Relations*

Ana Sokolova

Department of Computer Sciences, University of Salzburg

anas@cs.uni-salzburg.at

December 8, 2019

Recall that the direct product of two sets A and B is the set

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

Hence, elements of $A \times B$ are *ordered pairs* (x, y) where $x \in A$ and $y \in B$.

Can we define the product of three sets?

Not immediately using the product of two sets, as there are two options:
Given sets A, B, C we could consider

I. $A \times (B \times C)$
II. $(A \times B) \times C$

However $A \times (B \times C) \neq (A \times B) \times C$. To see this, take for example $A = \{a\}$, $B = \{1, 2\}$, $C = \{3\}$. Then

$$(a, (1, 3)) \in A \times (B \times C)$$

but

$$(a, (1, 3)) \notin (A \times B) \times C.$$

(Actually, $((a, 1), 3) \in (A \times B) \times C$.) Therefore we use neither I. nor II., but define instead

$$A \times B \times C = \{(x, y, z) \mid x \in A, y \in B, z \in C\}.$$

Hence, $A \times B \times C$ is the set of ordered triples whose first element is in A, second in B, and third in C.

Generalising this, for a finite family of sets $A_1, A_2, \ldots, A_n$ with $n \geq 1$, $n \in \mathbb{N}$ we define the product $A_1 \times A_2 \times \cdots \times A_n$ also denoted by $\prod_{i=1}^{n} A_i$ by

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{(x_1, x_2, \ldots, x_n) \mid \forall i \in \{1, \ldots, n\}.\ x_i \in A_i\}.$$

* Notes from the lectures Formale Systeme on naive set theory. I write these notes as the things that we cover this week on this topic are not to be found (in this form) in the book. I also write them so that you—the students—see the difference between lecture notes (written text) and slides (overview presentation), and so that you do not need to rely on hand-written notes.

If $A_i = A$ for all $i \in \{1, \dots, n\}$, then the product is denoted by A^n and called the n-th power of A. Hence,

$$A^n = \{(x_1, x_2, \dots, x_n) \mid \forall i \in \{1, \dots, n\}.\ x_i \in A\}.$$

1 Relations

Now we have all the needed background to define relations.

Definition 1 ((Binary) Relation). *Let A and B be sets. A (binary) relation R between A and B is a subset of $A \times B$. Hence, $R \subseteq A \times B$.*

Definition 2 (Relation on a set). *R is a relation* on A *if $R \subseteq A \times A$.*

Given a set A, a *unary relation* on A is a subset $P \subseteq A$. (Unary relations are often called predicates.)

Given sets $A_1, \dots, A_n$, an *n-ary relation* between $A_1, \dots, A_n$ is a subset $R \subseteq A_1 \times \cdots \times A_n$.

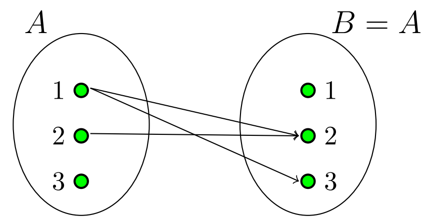
Example 1. The following are examples of relations:

- $R_1 = \{(x, y) \in M \times M \mid x \text{ is a child of } y\}$ where M denotes the set of all people.
- $R_2 = \leq_{\mathbb{N}} = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \leq m\}$.
- $R_3 = \subseteq_{\mathcal{P}(X)} = \{(A, B) \mid A \subseteq X, B \subseteq X, A \subseteq B\}$.
- $R_4 = \Delta_X = 1_X = \mathrm{Id}_X = \{(x, y) \in X \times X \mid x = y\} = \{(x, x) \mid x \in X\}$. We call this relation *the diagonal* on X, or the *identity relation* on X, or *equality*.
- $R_5 = \in_X = \{(x, Y) \mid x \in X, Y \subseteq X, x \in Y\}$. We call this relation *membership*.
- An example of a ternary relation on the set M of all people is

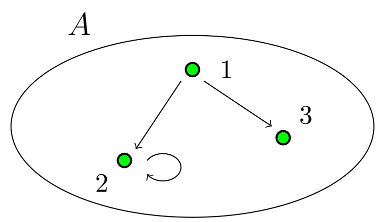
$$R_6 = \{(x, y, z) \mid x \text{ is a child of } y \text{ and } y \text{ is a child of } z\}.$$

We often write xRy instead of $(x, y) \in R$ and say in such a case that we use *infix notation*. For example, we write $A \subseteq B$ rather than $(A, B) \in \subseteq$ and $n \leq m$ rather than $(n, m) \in \leq$.

