Equivalences*

Ana Sokolova

Department of Computer Sciences, University of Salzburg

anas@cs.uni-salzburg.at

December 12, 2020

In this chapter, we deal with equivalence relations, already introduced in the part on relations, in more detail. Recall that an *equivalence relation*, or an *equivalence*, is a relation on a set A that is reflexive, symmetric, and transitive. Equivalence relations have a particularly important role, as generalisation of the equality relation, which is why we study them. Aside the equality, we already know well another equivalence relation: the relation $\overset{val}{=}$ on (abstract) propositions.

The first notion of importance related to an equivalence relation is that of an equivalence class. Intuitively, an equivalence class of an equivalence R on a set A is a subset of A containing element that are all interconnected by R. The definition, however, is much simpler.

Definition 1 (Equivalence Class). *Let $R \subseteq A \times A$ be an equivalence relation on A, and let $a \in A$. Then the equivalence class of a under R, notation $[a]_R$ is the set*

$$[a]_R = \{b \in A \mid (a, b) \in R\}.$$

Example 1. Consider $A = \{1, 2, 3\}$ and the relation

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$$

on A. It is easy to check that R is an equivalence relation. We have $[1]_R = [2]_R = \{1, 2\}$ and $[3]_R = \{3\}$.

Next, we discuss another, more generic, example, in order to see how equivalence relations "behave". Let $A = \{a, b, c, d, e, f\}$ and let R be an equivalence on A (that we do not fully specify yet).

Then, clearly, (a, a), (b, b), (c, c), (d, d), (e, e), $(f, f) \in R$ by reflexivity.

If $(a, b) \in R$, then also $(b, a) \in R$ by symmetry.

If in addition $(a, c) \in R$. Then we get: $(b, c) \in R$ as $(b, a) \in R$ and $(a, c) \in R$, by transitivity. Furthermore, also (c, a), $(c, b) \in R$ by symmetry.

So we see that assuming $(a, b) \in R$ and $(a, c) \in R$ already yields $\{a, b, c\} \times \{a, b, c\} \subseteq R$.

This explains our comment above that equivalence classes consist of interconnected elements: We have, by Definition 1, $(a, b) \in R \wedge (a, c) \in R \overset{val}{=} b \in [a]_R \wedge c \in [a]_R$

* Notes from the lectures Formale Systeme on naive set theory. Many thanks to Luis Thiele for helping me with producing the notes.

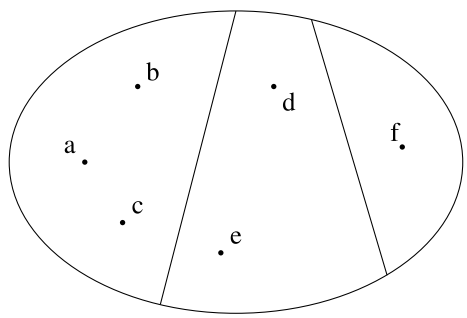
and hence assuming that we have two elements $b, c \in [a]_R$ yields (in particular) that $(b, c) \in R$. So, arbitrary two elements in an equivalence class of an equivalence R are related by R.

If we further assume that $(d, e) \in R$ then $(e, d) \in R$ by symmetry.

Hence, if R is the smallest equivalence with $(a, b) \in R$, $(a, c) \in R$, and $(d, e) \in R$, then

$$\begin{aligned} &[a]_R = [b]_R = [c]_R = \{a, b, c\} \\ &[d]_R = [e]_R = \{d, e\} \\ &[f]_R = \{f\} \end{aligned}$$

and the classes of R partition the set A as shown in the figure below.



Lemma 1. *Let R be an equivalence on A. Then for all $a, b \in A$,*

$$[a]_R = [b]_R \quad \textit{or} \quad [a]_R \cap [b]_R = \emptyset.$$

Proof. Let R be an equivalence on A and let $a, b \in A$. We consider two cases (one of which must occur) and provide a proof by case distinction.

