Discrete Structures (2IT50)

Rob Hoogerwoord & Hans Zantema

August, 2016

Contents

Introduction, preliminaries

0.1 Introduction

These are the lecture notes of the course Discrete Structures 2IT50.

For further information on the course see
`http://www.win.tue.nl/~hzantema/ds.html`

The main assumed preknowledge for this course consists of basics from logic and set theory; in the sequal we summarize a few key points.

Discrete structures provide a tool box in computer science: notions like graphs, relations, orders, groups, counting arguments and basic number theory play a role in many topics in and related to computer science. The goal of this course is to provide a background in these topics. They all deal with mathematically precise definitions and formal reasoning. Therefore there is quite some emphasis on formal definitions and formal proofs.

We start by some preliminaries: we give some basics of set theory and we present the principle of induction.

0.2 Basic set theory

Sets (usually written by capitals) consist of zero or more elementsi (usually written by lower case letters). We write $x \in X$ for x being an element of X. We write $x \notin X$ as an abbreviation of $\neg(x \in X)$.

A set X is a *subset* of a set Y, notation $X \subseteq Y$ if $\forall x \in X : x \in Y$.

Two sets X and Y are equal, notation $X = Y$ if $X \subseteq Y$ and $Y \subseteq X$. So in order to prove $X = Y$ a standard way is to prove both $X \subseteq Y$ and $Y \subseteq X$, that is, take an arbitrary element $x \in X$ and prove that $x \in Y$, and conversely.

For sets X, Y we define

- the *intersection* $X \cap Y$, defined by
$$X \cap Y = \{x \mid x \in X \wedge x \in Y\}.$$
- the *union* $X \cup Y$, defined by
$$X \cup Y = \{x \mid x \in X \vee x \in Y\}.$$
- the *difference* $X \setminus Y$, defined by
$$X \setminus Y = \{x \mid x \in X \wedge x \notin Y\}.$$

If a *universe* U is fixed, then for $X \subseteq U$ we define its *complement* X^C by
$$X^C = \{x \in U \mid x \notin X\}.$$

These operations satisfy the following properties:

- Idempotence: $X \cap X = X$, $X \cup X = X$.
- Commutativity: $X \cap Y = Y \cap X$, $X \cup Y = Y \cup X$.
- Associativity: $(X \cap Y) \cap Z = X \cap (Y \cap Z)$, $(X \cup Y) \cup Z = X \cup (Y \cup Z)$.
- Distributivity: $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$, $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.
- DeMorgan's Laws: $(X \cup Y)^C = X^C \cap Y^C$, $(X \cap Y)^C = X^C \cup Y^C$.

These rules satisfy the principle of *duality*: if in a valid rule every symbol $\cup$ is replaced by $\cap$ and conversely, then a valid rule is obtained.

The operations presented until now all result in subsets of the same universe. This does not hold for the following two operations:

- The *Cartesian product*

$$X \times Y = \{(x, y) \mid x \in X \wedge y \in Y\}.$$

- The *Power set*

$$\mathcal{P}(X) = 2^X = \{Y \mid Y \subseteq X\}.$$

0.3 The principle of induction

In proving properties we often use the *principle of induction*. In its basic version it states:

> Let P be a property depending on natural numbers, for which $P(0)$ holds, and for every n we can conclude $P(n+1)$ from the induction hypothesis $P(n)$. Then $P(n)$ holds for every natural number n.

A fruitful variant, sometimes called *strong induction* is the following:

> Let P be a property depending on natural numbers, for which for every n we can conclude $P(n)$ from the induction hypothesis $\forall k < n : P(k)$. Then $P(n)$ holds for every natural number n.

Here k, n run over the natural numbers.

So the difference is as follows. In the basic version we prove $P(n+1)$ from the assumption that $P(n)$ holds, that is, for n being the direct predecessor of the value $n+1$ for which we want to prove the property. In contrast, in the strong version we try to prove $P(n)$, assuming that $P(k)$ holds for *all* predecessors k of n, not only the direct predecessor.

Surprisingly, we can prove validity of the strong version by only using the basic version, as follows.

Assume that we can conclude $P(n)$ from the (strong) induction hypothesis $\forall k < n : P(k)$. We have to prove that $P(n)$ holds for every natural number n. We do this by proving that $Q(n) \equiv \forall k < n : P(k)$ holds for every n, by (the basic version of) induction on n. First we observe that $Q(0)$ holds, which is trivially true since no natural number $k < 0$ exists. Next we assume the (basic) induction hypothesis $Q(n)$ and try to prove $Q(n+1) \equiv \forall k < n+1 : P(k)$. So let $k < n+1$. If $k < n$ then we conclude $P(k)$ by the (basic) induction hypothesis $Q(n)$. If not, then $k = n$, and by our start assumption we obtain $P(n)$. So we conclude $Q(n+1) \equiv \forall k < n+1 : P(k)$. So by the basic version of induction we conclude that $Q(n)$ holds for every n. But we had to conclude that $P(n)$ holds for every n. So let n be arbitrary. Since $n < n+1$ and we know that $Q(n+1)$ holds, we conclude that $P(n)$ holds, concluding the proof.

1 Relations

1.1 Binary relations

A (binary) *relation* R from set U to set V is a subset of the Cartesian product $U{\times}V$. If $(u,v){\in}R$, we say that u is in relation R to v . We usually denote this by $u\,R\,v$. Set U is called the *domain* of the relation and V its *range* (or: *codomain*). If $U{=}V$ we call R an *(endo)relation on* U .

1.1 Examples.

(a) "Is the mother of" is a relation from the set of all women to the set of all people. It consists of all pairs $(\,\mathit{person1}\,,\mathit{person2}\,)$ where $\mathit{person1}$ is the mother of $\mathit{person2}$. Of course, this relation also is an (endo)relation on the set of people.

(b) "There is a train connection between" is a relation on the set of cities in the Netherlands.

(c) The equality relation " $=$ " is a relation on every set. This relation is often denoted by I (and also called the "identity" relation). Because, however, every set has its "own" identity relation we sometimes use subscription to distinguish all these different identity relations. That is, for every set U we define I_U by:

$$I_U \;=\; \{\,(u,u) \mid u{\in}U\,\} \quad .$$

Whenever no confusion is possible and it is clear which set is intended, we drop the subscript and write just I instead of I_U , and in ordinary mathematical language we use " $=$ ", as always. So, for any set U and for all $u,v{\in}U$, we have: $u\,I\,v \;\Leftrightarrow\; u{=}v$.

(d) Integer n divides integer m , notation $n|m$, if there is an integer $q{\in}\mathbb{Z}$ such that $q{*}n{=}m$. Divides $|$ is the relation on $\mathbb{Z}$ that consists of all pairs $(n,m)\in\mathbb{Z}\times\mathbb{Z}$ with $(\exists q : q{\in}\mathbb{Z} : q{*}n{=}m)$.

(e) "Less than" ($<$) and "greater than" ($>$) are relations on $\mathbb{R}$, and on $\mathbb{Q},\mathbb{Z}$, and $\mathbb{N}$ as well, and so are "at most" ($\leq$) and "at least" ($\geq$).

(f) The set $\{\,(a,p)\,,\,(b,p)\,,\,(b,q)\,,\,(c,q)\,\}$ is a relation from $\{\,a,b,c\,\}$ to $\{\,p,q\,\}$.