Binary relations on a set A are of particular interest in mathematics and computer science. We can picture a binary relation R between two sets A and B as a diagram by drawing the two sets and for each pair $(a, b) \in R$ we draw an arrow from $a \in A$ to $b \in B$. For example, for $A = B = \{1, 2, 3\}$ and $R = \{(1, 2), (1, 3), (2, 2)\}$, the relation diagram of R is:



When, like in this example, we depict a relation on a set A, there is no need to draw the set A twice — instead, the relation R can be represented as a graph. That is, we draw the set A once, and draw an edge (an arrow) from a to b whenever $(a, b) \in R$, like in the following figure for our example relation:



Graphs (and hence binary relations!) are a fundamental concept in computer science—a large part of the theory of algorithms focuses on graph algorithms.

2 Special Relations

Some relations have a particular structure/shape/property and hence deserve to be called by special names. A relation $R \subseteq A \times A$ on a set A is

reflexive	iff	$\forall a\,[a \in A : (a, a) \in R]$
symmetric	iff	$\forall a, b\,[a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R]$
transitive	iff	$\forall a, b, c\,[a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R]$
antisymmetric	iff	$\forall a, b\,[a, b \in A : (a, b) \in R \wedge (b, a) \in R \Rightarrow a = b]$
asymmetric	iff	$\forall a, b\,[a, b \in A : (a, b) \in R \Rightarrow (b, a) \notin R]$
irreflexive	iff	$\forall a\,[a \in A : (a, a) \notin R]$
total	iff	$\forall a, b\,[a, b \in A : (a, b) \in R \vee (b, a) \in R]$.

Note that equivalently, using standard notation, we can write for example the property of reflexivity as $\forall a \in A.(a, a) \in R$, and the property of antisymmetry as $\forall a, b \in A.(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$.

Example 2. We consider the relations from Example 1 and see if they satisfy some of the defined properties.

R_1, the relation “is a child of” is not reflexive, not symmetric, not transitive, irreflexive, asymmetric, antisymmetric, not total.

R_2, the order relation on $\mathbb{N}$, is reflexive, antisymmetric, transitive, and total. It is not symmetric, not asymmetric, not irreflexive. We will now show each of these mentioned properties in case of R_2:

Reflexivity: For any $n \in \mathbb{N}$ we have $n \leq n$.

Antisymmetry: Let $n, m \in \mathbb{N}$ be such that $n \leq m$ and $m \leq n$. Then $n = m$.

Transitivity: Let $n, m, k \in \mathbb{N}$ be such that $n \leq m$ and $m \leq k$. Then $n \leq k$.

Total: Let $n, m \in \mathbb{N}$. Then $n \leq m$ or $m \leq n$.

Not symmetric: $2 \leq 5$ but $\neg(5 \leq 2)$. Hence $2 \leq 5 \Rightarrow 5 \leq 2$ is not true. Hence $\exists a, b\,[a, b \in \mathbb{N} : \neg(a \leq b \Rightarrow b \leq a)]$ and therefore it is not true that $\forall a, b[a, b \in \mathbb{N} : a \leq b \Rightarrow b \leq a]$, i.e., the order relation on $\mathbb{N}$ is not symmetric.

Not asymmetric: $2 \leq 2$ and $2 \leq 2$. Hence $2 \leq 2 \Rightarrow 2 \nleq 2$ is not true. Hence $\exists a, b\,[a, b \in \mathbb{N} : \neg(a \leq b \Rightarrow b \nleq a)]$ and therefore it is not true that $\forall a, b\,[a, b \in \mathbb{N} : a \leq b \Rightarrow b \nleq a]$ showing that the relation is not asymmetric.