Case 1: $(a, b) \in R$. Then by symmetry also $(b, a) \in R$. If $x \in [a]_R$, i.e., $(a, x) \in R$, we get $(b, x) \in R$ by transitivity, and hence $x \in [b]_R$. Since x was arbitrary, this shows that $[a]_R \subseteq [b]_R$. For the opposite inclusion, it is enough to notice that we have just proven

$$(a, b) \in R \;\Rightarrow\; [a]_R \subseteq [b]_R. \tag{1}$$

Now when $(a, b) \in R$, we have $(b, a) \in R$ by symmetry, and hence, using (1) with the roles of a and b exchanged, we get $[b]_R \subseteq [a]_R$. This proves $[a]_R = [b]_R$ when $(a, b) \in R$.

Case 2: $(a, b) \notin R$. In this case, we want to show that $[a]_R \cap [b]_R = \emptyset$. Assume the contrary, i.e., assume towards a contradiction that $[a]_R \cap [b]_R \neq \emptyset$ This means $\exists x.\, x \in [a]_R \cap [b]_R$. Let c be such an element with $c \in [a]_R \cap [b]_R$. Then $(a, c) \in R$ and $(b, c) \in R$. By symmetry, also $(c, b) \in R$. From $(a, c) \in R$ and $(c, b) \in R$, by transitivity, $(a, b) \in R$ which contradicts the assumption $(a, b) \notin R$. Hence it must be that $[a]_R \cap [b]_R = \emptyset$.

$\square$

Definition 2 (Quotient). *When $R \subseteq A \times A$ is an equivalence relation, then the quotient (D. Faktormenge) of A under R is the set of all R-equivalence classes, i.e.,*

$$A/R = \{[a]_R \mid a \in A\}.$$

Note that $A/R \subseteq \mathcal{P}(A)$.

Before we proceed with a fundamental theorem about equivalences and their quotients, we need to define unions and intersections of multiple sets.

1 Unions and Intersections of Multiple Sets

Given $n \in \mathbb{N}$, $n \geq 1$, and sets $A_1, A_2, ..., A_n$ we define

$$\begin{aligned} \bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup \cdots \cup A_n \\ \bigcap_{i=1}^{n} A_i &= A_1 \cap A_2 \cap \cdots \cap A_n \end{aligned}$$

Note that the sets on the right-hand side are well defined (given that the "$\cdots$" are understood in the usual way) due to commutativity and associativity of union and intersection. In general, for an arbitrary family of sets $(A_i \mid i \in I)$ indexed by a set I, we define

$$\begin{aligned} \bigcup_{i \in I} A_i &= \{x \mid \exists i \in I.\, x \in A_i\} \\ \bigcap_{i \in I} A_i &= \{x \mid \forall i \in I.\, x \in A_i\}. \end{aligned}$$

Example 2. $([a]_R \mid a \in A)$ is a family of sets indexed by A.

Lemma 2. *Let $R \subseteq A \times A$ be an equivalence. Then*

$$A = \bigcup_{a \in A} [a]_R.$$

Proof. We need to prove both inclusions.

$\subseteq$: Let $x \in A$. Then, by reflexivity, $(x, x) \in R$, and hence $x \in [x]_R$. This shows that $\exists a \in A.\, x \in [a]_R$ (namely $a = x$) and hence $x \in \bigcup_{a \in A} [a]_R$.

$\supseteq$: Let $x \in \bigcup_{a \in A} [a]_R$. Then there is an $a \in A$ with $x \in [a]_R$. By definition $[a]_R \subseteq A$, and hence $x \in A$. $\square$

2 Partitions

We will see soon that equivalence classes form a partition of the underlaying set. But first, we need to define the notion of a partition.