(g) The set $\{\,(x,y)\in\mathbb{R}^2 \mid y=x^2\,\}$ is a relation on $\mathbb{R}$.

(h) Let Ω be a set, then "is a subset of" ($\subseteq$) is a relation on the set of all subsets of Ω .

Besides binary relations we can also consider n-ary relations for any $n{\geq}0$. An n-ary relation on sets $U_0,\cdots,U_{n-1}$ is a subset of the Cartesian product $U_0\times\cdots\times U_{n-1}$. Unless stated otherwise, in this text relations are binary.

Let R be a relation from set U to set V . Then for each element $u{\in}U$ we define $[\,u\,]_R$ as a subset of V , as follows:

$$[u]_R = \{v \in V \mid u R v\} \ .$$

(Sometimes $[u]_R$ is also denoted by $R(u)$.) This set is called the (R-)image of u. Similarly, for $v \in V$ a subset of U called ${}_R[v]$ is defined by:

$${}_R[v] = \{u \in U \mid u R v\} \ ,$$

which is called the (R-)pre-image of v.

1.2 Definition. If R is a relation from *finite* set U to *finite* set V, then R can be *represented* by means of a so-called *adjacency matrix*; sometimes this is convenient because it allows computations with (finite) relations to be carried out in terms of matrix calculations. We will see examples of this later.

With m for the *size* −the number of elements− of U and with n for the size of V, sets U and V can be represented by finite sequences, by numbering their elements. That is, we assume $U = \{u_1, \cdots, u_m\}$ and we assume $V = \{v_1, \cdots, v_n\}$. The adjacency matrix of relation R then is an $m \times n$ matrix A_R, say, the elements of which are 0 or 1 only, and defined by, for all $i, j : 1 \le i \le m \wedge 1 \le j \le n$:

$$A_R[i,j] = 1 \ \Leftrightarrow \ u_i \, R \, v_j \ .$$

Here $A_R[i,j]$ denotes the element of matrix A_R at row i and column j. Note that this definition is equivalent to stating that $A_R[i,j] = 0$ if and only if $\neg(u_i \, R \, v_j)$, for all i,j. Actually, adjacency matrices are *boolean* matrices in which, for the sake of conciseness, true is encoded as 1 and false as 0; thus, we might as well state that: $A_R[i,j] \Leftrightarrow u_i \, R \, v_j$.
□

Notice that this representation is not *unique*: the elements of finite sets can be assigned numbers in very many ways, and the distribution of 0's and 1's over the matrix depends crucially on how the elements of the two sets are numbered. For instance, if U has m elements it can be represented by $m!$ different sequences of length m; thus, a relation between sets of sizes m and n admits as many as $m! * n!$ (potentially different) adjacency matrices for its representation. Not surprisingly, if $U = V$ it is *good practice* to use one and the same element numbering for the two U's (in $U \times U$). If $1 \le i \le m$ then the set $[u_i]_R$ is represented by the row with index i in the adjacency matrix, that is:

$$[u_i]_R \ = \ \{ \, v_j \mid 1 \le j \le n \wedge A_R[i,j] = 1 \, \} \ .$$

Similarly, for $1 \le j \le n$ we have:

$${}_R[v_j] \ = \ \{ \, u_i \mid 1 \le i \le m \wedge A_R[i,j] = 1 \, \} \ .$$

1.3 Examples.

(a) An adjacency matrix for the relation $\{(a,p), (b,p), (b,q), (c,q)\}$ from $\{a,b,c\}$ to $\{p,q\}$ is:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \quad .$$

(b) Another adjacency matrix for the same relation and the same sets is obtained by reversing the order of the elements in one set: if we take (c, b, a) instead of (a, b, c) and if we keep (p, q) (as above), then the adjacency matrix becomes:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} \quad .$$

Note that standard set notation is *over specific*, as the order of the elements in an expression like $\{a, b, c\}$ is irrelevant: $\{a, b, c\}$ and $\{c, b, a\}$ are *the same* set! Therefore, when we decide to represent a relation by an adjacency matrix we need not take the order of the set's elements for granted: we really have quite some freedom here.

(c) An adjacency matrix for the identity relation on a set of size n is the $n \times n$ *identity matrix* I_n:

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \quad .$$

This matrix is unique, that is, independent of how the elements of the set are ordered, provided we stick to the convention of good practice, that both occurrences of the same set are ordered in the same way.

(d) An adjacency matrix of relation $\leq$ on the set $\{1, 2, 3, 4, 5\}$ is the upper triangular matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad .$$

* * *

Some relations have special properties, which deserve to be named.

1.4 Definition. Let R be a relation on a set U. Then R is called:

- *reflexive*, if for all $x \in U$ we have: $x R x$;
- *irreflexive*, if for all $x \in U$ we have: $\neg(x R x)$;
- *symmetric*, if for all $x, y \in U$ we have: $x R y \Leftrightarrow y R x$;
- *antisymmetric*, if for all $x, y \in U$ we have: $x R y \wedge y R x \Rightarrow x = y$;
- *transitive*, if for all $x, y, z \in U$ we have: $x R y \wedge y R z \Rightarrow x R z$.

1.5 Examples. We consider some of the examples given earlier:

(a) "Is the mother of" is a relation on the set of all people. It is irreflexive, antisymmetric, and not transitive.

(b) "There is a train connection between" is symmetric and transitive. If one is willing to accept traveling over a zero distance as a train connection, then this relation also is reflexive.

(c) On every set relation "equals" ($=$) is reflexive, symmetric, and transitive.

(d) Relation "divides" ($|$) is reflexive, antisymmetric, and transitive.

(e) "Less than" ($<$) and "greater than" ($>$) on $\mathbb{R}$ are irreflexive, antisymmetric, and transitive, whereas "at most" ($\leq$) and "at least" ($\geq$) are reflexive, antisymmetric, and transitive.

(f) The relation $\{ (x, y) \in \mathbb{R}^2 \mid y = x^2 \}$ is neither reflexive nor irreflexive.

□

For any relation R the proposition $(\forall x, y : x, y \in U : x R y \Leftrightarrow y R x)$ is (logically) equivalent to the proposition $(\forall x, y : x, y \in U : x R y \Rightarrow y R x)$, which is (formally) weaker. Hence, relation R is symmetric if $x R y \Rightarrow y R x$, for all $x, y \in U$. To *prove* that R is symmetric, therefore, it suffices to prove the latter, weaker, version of the proposition, whereas to *use* (in other proofs) that R is symmetric we may use the stronger version.

1.6 Lemma. Every reflexive relation R on set U satisfies: $u \in [u]_R$, for all $u \in U$.

Proof. By calculation:

$$
\begin{array}{ll}
 & u \in [u]_R \\
\Leftrightarrow & \qquad \{ \text{ definition of } [u]_R \ \} \\
 & u \, R \, u \\
\Leftrightarrow & \qquad \{ \ R \text{ is reflexive } \} \\
 & \mathsf{true}
\end{array}
$$

□

1.7 Lemma. Every symmetric relation R on set U satisfies: $v \in [u]_R \Leftrightarrow u \in [v]_R$, for all $u, v \in U$.