Not irreflexive: $5 \leq 5$, hence $\exists a[a \in \mathbb{N} : \neg(a \nleq a)]$ and therefore it is not true that.$\forall a[a \in \mathbb{N} : a \nleq a]$ showing that the relation is not irreflexive.

R_3 on $\mathcal{P}(M)$ is reflexive, antisymmetric, transitive, but not irreflexive, not symmetric, not asymmetric, and not total if $|M| \geq 2$. Here is a proof that it is not total in such a case: Let M have at least two elements. In such a case we can assume without loss of generality that $M \supseteq \{1, 2\}$. Then $\{1\}, \{2\} \in \mathcal{P}(M)$ and $\{1\} \nsubseteq \{2\}$ and $\{2\} \nsubseteq \{1\}$. Hence $\exists X, Y \in \mathcal{P}(M).\, \neg(X \subseteq Y \vee Y \subseteq X)$, and so it is not true that $\forall X, Y \in \mathcal{P}(M).\, X \subseteq Y \vee Y \subseteq X$.

With help of these notions, we can define even more important classes of (binary) relations on a set A.

Definition 3 (Equivalence). *A relation $R \subseteq A \times A$ is an equivalence iff R is reflexive, symmetric, and transitive.*

Definition 4 ((Partial) Order). *A relation $R \subseteq A \times A$ is a partial order iff R is reflexive, antisymmetric, and transitive.*

Definition 5 (Strict order). *A relation $R \subseteq A \times A$ is a strict order iff R is irreflexive and transitive.*

Definition 6 (Preorder). *A relation $R \subseteq A \times A$ is a preorder iff R is reflexive and transitive.*

Definition 7 (Total order / linear order / chain). *A relation $R \subseteq A \times A$ is a total order (or linear order, or chain) iff R is a total partial order.*

The name *chain* for a total order is justified by the look of the graph of such a relation: Leaving out the transitive edges, a chain looks like a chain.

Here are some obvious properties:

1. Every partial order is a preorder.
2. Every total order is a partial order.
3. Every total order is a preorder.
4. If $R \subseteq A \times A$ is relation that contains a cycle, i.e., there exist $a, b \in A$ such that $a \neq b$, aRb, bRa, then R is not a partial order, not a strict order, not a total order.

Remark 1. From now on we will almost exclusively use the standard notation for predicate formulas, and only recall the formulas with explicit domains if we wish to do a formal proof using derivations or calculate with propositions.

3 Operations on Relations

Definition 8 (Relation composition). *Given $R \subseteq A \times B$ and $S \subseteq B \times C$, the relational composition $R \circ S \subseteq A \times C$ is given by*

$$R \circ S = \{(a, c) \in A \times C \mid \exists b \in B.\, (a, b) \in R \wedge (b, c) \in S\}.$$

It is not difficult to show that composition of relations is associative, i.e.,

$$R \circ (S \circ T) = (R \circ S) \circ T.$$

We write R^n for the composition of R with itself n times, if $R \subseteq A \times A$.

Definition 9 (Inverse relation). *Given a relation $R \subseteq A \times B$, the inverse relation of R, denoted by R^{-1}, is defined as*

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

Clearly, for $R \subseteq A \times B$, we have that $R^{-1} \subseteq B \times A$.

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

This is because: (1) for $b = 2$ we have $(1, b) \in R$ and $(b, 2) \in S$, showing that $(1, 2) \in R \circ S$; (2) for $b = 2$ we also have $(1, b) \in R$ and $(b, 3) \in S$, showing that $(1, 2) \in R \circ S$; and (3) no other pair $(a, c) \in A \times C$ satisfies the predicate $\exists b \in B.\, (a, b) \in R \wedge (b, c) \in S$.

You can convince yourself (even more easily) that $S \circ R = \{(3, 2)\}$.