Definition 3 (Partition). *Let A be a set. A subset P of the powerset of A ($P \subseteq \mathcal{P}(A)$) is a partition of A if it satisfies the following three properties:*

P1. *For all $U \in P$, $U \neq \emptyset$.*
P2. *For all $U, V \in P$, if $U \neq V$ then $U \cap V = \emptyset$.*
P3. $\bigcup\limits_{U \in P} U = A$.

The elements of a partition are called classes*.*

Note that the property P1 states that all classes of a partition are nonempty. The property P2 states that two classes that are not equal are disjoint, or equivalently: classes are either equal or disjoint. Finally, the property P3 states that P *covers* A, i.e., that every element of A belongs to some class of the partition. This also justifies the name *partition* as the set A is parted into disjoint classes.

Example 3. $P = \{\{a, b, c\}, \{d, e\}, \{f\}\}$ is a partition of the set $A = \{a, b, c, d, e, f\}$.

The next theorem gives us a characterisation of equivalences with help of partitions and vice versa. This is the first somewhat serious theorem that we prove in our course, if seriousness is measured in terms of not-too-short proof. Our course is not about big theorems, and this is also not a big theorem, but definitely a notable characterisation. The theorem tells us that an equivalence is fully described by its partition into equivalence classes: For any equivalence, the quotient set is a partition, and from any partition there is a canonical way of obtaining an equivalence whose classes are the elements of the partition.

Theorem 1 (Equivalences and Partitions). *Let A be a set.*

(1) If R is an equivalence on A, then the set

$$P(R) = A/R = \{[a]_R \mid a \in A\}$$

is a partition.

(2) If P is a partition of A, then the relation

$$R(P) = \{(x, y) \in A \times A \mid \exists U \in P.\, x \in U \wedge y \in U\}$$

is an equivalence.

Moreover, the assignments $R \mapsto P(R)$ and $P \mapsto R(P)$ are inverse to each other, i.e.,

$$R(P(R)) = R \quad \text{and} \quad P(R(P)) = P.$$

Note that within this theorem there is a hidden definition: we defined $P(R)$ and $R(P)$. While $P(R)$ is just another name for the quotient, $R(P)$ is something new. Before we proceed with the proof of the theorem, we give an example, to make sure that the definition of $R(P)$ is well understood.

Example 4. Given a set $A = \{1, 2, 3, 4\}$ and a partition $P = \{\{1\}, \{2\}, \{3, 4\}\}$, the associated equivalence $R(P)$ is then

$$R(P) = \{(1, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}.$$

Proof (of Theorem 1). We start by proving each of the properties (1) and (2).

(1) Let $a \in A$. The class $[a]_R$ is nonempty as $a \in [a]_R$, by reflexivity. Hence, we have proven P1 for $P(R)$. Lemma 1 shows that if $[a]_R \neq [b]_R$, then $[a]_R \cap [b]_R = \emptyset$. Hence, P2 holds for $P(R)$. Finally, Lemma 2 shows that $A = \bigcup_{a \in A} [a]_R$, thus proving P3 for $P(R)$. All together, we have proven that

$$P(R) = A/R = \{[a]_R \mid a \in A\}$$

is a partition.

(2) Let P be a partition and consider the relation

$$R(P) = \{(x, y) \in A \times A \mid \exists U \in P.\, x \in U \wedge y \in U\}.$$

Reflexivity: Let $x \in A$. Then, since $A = \bigcup_{U \in P} U$, there exists $U \in P$ with $x \in U$. Certainly $x \in U \wedge x \in U$. This shows

$$(x, x) \in R(P).$$

Symmetry: Let $x, y \in A$ and assume $(x, y) \in R(P)$. Then there is $U \in P$ with $x \in U \wedge y \in U$. But certainly also $y \in U \wedge x \in U$, showing that

$$(y, x) \in R(P).$$

Transitivity: Let $x, y, z \in A$ be such that $(x, y) \in R(P)$ and $(y, z) \in R(P)$. This means that there are $U_1, U_2 \in P$ such that $x \in U_1 \wedge y \in U_1$ and $y \in U_2 \wedge z \in U_2$. It is very important here that we distinguish between U_1 and U_2 by definition, as long as we do not have further evidence! Now, obviously, $y \in U_1 \cap U_2$. Since P is a partition, from $U_1 \cap U_2 \neq \emptyset$ we can conclude that $U_1 = U_2$. So there is a U, namely $U = U_1 = U_2$, with $x, y, z \in U$. In particular, $x \in U \wedge z \in U$, showing that

$$(x, y) \in R(P).$$

This proves (2).