Proof. By calculation:

$$
\begin{array}{ll}
 & v \in [u]_R \\
\Leftrightarrow & \quad \{ \text{ definition of } [u]_R \ \} \\
 & u\,R\,v \\
\Leftrightarrow & \quad \{ \ R \text{ is symmetric } \} \\
 & v\,R\,u \\
\Leftrightarrow & \quad \{ \text{ definition of } [v]_R \ \} \\
 & u \in [v]_R
\end{array}
$$

□

* * *

If R is a relation on a finite set S, then special properties like reflexivity, symmetry and transitivity can be read off from the adjacency matrix. For example, R is reflexive if and only if the main diagonal of R's adjacency matrix contains 1's only, that is if $A_R[i,i] = 1$ for all (relevant) i.

Relation R is symmetric if and only if the transposed matrix A_R^{T} equals A_R. The *transposed matrix* M^{T} of an $m \times n$ matrix M is the $n \times m$ matrix defined by, for all i, j:

$$M^{\mathrm{T}}[j,i] \ = \ M[i,j] \quad .$$

1.2 Equivalence relations

Relations that are reflexive, symmetric, and transitive deserve some special attention: they are called *equivalence relations*.

1.8 Definition. A relation R is an *equivalence relation* if and only if it is reflexive, symmetric, and transitive.
□

If elements u and v are related by an equivalence relation R, that is, if uRv, then u and v are also called "equivalent (under R)".

1.9 Example. On every set relation "equals" ($=$) is an equivalence relation.

1.10 Example. Consider the plane $\mathbb{R}^2$ and in it the set S of straight lines. We call two lines in S parallel if and only if they are equal or do not intersect. Hence, two lines in S are parallel if and only if their slopes are equal. Being parallel is an equivalence relation on the set S.

1.11 Example. We consider a fixed $d \in \mathbb{Z}$, $d > 0$, and we define a relation R on $\mathbb{Z}$ by: $m\,R\,n$ if and only if $m - n$ is divisible by d. The latter can be formulated as $(m-n) \,\mathsf{mod}\, d = 0$, and a more traditional mathematical rendering of this is $m = n\,(\mathsf{mod}\, d)$. Thus defined, R is an equivalence relation.
□

Actually, the last two examples are instances of Theorem 1.13. Before giving this theorem, first we introduce equivalence classes and prove a lemma about them.
If R is an equivalence relation on set U, then, for every $u \in U$ the set $[\,u\,]_R$ is called the *equivalence class of* u. Because equivalence relations are reflexive we have, as we have seen in lemma 1.6: $u \in [\,u\,]_R$, for all $u \in U$. From this it follows immediately that equivalence classes are nonempty. Equivalence classes have several other interesting properties. For example, the equivalence classes of two elements are equal if and only if these elements are equivalent:

1.12 Lemma. Every equivalence relation R on set U satisfies, for all $u, v \in U$:

$$[\,u\,]_R = [\,v\,]_R \;\Leftrightarrow\; u\,R\,v \quad .$$

Proof. The left-hand side of this equivalence contains the function $[\,\cdot\,]_R$, whereas the right-hand side does not. To eliminate $[\,\cdot\,]_R$ we rewrite the left-hand side first:

$$\begin{array}{ll} & [\,u\,]_R = [\,v\,]_R \\ \Leftrightarrow & \quad \{ \text{ set equality } \} \\ & (\forall x : x \in U : x \in [\,u\,]_R \Leftrightarrow x \in [\,v\,]_R\,) \\ \Leftrightarrow & \quad \{ \text{ definition of } [\,\cdot\,]_R \;\} \\ & (\forall x : x \in U : u\,R\,x \;\Leftrightarrow\; v\,R\,x\,) \quad , \end{array}$$

hence, the lemma is equivalent to:

$$(\forall x : x \in U : u\,R\,x \;\Leftrightarrow\; v\,R\,x\,) \;\;\Leftrightarrow\;\; u\,R\,v \quad .$$

This we prove by mutual implication.

$$\begin{array}{ll} \text{“}\Rightarrow\text{”:} & (\forall x : x \in U : u\,R\,x \;\Leftrightarrow\; v\,R\,x\,) \\ \Rightarrow & \quad \{ \text{ instantiation } x := v \;\} \\ & u\,R\,v \;\Leftrightarrow\; v\,R\,v \\ \Leftrightarrow & \quad \{ \; R \text{ is an equivalence relation, so it is reflexive } \} \\ & u\,R\,v \quad . \end{array}$$

“$\Leftarrow$”: Assuming $u\,R\,v$ and for any $x \in U$ we prove $u\,R\,x \Leftrightarrow v\,R\,x$, again by mutual implication:

$$\begin{array}{ll} & u\,R\,x \\ \Leftrightarrow & \quad \{ \text{ assumption } \} \end{array}$$

$$
\begin{array}{ll}
 & u\,R\,v \;\;\wedge\;\; u\,R\,x \\
\Leftrightarrow & \qquad \{\ R \text{ is an equivalence relation, so it is symmetric }\} \\
 & v\,R\,u \;\;\wedge\;\; u\,R\,x \\
\Rightarrow & \qquad \{\ R \text{ is an equivalence relation, so it is transitive }\} \\
 & v\,R\,x \quad ,
\end{array}
$$

and:

$$
\begin{array}{ll}
 & v\,R\,x \\
\Leftrightarrow & \qquad \{\ \text{assumption }\} \\
 & u\,R\,v \;\;\wedge\;\; v\,R\,x \\
\Rightarrow & \qquad \{\ R \text{ is an equivalence relation, so it is transitive }\} \\
 & u\,R\,x \quad ,
\end{array}
$$

which concludes the proof of this lemma.

□

1.13 Theorem. A relation R on a set U is an equivalence relation if and only if a set V and a function $f : U \to V$ exists such that

$$x\,R\,y \;\;\Leftrightarrow\;\; f(x) = f(y)$$

for all $x, y{\in}U$.

Proof.

First we prove the 'if'-part: assume such a V and f exists; we have to prove that R is an equivalence relation.

Choose $x \in U$ arbitrary, then xRx holds since $f(x) = f(x)$. So R is reflexive.

Choose $x, y \in U$ arbitrary for which then xRy holds. Then $f(x) = f(y)$, so also $f(y) = f(x)$, so yRx holds. So R is symmetric.

Choose $x, y, z \in U$ arbitrary for which xRy and yRz holds. Then $f(x) = f(y)$ and $f(y) = f(z)$, so also $f(x) = f(z)$. Hence xRz holds. This proves that R is transitive.

Combining these three properties we conclude that R is an equivalence relation, concluding the 'if'-part.

Next we prove the 'only if'-part: assume R is an equivalence relation; we have to find V and f having the required property.

Choose V to be the set of all subsets of U and define $f(x) = [\,x\,]_R$ for all $x \in U$. Then the required property

$$x\,R\,y \;\;\Leftrightarrow\;\; f(x) = f(y)$$

holds due to Lemma 1.12.