Furthermore, $R^{-1} = \{(2, 1)\}$ and $S^{-1} = \{(2, 2), (3, 2), (1, 3)\}$.

Example 4. For $\leq$ on $\mathbb{N}$, we have $\leq^{-1} = \geq$ and $\leq^2 = \leq$. This second fact follows from the next Lemma, and an additional property, since $\leq$ is transitive and reflexive.

In the next small result, we give alternative characterisations of the notions of reflexivity, symmetry, and transitivity, using the operations on relations. The goal here is to understand that once we have defined a notion via a property, we can prove it is equivalent to another property and since then have both properties characterising the same notion. In some occasions, it is easier to use the definition (the defining property), in other it is better to use the characterisation (the equivalent property proven in a lemma or proposition or theorem). It would equally be possible to give the original definition via the new property, and then a characterisation via the original defining property: as long as the properties are equivalent. The more characterisations we know of a given notion, the more we know and understand the notion.

Lemma 1. *Let $R \subseteq A \times A$. Then*

- *R is reflexive iff $\Delta_A \subseteq R$.*
- *R is symmetric iff $R \subseteq R^{-1}$.*
- *R is transitive iff $R^2 \subseteq R$.*

Proof. Recall that Δ_A is the diagonal relation on A defined in Example 1. We will write the proof by simply stating equivalent propositions, one could also write it in different ways. We have

$$\begin{aligned} R \text{ is reflexive } &\overset{val}{=} \forall a \in A.(a,a) \in R \\ &\overset{val}{=} \forall a\,[a \in A : (a,a) \in R] \\ &\overset{val}{=} \forall a\,[(a,a) \in \Delta_A : (a,a) \in R] \\ &\overset{val}{=} \Delta_A \subseteq R \end{aligned}$$

where the third equivalence holds as $a \in A \overset{val}{=} (a,a) \in \Delta_A$ by the definition of the relation $\Delta_A = \{(a,a) \mid a \in A\}$ and the fact that for a set $\mathbb{P}$ defined as the extension of a predicate P, namely $\mathbb{P} = \{x \mid P(x)\}$, we have $x \in \mathbb{P} \overset{val}{=} P(x)$. The last (fourth) equivalence holds by the definition of subset.

$$\begin{aligned} R \text{ is symmetric } &\overset{val}{=} \forall a,b \in A.(a,b) \in R \Rightarrow (b,a) \in R \\ &\overset{val}{=} \forall a,b\,[a,b \in A \wedge (a,b) \in R : (b,a) \in R] \\ &\overset{val}{=} \forall a,b\,[(a,b) \in R : (b,a) \in R] \\ &\overset{val}{=} \forall a,b\,[(a,b) \in R : (a,b) \in R^{-1}] \\ &\overset{val}{=} R \subseteq R^{-1} \end{aligned}$$

and here again the fourth equivalence is a consequence of the fact that $(b,a) \in R \overset{val}{=} (a,b) \in R^{-1}$ by the definition of R^{-1}, and the last equivalence is the definition of a subset.

$$
\begin{aligned}
R \text{ is transitive} &\overset{val}{=} \forall a,b,c \in A.(a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R \\
&\overset{val}{=} \forall a,b,c\,[a,b,c \in A \wedge (a,b) \in R \wedge (b,c) \in R : (a,c) \in R] \\
&\overset{val}{=} \forall a,b,c\,[(a,b) \in R \wedge (b,c) \in R : (a,c) \in R] \\
&\overset{val}{=} \forall a,c\,[(a,c) \in R^2 : (a,c) \in R] \\
&\overset{val}{=} R^2 \subseteq R
\end{aligned}
$$

where the fourth equivalence requires more attention: Assume for all $a,b,c \in A$ when $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$ (1). Then for arbitrary $(a,c) \in R^2$ we have $a \in A, c \in A$ and there exists $b \in A$ such that $(a,b) \in R$ and $(b,c) \in R$. So, by (1) we get $(a,c) \in R$. This proves $R^2 \subseteq R$. For the opposite direction, assume that $R^2 \subseteq R$. Then for arbitrary $a,b,c \in A$ if $(a,b) \in R$ and $(b,c) \in R$, we have $(a,c) \in R^2$, and hence, by the assumption, $(a,c) \in R$. □

