 *is the set $A_2 = \{2, 3\}$. In the more general third example of 3.31, the equivalence class of $x \in A$ is the unique set A_i of the partition which contains x.*

The appearance of partitions in the context of equivalence relations is not accidental. Given an equivalence relation R on a set A, we can partition A into subsets in such a way that all elements in each subset are related to each other. This is the content of the following theorem.

Theorem 3.34 *Let R be an equivalence relation on a set A. The collection of all distinct equivalence classes is a partition of A.*

Note that we can have $E_x = E_y$ as sets even when $x \neq y$. The equivalence classes are distinct when $E_x \neq E_y$.

Proof: Fix an arbitrary $x \in A$. Because R is reflexive we have $x \in E_x$. By universal generalization, every $x \in A$ is contained in at least one of the equivalence classes. It remains to show that distinct equivalence classes are mutually disjoint.

For any $x \in A$ and $y \in A$ suppose that $E_x \cap E_y$ is not empty, so there exists $z \in E_x \cap E_y$. We will show that $E_x = E_y$, so the classes are not distinct. Let w be an arbitrary element of E_x. By definition of E_x we then have $(w, x) \in R$ and $(z, x) \in R$ and similarly $(z, y) \in R$. Because R is symmetric we also have $(x, z) \in R$ and because R is transitive we then find that $(w, z) \in R$ and $(w, y) \in R$, i.e. $w \in E_y$. By universal generalization we see that $E_x \subseteq E_y$. Reversing the roles of x and y we also find that $E_y \subseteq E_x$ and therefore $E_x = E_y$. This means that E_x and E_y are not distinct. By contraposition: if the sets are distinct, then they are disjoint. This shows that the collection of all distinct equivalence classes is a partition of A, as was to be shown. □

Note that this partitioning only works for equivalence relations. The proof makes explicit use reflexivity, symmetry and transitivity of the relation.

The following equivalence relations occur in cryptography to construct hashing functions.

Example 3.35 *Let $m \in \mathbb{N}$ and define a relation R_m on $\mathbb{Z}$ such that $(a, b) \in R_m$ if and only if $a - b$ is an integer multiple of m, i.e. $a - b = km$ for some $k \in \mathbb{Z}$.*

If we picture $\mathbb{Z}$ as an infinite grid on the number line whose points are separated by a distance 1, then the equivalence class E_a of $a \in \mathbb{Z}$ is a grid whose points are separated by a distance m and which contains the number a. If $m = 1$ all elements of $\mathbb{Z}$ are equivalent. When $m = 2$ all even numbers are equivalent to each other and all odd numbers too. The set of all equivalence classes is often denoted by $\mathbb{Z}/m\mathbb{Z}$.

For general $m > 1$ we can use the numbers in the set $A = \{0, 1, \ldots, m - 1\}$ to represent all the distinct equivalence classes. Indeed, A contains no two elements that are equivalent to each other, but every $a \in \mathbb{Z}$ is equivalent to one of the numbers in A. This can be seen using division by m with remainder. The remainder is sometimes written in a formula using mod *or* %*. E.g., if $m = 3$ and we divide 17 by 3, then the result is 5 with remainder 2. This last statement is written in a formula as* $17\mathrm{mod}3 = 2$ *or* $17\%3 = 2$.

3.6 Partial Order Relations

Definition 3.36 *A* partial order relation *on a set A is a relation R which is reflexive, anti-symmetric and transitive. A set together with a partial order relation is called a* partially ordered set *(or* poset *for short).*

Following the arrows in the directed graph of a partial order relation R one cannot obtain any loops, except loops at a single point, when $(x, x) \in R$.

Example 3.37 *Here are some examples of partially ordered sets.*

1. *The set $\mathbb{R}$ with the relation $x \leq y$ is a partially ordered set. To check this we note that for all $x, y, z \in \mathbb{R}$: $x \leq x$ (reflexivity); $x \leq y$ and $y \leq x$ imply $x - y \leq 0$ and $0 \leq x - y$ and hence $x - y = 0$, i.e. $x = y$ (anti-symmetry); $x \leq y$ and $y \leq z$ imply $x \leq z$ (transitivity).*

2. *The power set $\mathcal{P}(A)$ of a set A with the relation $X \subseteq Y$ (where X and Y are elements of $\mathcal{P}(A)$, i.e. subsets of A) is a partially ordered set. To check this we note that for all*

$X, Y, Z \subset A$: $X \subseteq X$ (reflexivity); $X \subseteq Y$ and $Y \subseteq X$ imply $X = Y$ (anti-symmetry); $X \subseteq Y$ and $Y \subseteq Z$ imply $X \subseteq Z$ (transitivity).

3. *For any sets A and B we can consider the set of relations from A to B and define a relation on these relations by $R_1 \subseteq R_2$. Indeed, relations are subsets of $A \times B$, so this is just a special case of the previous example, taking the partial order relation on $\mathcal{P}(A \times B)$.*

The word "partial" in "partial order relation" refers to the fact that there may be elements $x, y \in A$ for which neither $(x, y) \in A$ nor $(y, x) \in A$, i.e. we cannot always order a finite list of elements. This happens e.g. for subset $X \subseteq A$ and $Y \subseteq A$ when neither $X \subseteq Y$ nor $Y \subseteq X$.

This ordering does work if we require an additional property as follows.

Definition 3.38 *A* total order relation *on a set A is a partial order relation R with the additional property that for all $x \in A$ and $y \in A$ either $(x, y) \in R$ or $(y, x) \in R$. A set with a total order relation is called a* totally ordered set.

Example 3.39 *Here are two examples of totally ordered sets.*

1. *$\mathbb{R}$ with the relation $x \leq y$ is totally ordered: if $x \in \mathbb{R}$ and $y \in \mathbb{R}$ then either $x - y \leq 0$ or $x - y > 0$ and hence either $x \leq y$ or $x > y$ and hence $y \leq x$. (If both of these are true then $x = y$, by anti-symmetry of the relation.)*

2. *The alphabet $\{a, c, \ldots, z\}$ with its usual ordering is totally ordered. For any two distinct letters we can say whether one comes before the other or after it.*

The ordering of the alphabet can be extended to give an ordering on a much larger set of words, as in a dictionary. This can be described mathematically as follows. When A and B are totally ordered sets with total order relations R_A and $_B$, respectively, then we can also give $A \times B$ a total order relation R_{AB} as follows: $((x, y), (x', y')) \in R_{AB}$ if and only if $(x, x') \in R_A$ and if $x = x'$ then $(y, y') \in R_B$. (One can check that this relation is indeed a total order relation.) Now if A is a totally ordered set we can use this construction to define a total order relation on $A \times A$, then on $A \times A \times A$ and then (by induction) on $A^{\times n}$ for any $n \in \mathbb{N}$. This is called the *lexicographic order relation* on $A^{\times n}$.

Example 3.40 *On $\{0, 1\}$ consider the relation $\leq$, which is a total order relation. The three-fold Cartesian product $\{0, 1\}^{\times 3}$ can then be given the lexicographic order relation. In this order the elements of $\{0, 1\}^{\times 3}$ are:*

000
001
010
011
100
101
110
111

where we omitted the brackets and the commas for convenience. (To remain in line with our general notation it would have more precise to write $(0, 0, 0)$, $(0, 0, 1)$, etc.)