□

1.14 Example. We reconsider Example 1.11. The predicate $(m-n) \bmod d = 0$ is equivalent to $m \bmod d = n \bmod d$, so with $\mathbb{Z}$ both for set U and for set V, function f, defined by $f(m) = m \bmod d$, for all $m \in \mathbb{Z}$, does the job.
□

As a further investigation of equivalence classes we now observe that they are either disjoint or equal:

1.15 Lemma. Every equivalence relation R on set U satisfies, for all $u, v \in U$:

$$[u]_R \cap [v]_R = \emptyset \ \vee \ [u]_R = [v]_R \quad .$$

Proof. This proposition is equivalent to:

$$[u]_R \cap [v]_R \neq \emptyset \ \Rightarrow \ [u]_R = [v]_R \quad ,$$

which we prove as follows:

$$\begin{array}{ll}
 & [u]_R \cap [v]_R \neq \emptyset \\
\Leftrightarrow & \quad \{ \text{ definition of } \emptyset \text{ and } \cap \ \} \\
 & (\exists x : x \in U : x \in [u]_R \wedge x \in [v]_R \,) \\
\Leftrightarrow & \quad \{ \text{ definition of } [\,\cdot\,]_R \ \} \\
 & (\exists x : x \in U : u\,R\,x \wedge v\,R\,x \,) \\
\Rightarrow & \quad \{ \ R \text{ is symmetric and transitive } \} \\
 & (\exists x : x \in U : u\,R\,v \,) \\
\Rightarrow & \quad \{ \text{ predicate calculus } \} \\
 & u\,R\,v \\
\Leftrightarrow & \quad \{ \text{ lemma 1.12 } \} \\
 & [u]_R = [v]_R
\end{array}$$

□

The equivalence classes of an equivalence relation "cover" the set:

1.16 Lemma. Every equivalence relation R on set U satisfies: $(\bigcup_{u:\, u \in U} [u]_R) = U$.

Proof. By mutual set inclusion. On the one hand, every equivalence class is a subset of U, that is: $[u]_R \subseteq U$, for all $u \in U$; hence, their union, $(\bigcup_{u:\, u \in U} [u]_R)$, is a subset of U as well. On the other hand, we have for every $v \in U$ that $v \in [v]_R$, so, also $v \in (\bigcup_{u:\, u \in U} [u]_R)$. Hence, U is a subset of $(\bigcup_{u:\, u \in U} [u]_R)$ too.
□

These lemmas show that the equivalence classes of an equivalence relation form a, so-called, *partition* of set U.

1.17 Definition. A partition of set U is a set Π of nonempty and disjoint subsets of U, the union of which equals U. Formally, that set Π is a partition of U means the conjunction of:

(a) $(\forall X : X \in \Pi : X \subseteq U \wedge X \neq \emptyset)$
(b) $(\forall X, Y : X, Y \in \Pi : X \cap Y = \emptyset \vee X = Y)$
(c) $(\bigcup_{X : X \in \Pi} X) = U$
□

Clause (a) in this definition expresses that the elements of a partition of U are nonempty subsets of U, clause (b) expresses that the sets in a partition are disjoint, whereas clause (c) expresses that the sets in a partition together "cover the whole" U. Phrased differently, clause (b) and (c) together express that every element of U is an element of *exactly one* of the sets in the partition.

Conversely, every partition also represents an equivalence relation. Every element of set U is element of exactly one of the subsets in the partition. "Being in the same subset" (in the partition) is an equivalence relation.

1.18 Theorem. Every partition Π of a set U represents an equivalence relation on U, the equivalence classes of which are the sets in Π.

Proof. Because Π is a partition, every element of U is an element of a unique subset in Π. Now, the relation "being elements of the same subset in Π" is an equivalence relation. Formally, we prove this by defining a function $\varphi : U \to \Pi$, as follows, for all $u \in U$ and $X \in \Pi$:

$$\varphi(u) = X \;\Leftrightarrow\; u \in X \quad .$$

Thus defined, φ is a function indeed, because for every $u \in U$ one and only one $X \in \Pi$ exists satisfying $u \in X$. Now relation $\sim$ on U, defined by, for all $u, v \in U$:

$$u \sim v \;\Leftrightarrow\; \varphi(u) = \varphi(v) \quad ,$$

is an equivalence relation – Theorem 1.13 ! –. Furthermore, by its very construction φ satisfies $u \in \varphi(u)$ and, hence, $\varphi(u)$ is the equivalence class of u, for all $u \in U$.
□

1.3 Operations on Relations

Relations between two sets are subsets of the Cartesian Product of these two sets. Hence, all usual set operations can be applied to relations as well. In addition, relations admit of some dedicated operations that happen to have nice algebraic properties. It is even possible to develop a viable Relational Calculus, but this falls outside the scope of this text.

These relational operations play an important role in the mathematical study of programming constructs, such as recursion and data structures. They are also useful in some theorems about graphs. We will see applications of this later.

1.3.1 Set operations

- For sets U and V, the *extreme relations* from U to V are the *empty relation* $\emptyset$ and the *full relation* $U \times V$. For the sake of brevity and symmetry, we denote these two relations by $\perp$ ("bottom") and $\top$ ("top"), respectively; element wise, they satisfy, for all $u \in U$ and $v \in V$:

$$\neg(u \perp v) \quad \wedge \quad u \top v \quad .$$

  For example, every relation R satisfies: $\perp \subseteq R$ and $R \subseteq \top$, which is why we call $\perp$ and $\top$ the extreme relations.

- If R and S are relations, with the same domain and and with the same range, then $R \cup S$, and $R \cap S$, and $R \setminus S$ are relations too, between the same sets as R and S, and with the obvious meaning. The complement R^{C} of relation R is $\top \setminus R$.

- These operations have their usual algebraic properties. In particular, $\top$ and $\perp$ are the identity elements of $\cup$ and $\cap$, respectively: $R \cup \perp = R$ and $R \cap \top = R$. They are zero elements as well, that is: $R \cup \top = \top$ and $R \cap \perp = \perp$.

1.3.2 Transposition

With every relation R from set U to set V a corresponding relation exists from V to U that contains (v, u) if and only if $(u, v) \in R$. This relation is called the *transposition* of R and is denoted by R^{T}. (Some mathematicians use R^{-1}, but this may be confusing: transposition is not the same as inversion, especially with functions.) Formally, transposition is defined as follows.

1.19 Definition. For every relation R from set U to set V, relation R^{T} from V to U is defined by, for all $v \in V$ and $u \in U$:

$$v\, R^{\mathrm{T}} u \;\Leftrightarrow\; u R v \quad .$$

1.20 Lemma. Transposition distributes over all set operations, that is:

$$\begin{array}{l}
\perp^{\mathrm{T}} = \perp \;\text{ and: }\; \top^{\mathrm{T}} = \top \quad ; \\
(R \cup S)^{\mathrm{T}} \;=\; R^{\mathrm{T}} \cup S^{\mathrm{T}} \quad ; \\
(R \cap S)^{\mathrm{T}} \;=\; R^{\mathrm{T}} \cap S^{\mathrm{T}} \quad ; \\
(R \setminus S)^{\mathrm{T}} \;=\; R^{\mathrm{T}} \setminus S^{\mathrm{T}} \quad ; \\
(R^{\mathrm{C}})^{\mathrm{T}} = (R^{\mathrm{T}})^{\mathrm{C}} \quad .
\end{array}$$

1.21 Lemma. Transposition is its own *inverse*, that is, every relation R satisfies:

$$(R^{\mathrm{T}})^{\mathrm{T}} = R \quad .$$

□

For finite relations there is a direct connection between relation transposition and matrix transposition:

1.22 Lemma. If A_R is an adjacency matrix for relation R then $(A_R)^{\mathrm{T}}$ is an adjacency matrix for R^{T}.

1.23 Examples. Properties of relations, like (ir)reflexivity and (anti)symmetry, can now be expressed concisely by means of relational operations; for R a relation on set U:

- "R is reflexive" $\Leftrightarrow$ $I_U \subseteq R$
- "R is irreflexive" $\Leftrightarrow$ $I_U \cap R = \perp$
- "R is symmetric" $\Leftrightarrow$ $R^{\mathrm{T}} = R$
- "R is antisymmetric" $\Leftrightarrow$ $R \cap R^{\mathrm{T}} \subseteq I_U$

□

Unfortunately, transitivity cannot be expressed so nicely in terms of the set operations. For this we need yet another operation on relations, which turns out to be quite useful for other purposes too.