Example 5. We next mention several equivalence and order relation examples:

- Δ_X is an equivalence for any set X.
- Δ_X is also a partial order for any set X.
- $\leq$ on $\mathbb{N}$ is a partial order; it is also a chain (total / linear order).
- $\subseteq$ on $\mathcal{P}(M)$ is a partial order.
- $<$ on $\mathbb{N}$ is a strict order.
- $\subset$ on $\mathcal{P}(M)$ is a strict order.

In the next section we define an important (class of) equivalence(s) on $\mathbb{Z}$.

4 Important Equivalence on $\mathbb{Z}$

Definition 10 (Equivalence modulo n**).** *Let $n \in \mathbb{N}$. The relation $\equiv_n$ on $\mathbb{Z}$ is defined as*

$$i \equiv_n j \quad \textit{iff} \quad n|(i-j).$$

We say "i is equivalent (or equal or congruent) j modulo n" for $i \equiv_n j$.

Here $|$ denotes the divisibility relation on $\mathbb{Z}$, concretely in this case we have $n|(i-j)$ iff $i - j = k \cdot n$ for some $k \in \mathbb{Z}$, or as a predicate formula:

$$n|(i-j) \overset{val}{=} \exists k \in \mathbb{Z}.\, i - j = k \cdot n.$$

This way, we have defined infinitely many relations, one for each natural number n.

Example 6. For $n = 5$, we have $132 \equiv_5 2$ (as $132 - 2 = 130 = 26 \cdot 5$) and $1 \equiv_5 6$ (as $1 - 6 = -5 = (-1) \cdot 5$).

The following small result justifies the name of the relation $\equiv_n$, i.e, it justifies that we call this relation *equivalence* modulo n.

Lemma 2. *The relation $\equiv_n$ is an equivalence for every $n \in \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$ be arbitrary. We need to prove reflexivity, symmetry, and transitivity of $\equiv_n$.

Reflexivity: Let $i \in \mathbb{Z}$ be arbitrary. Then $i - i = 0 = 0 \cdot n$ and $0 \in \mathbb{Z}$. Hence $i \equiv_n i$. Since i was arbitrary, $\forall i \in \mathbb{Z}.\, i \equiv_n i$.

Symmetry: Let $i, j \in \mathbb{Z}$ be such that $i \equiv_n j$. Then $i - j = k \cdot n$ for some $k \in \mathbb{Z}$. But then $j - i = -(i - j) = -k \cdot n = (-k) \cdot n$ and $-k \in \mathbb{Z}$ showing that $j \equiv_n i$. Since i, j were arbitrary, we get $\forall i, j \in \mathbb{Z}.\, i \equiv_n j \Rightarrow j \equiv_n i$ and hence $\equiv_n$ is symmetric.

Transitivity: Let $i, j, l \in \mathbb{Z}$ be such that $i \equiv_n j$ and $j \equiv_n l$. Then there exist k_1 and k_2 in $\mathbb{Z}$ such that

$$i - j = k_1 \cdot n, \quad j - l = k_2 \cdot n.$$

But then

$$i - l = (i - j) + (j - l) = k_1 \cdot n + k_2 \cdot n = (k_1 + k_2) \cdot n$$

and $k_1 + k_2 \in \mathbb{Z}$, proving that $i \equiv_n l$. Again, since i, j, l were arbitrary, we get that $\forall i, j, l \in \mathbb{Z}.\, i \equiv_n j \wedge j \equiv_n l \Rightarrow i \equiv_n l$ and hence $\equiv_n$ is transitive. $\square$

Numbers and topics such as divisibility on $\mathbb{Z}$ and $\equiv_n$ will be studied more in the course on Discrete Mathematics, but also within our course we will refer to and use these equivalences multiple times.