To show that $P(R(P)) = P$, we will show both inclusions. Let first $U \in P$. We will show $U \in P(R(P))$, i.e., $U = [x]_{R(P)}$ for some $x \in A$. Actually we will show $U = [x]_{R(P)}$ for all $x \in U$ which is certainly enough as $U \neq \emptyset$ since P is a partition and $U \in P$.

Let $x \in U$. We have

$$\begin{aligned} y \in [x]_{R(P)} &\overset{val}{=} (x,y) \in R(P) \\ &\overset{val}{=} \exists V \in P.\, x \in V \wedge y \in V \\ &\overset{val}{=} x \in U \wedge y \in U && (*) \\ &\overset{val}{=} y \in U. && (**) \end{aligned}$$

Here, the equivalence marked by $(*)$ holds since we have assumed that $x \in U$ and classes are either disjoint or equal, so the class that exists must be the class U. The equivalence marked by $(**)$ is a consequence of $x \in U$ being true by assumption. This shows

$$P \subseteq P(R(P)).$$

For the opposite inclusion, let $[x]_{R(P)} \in P(R(P))$. Since $x \in A$ and P is a partition of A, there is a $U_x \in P$ with $x \in U_x$. Then, like above $U_x = [x]_{R(P)}$ showing that $[x]_{R(P)} \in P$. Hence

$$P(R(P)) \subseteq P \text{ and therefore } P = P(R(P)).$$

To show $R = R(P(R))$:

$$\begin{aligned} y \in [x]_R &\overset{val}{=} x \in [x]_R \wedge y \in [x]_R \\ &\overset{val}{=} \exists U \in P(R).\, x \in U \wedge y \in U \quad (***) \\ &\overset{val}{=} (x,y) \in R(P(R)). \end{aligned}$$

where the first equivalence holds since $x \in [x]_R$ is true and (***) holds since: If $x \in [x]_R \wedge y \in [x]_R$, then $U = [x]_R$ is the needed one, and it exists in $P(R)$; Furthermore, if $\exists U \in P(R).\, x \in U \wedge y \in U$, then since $[x]_R \in P(R)$ and $x \in [x]_R$ and since equivalence classes are either equal or disjoint (and these are not disjoint as $x \in [x]_R \cap U$) it must be that $U = [x]_R$, so $x \in [x]_R$ and $y \in [x]_R$. This completes the proof of the theorem. □

Note that the assignments that we just saw

$$P \mapsto R(P) \quad \text{and} \quad R \mapsto P(R).$$

are examples of functions (that we will learn next). In particular, we will see later that they are bijective functions that are inverses of each other. But before that, we will learn how to extend a relation to the smallest equivalence that contains it, relaying on one more important notion related to relations – the notion of transitive closure.

3 Transitive Closure of a Relation

Let R be a relation on a set A, so $R \subseteq A \times A$. The *transitive closure* (D. Transitive Hülle) of R, notation R^+, is the relation

$$R^+ = \bigcup_{\substack{n \in \mathbb{N} \\ n \neq 0}} R^n = R \cup R^2 \cup R^3 \cup \dots \tag{2}$$

Proposition 1. *Let R be a relation on A. The transitive closure R^+ is the smallest transitive relation that contains R.* $\square$

This proposition gives us a characterisation of the transitive closure in other terms. The proof of the proposition is not difficult, and it is left out as an exercise for the reader. Here, by smallest we mean smallest with respect to inclusion, i.e., contained in any other transitive relation that contains R.