1.3.3 Composition

Let R be a relation from U to V and let S be a relation from V to W. If $u\,R\,v$, for some $v{\in}V$ and if $v\,S\,w$, for that *same* v, then we say that u is related to w in the *composition* of R and S, written as $R\,;S$. So, the composition of R and S is a relation from U to W. Phrased differently, in this composition $u{\in}U$ is related to $w{\in}W$ if u and w are "connected via" some "intermediate" value in V. This is rendered formally as follows.

1.24 Definition. If R is a relation from U to V, and if S is a relation from V to W, then the composition $R\,;S$ is the relation from U to W defined by, for all $u{\in}U$ and $w{\in}W$:

$$u\,(R\,;S)\,w \;\Leftrightarrow\; (\exists v : v{\in}V : u R v \wedge v S w) \quad .$$

1.25 Example. Let $R = \{(1,2),(2,3),(2,4),(3,1),(3,3)\}$ be a relation from $\{1,2,3\}$ to $\{1,2,3,4\}$ and let $S = \{(1,a),(2,c),(3,a),(3,d),(4,b)\}$ be a relation from $\{1,2,3,4\}$ to $\{a,b,c,d\}$. Then the composition $R\,;S$ is the relation $\{(1,c),(2,a),(2,b),(2,d),(3,a),(3,d)\}$, from $\{1,2,3\}$ to $\{a,b,c,d\}$.

1.26 Lemma. For any endorelation R we have:

$$R \text{ is transitive} \;\Leftrightarrow\; (R\,;R) \subseteq R \quad .$$

Proof. Assume R is transitive. Let $(x,y) \in R;R$. Then there exists z such that $(x,z) \in R$ and $(z,y) \in R$. By transitivity we conclude that $(x,y) \in R$. So we have proved $R;R \subseteq R$.

Conversely, assume $R;R \subseteq R$. Let xRy and yRz. Then by definition of composition we have $(x,z) \in R;R$. Since $R;R \subseteq R$ we conclude $(x,z) \in R$, by which we have proved that R is transitive.
□

1.27 Lemma. The identity relation is the identity of relation composition. More precisely, every relation R from set U to set V satisfies: $I_U \,;R = R$ and $R\,; I_V = R$.
Proof. We prove the first claim; the second is similar.

If $(x,y) \in I_U;R$ then there exists $z \in U$ such that $(x,z) \in I_U$ and $(z,y) \in R$. From the definition of I_U we conclude $x = z$, so from $(z,y) \in R$ we conclude $(x,y) \in R$.

Conversely, let $(x,y) \in R$. Then $(x,x) \in I_U$, so $(x,y) \in I_U;R$.

□

1.28 Lemma. Relation composition is associative, that is, all relations R,S,T satisfy: $(R\,;S)\,;T = R\,;(S\,;T)$.

Proof. For all u,x we calculate:

$$
\begin{array}{ll}
 & u\,((R\,;S)\,;T)\,x \\
\Leftrightarrow & \quad \{ \text{ definition of } ; \ \} \\
 & (\exists w :: \ u\,(R;S)\,w \wedge wTx\,) \\
\Leftrightarrow & \quad \{ \text{ definition of } ; \ \} \\
 & (\exists w :: \ (\exists v :: uRv \wedge vSw) \ \wedge wTx\,) \\
\Leftrightarrow & \quad \{ \wedge \text{ over } \exists \ \} \\
 & (\exists w :: \ (\exists v :: uRv \wedge vSw \wedge wTx\,)\,) \\
\Leftrightarrow & \quad \{ \text{ swapping dummies } \} \\
 & (\exists v :: \ (\exists w :: uRv \wedge vSw \wedge wTx\,)\,) \\
\Leftrightarrow & \quad \{ \text{ (almost) the same steps as above, in reverse order } \} \\
 & u\,(R\,;(S\,;T))\,x
\end{array}
$$

□

Remark: In other mathematical texts relation composition is sometimes called "(relational) product", denoted by infix operator $*$. From a formal point of view, this is harmless, of course, but it is important to keep in mind that composition is *not commutative*: generally, $R\,;S$ differs from $S\,;R$. This is the reason why we prefer to use an asymmetric symbol, " ; ", to denote composition: from a practical point of view the term "product" and the symbol " $*$ " may be misleading.
□

An important property is that relation composition *distributes over arbitrary unions* of relations, both from the left and from the right:

1.29 Theorem. Every relation R and every collection Ω of relations satisfies:

$$R\,;\,(\bigcup_{X:X\in\Omega} X) \;=\; (\bigcup_{X:X\in\Omega} R\,;X) \quad ,$$

and also:

$$(\bigcup_{X:X\in\Omega} X)\,;\,R \;=\; (\bigcup_{X:X\in\Omega} X\,;R) \quad .$$

Proof. We prove the first claim; the second is similar.
$(x,y) \in R;(\bigcup_{X:X\in\Omega} X)$
$\quad\Leftrightarrow \qquad$ { definition composition }
$\exists z : (x,z) \in R \wedge (z,y) \in \bigcup_{X:X\in\Omega} X$
$\quad\Leftrightarrow \qquad$ { definition $\bigcup$ }
$\exists z : (x,z) \in R \wedge \exists X \in \Omega : (z,y) \in X$
$\quad\Leftrightarrow \qquad$ { property $\exists$ }
$\exists X \in \Omega : \exists z : (x,z) \in R \wedge (z,y) \in X$
$\quad\Leftrightarrow \qquad$ { definition composition }
$\exists X \in \Omega : (x,y) \in R;X$
$\quad\Leftrightarrow \qquad$ { definition $\bigcup$ }
$(x,y) \in \bigcup_{X:X\in\Omega} R;X$.

□

Corollary: Relation composition is *monotonic*, that is, for all relations R, S, T:

$S \subseteq T \;\Rightarrow\; R\,;S \subseteq R\,;T$, and also:

$R \subseteq S \;\Rightarrow\; R\,;T \subseteq S\,;T$.

□

* * *

The n-fold composition of a relation R with itself also is written as R^n, as follows.

1.30 Definition. (exponentiation of relations) For any (endo)relation R and for all natural n, we define (recursively):

$$R^0 = I \;\wedge\; R^{n+1} = R\,;R^n \quad .$$

□

For example, the formula expressing transitivity of R, as in Lemma 1.26, can now also be written as: $R^2 \subseteq R$.

1.31 Lemma. For endorelation R and for all natural m and n:

$$R^{m+n} \;=\; R^m \,;R^n \quad .$$

Proof. We apply induction on m. For $m = 0$ using Lemma 1.27 we obtain

$$R^{0+n} \;=\; R^n \;=\; I; R^n \;=\; R^0; R^n.$$

For the induction step we assume the induction hypothesis $R^{m+n} = R^m; R^n$.

$$\begin{array}{rcll} R^{(m+1)+n} & = & R^{(m+n)+1} & \\ & = & R; R^{m+n} & \text{(definition)} \\ & = & R; (R^m; R^n) & \text{(induction hypothesis)} \\ & = & (R; R^m); R^n & \text{(associativity, Lemma 1.28)} \\ & = & R^{m+1}; R^n, & \text{(definition)} \end{array}$$

concluding the proof.
□

* * *

In the representation of relations by adjacency matrices, relation composition is represented by matrix multiplication. That is, if A_R is an adjacency matrix for relation R and if A_S is an adjacency matrix for relation S then the product matrix $A_R \times A_S$ is an adjacency matrix for the composition $R\,;S$. This matrix product is well-defined only if the number of columns of matrix A_R equals the number of rows of matrix A_S. This is true because the number of columns of A_R equals the size of the range of relation R. As this range also is the domain of relation S –otherwise composition of R and S is impossible– this size also equals the number of rows of A_S.

Recall that adjacency matrices actually are boolean matrices; hence, the matrix multiplication must be performed with boolean operations, not integer operations, in such a way that addition and multiplication boil down to disjunction ("or") and conjunction ("and") respectively. So, a formula like $(\Sigma j :: A_R[i,j] * A_S[j,k]\,)$ actually becomes: $(\exists j :: A_R[i,j] \wedge A_S[j,k]\,)$.

1.32 Example. Let $R = \{(1,2), (2,3), (2,4), (3,1), (3,3)\}$ be a relation from $\{1,2,3\}$ to $\{1,2,3,4\}$ and let $S = \{(1,a), (2,c), (3,a), (3,d), (4,b)\}$ be a relation from $\{1,2,3,4\}$ to $\{a,b,c,d\}$. Then adjacency matrices for R and S are:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \;\text{, and:}\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad .$$

The product of these matrices is an adjacency matrix for $R\,;S$:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad .$$

1.3.4 Closures

Some (endo)relations have properties, like reflexivity, symmetry, or transitivity, whereas other relations do not. For any such property, the *closure* of a relation with respect to that property is the *smallest extension* of the relation that does have the property. More precisely, it is fully characterized by the following definition.

1.33 Definition. (closure) Let $\mathcal{P}$ be a predicate on relations, then the $\mathcal{P}$-closure of relation R is the relation S satisfying the following three requirements:

(a) $R \subseteq S$,

(b) $\mathcal{P}(S)$,

(c) $R \subseteq X \land \mathcal{P}(X) \Rightarrow S \subseteq X$, for all relations X.

Indeed, (a) expresses that S is an *extension* of R, and (b) expresses that S has property $\mathcal{P}$, and (c) expresses that S is contained in every relation X that is an extension of R and that has property $\mathcal{P}$; this is what we mean by the *smallest* extension of R.

For instance, if a relation R already has property $\mathcal{P}$, so $\mathcal{P}(R)$ holds, then $S = R$ satisfies the properties (a), (b) and (c), so we conclude that then the $\mathcal{P}$-closure of R is R itself.

For any given property $\mathcal{P}$ and relation R the $\mathcal{P}$-closure of R need not exist, but if it exists it is unique, as is stated in the following theorem.

1.34 Theorem. If both S and S' satisfy properties (a), (b) and (c) from Definition 1.33, then $S = S'$.

Proof. By (a) and (b) for S we conclude $R \subseteq S$ and $\mathcal{P}(S)$, so by property (c) for S' we conclude $S' \subseteq S$.

By (a) and (b) for S' we conclude $R \subseteq S'$ and $\mathcal{P}(S')$, so by property (c) for S we conclude $S \subseteq S'$.

Combining $S' \subseteq S$ and $S \subseteq S'$ yields $S = S'$. □

* * *

The simplest possible property of relations is reflexivity. The reflexive closure of an (endo)relation R now is the smallest extension of R that is reflexive.

1.35 Theorem. The reflexive closure of a relation R is $R \cup I$.

Proof. We have to prove (a), (b) and (c) for $\mathcal{P}$ being reflexivity. Indeed, $R \subseteq R \cup I$, proving (a), and $R \cup I$ is reflexive since $I \subseteq R \cup I$, proving (b). For proving (c) assume that $R \subseteq X$ and X reflexive; we have to prove that $R \cup I \subseteq X$. Let $(x, y) \in R \cup I$. Then $(x, y) \in R$ or $(x, y) \in I$. If $(x, y) \in R$ then from $R \subseteq X$ we conclude $(x, y) \in X$; if $(x, y) \in I$ then from reflexivity we conclude that $(x, y) \in X$. So in both cases we have $(x, y) \in X$, so $R \cup I \subseteq X$, concluding the proof. □

1.36 Theorem. The symmetric closure of a relation R is $R \cup R^{\mathrm{T}}$.

Proof. We have to prove (a), (b) and (c) for $\mathcal{P}$ being symmetry. Indeed, $R \subseteq R \cup R^{\mathrm{T}}$, proving (a).

For proving (b) let $(x, y) \in R \cup R^{\mathrm{T}}$. If $(x, y) \in R$ then $(y, x) \in R^{\mathrm{T}} \subseteq R \cup R^{\mathrm{T}}$. If $(x, y) \in R^{\mathrm{T}}$ then $(y, x) \in (R^{\mathrm{T}})^{\mathrm{T}} = R \subseteq R \cup R^{\mathrm{T}}$. So in both cases $(y, x) \in R \cup R^{\mathrm{T}}$, proving that i$R \cup R^{\mathrm{T}}$ is symmetric, so proving (b).

For proving (c) assume that $R \subseteq X$ and X is symmetric; we have to prove that $R \cup R^{\mathrm{T}} \subseteq X$. Let $(x, y) \in R \cup R^{\mathrm{T}}$. If $(x, y) \in R$ then from $R \subseteq X$ we conclude $(x, y) \in X$. If $(x, y) \in R^{\mathrm{T}}$ then $(y, x) \in R \subseteq X$; since X is symmetric we conclude $(x, y) \in X$. So in both cases we have $(x, y) \in X$, concluding the proof. □

*   *   *

The game becomes more interesting when we ask for the *transitive closure* of a relation R.

We define

$$R^{+} \;=\; \bigcup_{i=1}^{\infty} R^{i} \;=\; R \cup R^{2} \cup R^{3} \cup R^{4} \cup \cdots .$$

1.37 Theorem. The transitive closure of a relation R is R^{+}.

Proof. We have to prove (a), (b) and (c) for $\mathcal{P}$ being transitivity. Indeed, $R \subseteq R^{+}$, proving (a).

For proving (b) we have to prove that R^{+} is transitive. So let $(x, y), (y, z) \in R^{+}$. Since $R+ = \bigcup_{i=1}^{\infty} R^{i}$ there are $i, j \geq 1$ such that $(x, y) \in R^{i}$ and $(y, z) \in R^{j}$. So $(x, z) \in R^{i}; R^{j} = R^{i+j}$ by Lemma 1.31. Since $R^{i+j} \subseteq \bigcup_{i=1}^{\infty} R^{i} = R^{+}$ we conclude $(x, z) \in R^{+}$, concluding the proof of (b).

For proving (c) assume that $R \subseteq X$ and X is transitive; we have to prove that $R^{+} \subseteq X$. For doing so first we prove that $R^{n} \subseteq X$ for all $n \geq 1$, by induction on n. For $n = 1$ this is immediate from the assumption $R \subseteq X$. So next assume the induction hypothesis $R^{n} \subseteq X$ and we will prove $R^{n+1} \subseteq X$. Let $(x, y) \in R^{n+1} = R; R^{n}$, so there exists z such that $(x, z) \in R$ and $(z, y) \in R^{n}$. Since $R \subseteq X$ we conclude $(x, z) \in X$, and by the induction hypothesis we conclude $(z, y) \in X$. Since X is transitive we conclude $(x, y) \in X$. Hence $R^{n+1} \subseteq X$. By the principle of induction we have proved $R^{n} \subseteq X$ for all $n \geq 1$.