Note that one could do things the other way around, i.e., define R^+ as

$$R^+ = \bigcap_{\substack{T \subseteq A \times A \\ T^2 \subseteq T \\ R \subseteq T}} T \tag{3}$$

that is, as the smallest transitive relation that contains R, and then prove that $R^+ = \bigcup_{\substack{n \in \mathbb{N} \\ n \neq 0}} R^n$. Intuitively, Eq. (3) gives us an outer-characterisation of R^+ whereas Eq. (2) is an inner-characterisation, via a so-called *fixpoint*, a topic that you will learn about in your master studies.

Example 5. Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3), (2, 2)\}$. Then

$$\begin{aligned} R^2 &= \{(1, 2), (2, 3), (1, 3), (2, 2)\} \\ R^3 &= R \circ R^2 = \{(1, 2), (1, 3), (2, 3), (2, 2)\} = R^2 \end{aligned}$$

Recall that $R^2 = \{(a, c) \in A \times A \mid \exists b \in A.(a, b) \in R \wedge (b, c) \in R\}$. We have that

$$(1, 2) \in R^2 \;\text{ since }\; (1, 2), (2, 2) \in R$$

and hence there exists an element $a \in A$ such that $(1, a), (a, 2) \in R$;

$$\begin{aligned} &(2, 3) \in R^2 \;\text{ since }\; (2, 2), (2, 3) \in R; \\ &(1, 3) \in R^2 \;\text{ since }\; (1, 2), (2, 3) \in R; \;\text{ and} \\ &(2, 2) \in R^2 \;\text{ since }\; (2, 2), (2, 2) \in R. \end{aligned}$$

Note that, due to the existential quantifier in the definition of R^2, there could in general be more than one reason why a pair of elements is in R^2. However, in this small example, there happens to be always exactly one reason for every pair, the one mentioned above.

Further on,

$$R^4 = R \circ R^3 = R \circ R^2 = R^3 = R^2$$

and we will show in some weeks by induction, after we have learned induction, that

$$R^n = R \text{ for all } n \geq 2.$$

Therefore

$$R^+ = R \cup R^2 = R^2 = \{(1,2),(2,3),(1,3),(2,2)\}.$$

Note that even though the definition of R^+ is via an infinite union, on a finite set A as in this example, $R^+ \subseteq A \times A$ is finite as well, as any relation on A is, and so the process of constructing R^+ is finite too: at least one pair is added in every iteration, and there are only finitely many available pairs to add. We will learn about finite and infinite sets when we learn about cardinals in several weeks.

The transitive closure of a relation has an important computational meaning: A set A together with a relation R on A forms a directed graph whose nodes are the elements of A and transitions are given by pairs in R. A transition $a \to b$ from an element a to an element b models that there is a one-step directed path from a to b. The transitive closure gives us the *reachability* relation: $(a,b) \in R^+$ if and only if there is a path of one or more steps from a to b in the above mentioned graph. Reachability checking is behind many interesting verification problems in computer science.

We can now also define the *transitive and reflexive closure* R^* of a relation R on a set A, by

$$R^* = \Delta_A \cup R^+$$

hence, setting $R^0 = \Delta_A$, we see that

$$R^* = \bigcup_{n \in \mathbb{N}} R^n.$$

Similarly as in Proposition 1, we can formulate and prove (left to the reader as an exercise) the following property.

Proposition 2. *Let R be a relation on A. The transitive and reflexive closure R^* is the smallest transitive and reflexive relation that contains R.* □

Finally, the *equivalence closure* of a relation R on a set A is given by

$$E(R) = (R \cup R^{-1})^*.$$

The next proposition shows (again, the proof is left as an exercise) that the name equivalence closure is deserved.

Proposition 3. *Let R be a relation on A. The equivalence closure $E(R)$ is the smallest equivalence relation that contains R.* □