For (c) we had to prove $R^{+} \subseteq X$. So let $(x, y) \in R^{+} = \bigcup_{i=1}^{\infty} R^{i}$. Then there exists $n \geq 1$ such that $(x, y) \in R^{n}$. Since $R^{n} \subseteq X$ we conclude $(x, y) \in X$, concluding the proof. □

In computer science the notation $+$ is often used for 'one or more times', while notation $*$ is often used for 'zero or more times'. Consistent with this convention we define

$$R^{*} \;=\; \bigcup_{i=0}^{\infty} R^{i} \;=\; I \cup R \cup R^{2} \cup R^{3} \cup R^{4} \cup \cdots .$$

It can be shown that R^* is the reflexive-transitive closure of R, that is, the $\mathcal{P}$-closure for $\mathcal{P}$ being the conjunction of reflexivity and transitivity.

1.4 Exercises

1. Give an example of a relation that is:
   (a) both reflexive and irreflexive;
   (b) neither reflexive nor irreflexive;
   (c) both symmetric and antisymmetric;
   (d) neither symmetric nor antisymmetric.

2. For each of the following relations, investigate whether it is (ir)reflexive, (anti-) symmetric, and/or transitive:
   (a) $R = \{(x,y) \in \mathbb{R}^2 \mid x+1 < y\}$
   (b) $S = \{(x,y) \in \mathbb{R}^2 \mid x < y+1\}$
   (c) $T = \{(x,y) \in \mathbb{Z}^2 \mid x < y+1\}$

3. Prove that each irreflexive and transitive relation is antisymmetric.

4. Which of the following relations on set U, with $U = \{1,2,3,4\}$, is reflexive, irreflexive, symmetric, antisymmetric, or transitive?
   (a) $\{(1,3),(2,4),(3,1),(4,2)\}$;
   (b) $\{(1,3),(2,4)\}$;
   (c) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(2,4),(3,1),(4,2)\}$;
   (d) $\{(1,1),(2,2),(3,3),(4,4)\}$;
   (e) $\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,3),(3,4),(4,3),(3,2),(2,1)\}$.

5. Construct for each of the relations in Exercise 4 the adjacency matrix.

6. Let R be a relation on a set U. Prove that, if $[u]_R \neq \emptyset$, for all $u \in U$, and if R is symmetric and transitive, then R is reflexive.

7. The natural numbers admit addition but not subtraction: if $a < b$ the difference $a-b$ is undefined, because it is not a natural number. To achieve a structure in which all differences are defined we need the "integer numbers". These can be constructed from the naturals in the following way, a process called "definition by abstraction".

   We consider the set V of all pairs of natural numbers, so $V = \mathbb{N} \times \mathbb{N}$. On V we define a relation $\sim$, as follows, for all $a,b,c,d \in \mathbb{N}$:

   $$(a,b) \sim (c,d) \quad \Leftrightarrow \quad a+d = c+b \quad .$$

(a) Prove that $\sim$ is an equivalence relation.

(b) Formulate in words what this equivalence relation expresses.

(c) We investigate the equivalence classes of $\sim$. Obviously, there is a class containing the pair $(0,0)$. Prove that, in addition, every *other* class contains *exactly one* pair of the shape either $(a,0)$ or $(0,a)$, so not both in the same class, with $1 \leq a$.

(d) We call the pairs $(0,0)$, $(a,0)$ and $(0,a)$, with $1 \leq a$, the "representants" of the equivalence classes. These classes can now be ordered in the following way, by means of their representants:

$$\cdots, (0,2), (0,1), (0,0), (1,0), (2,0), (3,0), \cdots \quad .$$

We call these classes "integer numbers"; a more usual notation of the representants is:

$$\cdots, -2, -1, 0, +1, +2, +3, \cdots \quad .$$

Thus, we obtain the integer numbers indeed. To illustrate this: define, on the set of representants, two binary operators pls and min that correspond with the usual "addition" and "subtraction". Also define the "less than" relation on the set of representants.

8. Prove that every reflexive and transitive endorelation R satisfies: $R^2 = R$.

9. Construct for each relation, named R here, in Exercise 4 an adjacency matrix for R^2.

10. Suppose R and S are finite relations with adjacency matrices A and B, respectively. Define adjacency matrices, in terms of A and B, for the relations $R \cup S$, $R \cap S$, $R \backslash S$, and R^{C}.

11. Suppose R and S are endorelations. Prove or disprove:

(a) If R and S are reflexive, then so is $R ; S$.

(b) If R and S are irreflexive, then so is $R ; S$.

(c) If R and S are symmetric, then so is $R ; S$.

(d) If R and S are antisymmetric, then so is $R ; S$.

(e) If R and S are transitive, then so is $R ; S$.

(f) If R and S are equivalence relations, then so is $R ; S$.

12. Prove that every endorelation R satisfying $R \subseteq I$ satisfies:

(a) R is symmetric.

(b) R is antisymmetric.

(c) R is transitive.

13. Let $\mathcal{D}$ be the set of differentiable functions $f : \mathbb{R} \to \mathbb{R}$. On $\mathcal{D}$ we define a relation $\sim$ as follows, for all $f, g \in \mathcal{D}$:

$$f \sim g \;\Leftrightarrow\; \text{“function } f-g \text{ is constant”} \quad .$$

Prove that $\sim$ is an equivalence relation. How can relation $\sim$ be defined in the way of Theorem 1.13?

14. We consider the relation $\sim$ on $\mathbb{Z}$ defined by, for all $x, y \in \mathbb{Z}$:

$$x \sim y \;\Leftrightarrow\; (\exists z \in \mathbb{Z} : x - y = 7z)$$

Prove that $\sim$ is an equivalence relation. Describe the equivalence classes of $\sim$. In particular, establish how many equivalence classes $\sim$ has.

15. Let R and S be two equivalence relations on a finite set U satisfying $R \subseteq S$.

    (a) Prove that every equivalence class of R is a subset of an equivalence class of S.

    (b) Let n_R be the number of equivalence classes of R and let n_S be the number of equivalence classes of S. Prove that $n_R \geq n_S$.

16. On the set $U = \{1, 2, 3, 4, 5, 6\}$ define the relation

$$R \;=\; \{(i,i) \mid i \in U\} \cup \{(1,2),(2,1),(2,3),(3,2),(1,3),(3,1),(4,6),(6,4)\}.$$

Show that R is an equivalence relation. Establish what are the equivalence classes of R, in particular, how many equivalence classes R has, and how many elements each of them has.

17. We consider a linear vector space V and a (fixed) subspace W of V On V we define a relation $\sim$ by, for all $x, y \in V$:

$$x \sim y \;\Leftrightarrow\; x - y \in W \quad .$$

Prove that $\sim$ is an equivalence relation. Describe the equivalence classes for the special case that $V = \mathbb{R}^2$ W is the straight line given by the equation $x_1 + x_2 = 0$. Also characterize, for this special case, the equivalence relation in the way of Theorem 1.13.

18. An adjacency matrix for a relation R is: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Investigate whether R is (ir)reflexive, (anti)symmetric, and/or transitive.

19. Prove that $(R\,;S)^{\mathrm{T}} = S^{\mathrm{T}}\,;R^{\mathrm{T}}$.

20. (a) Prove that, for all sets A, B, C: $A \subseteq C \wedge B \subseteq C \;\Leftrightarrow\; A \cup B \subseteq C$.

(b) Prove that, for all sets A, B: $A \subseteq B \;\Leftrightarrow\; A \cup B = B$ and also: $A \subseteq B \;\Leftrightarrow\; A \cap B = A$.

(c) Prove that relation composition distributes over union, that is: $R\,;(S \cup T) \;=\; (R\,;S) \cup (R\,;T)$ and: $(R \cup S)\,;T \;=\; (R\,;T) \cup (S\,;T)$.

(d) Using the previous result(s), prove that $;$ is *monotonic*, that is: $S \subseteq T \;\Rightarrow\; R\,;S \subseteq R\,;T$ and also: $R \subseteq S \;\Rightarrow\; R\,;T \subseteq S\,;T$.

21. Prove that, indeed, $R \cup R^{\mathrm{T}}$ is the smallest solution of equation, with unknown X: $R \subseteq X \wedge X^{\mathrm{T}} \subseteq X$.

22. Prove that $R\,;\bot \;=\; \bot$, for every relation R.

23. Let R, S be relations on a set U, of which R is transitive. Prove that $R; (S; R)^+$ is transitive.

24. We consider a relation R from U to V for which it is given that it is a function. Prove that R is surjective if and only if $I_V \;=\; R^{\mathrm{T}}\,;R$.

25. Relation R, on $\mathbb{Z}$, is defined by $m\,R\,n \Leftrightarrow m{+}1 = n$, for all $m, n \in \mathbb{Z}$. What is relation R^+?

26. For some given set Ω, a function ϕ, mapping subsets of Ω to subsets of Ω, is called *monotonic* if $X \subseteq Y \Rightarrow \phi(X) \subseteq \phi(Y)$, for all $X, Y \subseteq \Omega$.

(a) We consider the equations: $X : \phi(X) \subseteq X$ and: $X : \phi(X) = X$, and we *assume* they have smallest solutions; so, proving the *existence* of these smallest solutions is not the subject of this exercise. Prove that, if ϕ is monotonic then the smallest solutions of these equations are equal.

(b) For each of the closures in Subsection 1.3.4, define a function ϕ such that the corresponding equation is equivalent to $\phi(X) \subseteq X$; for each case, prove that ϕ is monotonic. What is Ω in these cases?

27. Prove that $R^* \;=\; I \cup R^+$ and that $R^+ \;=\; R\,;R^*$.

28. Prove that for every endorelation R: "R is transitive" $\Leftrightarrow R^+ = R$.

29. We consider two endorelations R and S satisfying $R\,;S \;\subseteq\; S\,;R^+$. Prove that: $R^+\,;S \;\subseteq\; S\,;R^+$.

30. Let R, S be relations on a set U satisfying $R \subseteq S$. Prove that $R; R \subseteq S; S$.

31. Give an example of relations R, S on a set U satisfying $R; R \subseteq S; S$, but not $R \subseteq S$.

32. Let R, S be relations on a set U satisfying $R \subseteq S$. Prove that $R^+ \subseteq S^+$.

33. Let R, S be two relations on a set U, of which R is transitive and S is reflexive. Prove that

$$(R; S; R)^2 \;\subseteq\; (R; S)^3.$$

34. Let R, S be two relations on a set U.

    (a) Prove that $(R;S)^n;R \;=\; R;(S;R)^n$ for all $n \geq 0$.

    (b) Prove that $(R;S)^*;R \;=\; R;(S;R)^*$.

35. (a) Let R be an endorelation and let S be a transitive relation. Prove that:

    $$R \subseteq S \;\Rightarrow\; R^+ \subseteq S \quad .$$

    (b) Apply this, by defining suitable relations R and S, to prove that every function f on $\mathbb{N}$ satisfies:

    $$(\forall i : 0 \leq i < n : f_i = f_{i+1}) \;\Rightarrow\; f_0 = f_n \quad \text{, for all } n \in \mathbb{N} \quad .$$

36. We call a relation on a set *inductive* if it admits proofs by Mathematical Induction. Formally, a relation R on a set V is inductive if, for every predicate P on V:

    $$(\forall v : v \in V : (\forall u : u R v : P(u)) \Rightarrow P(v)) \;\Rightarrow\; (\forall v : v \in V : P(v)) \quad .$$

    Prove that, for every relation R:

    "R is inductive" $\Rightarrow$ "R^+ is inductive" .

    Hint: To prove the right-hand side of this implication one probably will introduce a predicate P. To apply the (assumed) left-hand side of the implication one may select any predicate desired, not necessarily P: use predicate Q defined by, for all $v \in V$: $Q(v) \;=\; (\forall u : u R^* v : P(u))$.

37. On the natural numbers a distinction is often made between (so-called) "weak" (or "step-by-step") induction and "strong" (or "course-of-values") induction. Weak induction is the property that, for every predicate P on $\mathbb{N}$:

    $$P(0) \wedge (\forall n :: P(n) \Rightarrow P(n{+}1)) \;\Rightarrow\; (\forall n :: P(n)) \quad ,$$

    whereas strong induction is the property that, for every predicate P on $\mathbb{N}$:

    $$(\forall n :: (\forall m : m < n : P(m)) \Rightarrow P(n)) \;\Rightarrow\; (\forall n :: P(n)) \quad ,$$

    Show that the proposition:

    "weak induction" $\Rightarrow$ "strong induction" ,

    is a special case of the proposition in the previous exercise.

38. Construct an example, as simple as possible, illustrating that relation composition is not *commutative*, which means that it is *not* true that: $R;S \;=\; S;R$, for all relations R, S.

39. Suppose that endorelation R satisfies $I \cap R^{+} = \perp$. What does this mean?

40. We investigate some well-known relations on $\mathbb{R}$:

    (a) What is the reflexive closure of $<$?

    (b) What is the symmetric closure of $<$?

    (c) What is the symmetric closure of $\leq$?

    (d) What is the reflexive closure of $\neq$?

    Compute for each of the relations in Exercise 4 their reflexive, symmetric, and transitive closures.

2 Graphs

2.1 Directed Graphs

Both in Computer Science and in the rest of Mathematics *graphs* are studied and used frequently. Graphs come in two flavors, *directed* graphs and *undirected* graphs.

There is no fundamental difference between directed graphs and relations: a directed graph just *is* an endorelation on a given set. If V −for Vertexes− is this set and if E −for Edges− is the relation we call the pair (V, E) a directed graph. Usually, set V will be finite, but this is not really necessary: infinite graphs are conceivable too. A directed graph (V, E) is finite if and only if V is finite. Unless stated otherwise, we confine our attention to finite graphs. Always set V will be *nonempty*.

Traditionally, the elements of set V are called "vertexes" or "nodes", whereas the elements of E, that is, the pairs (u, v) satisfying $u\,E\,v$, are called "directed edges" or "arrows". In this terminology we say that the graph contains "an arrow from u to v" if and only if $u\,E\,v$. Also, in this case, we say that u is a "predecessor" of v and that v is a "successor" of u.

Graphs can be represented by pictures, in the following way. Every vertex is drawn as a small circle with its name inside the circle, and every arrow from u to v is drawn as an arrow from u's circle to v's circle. Such a picture may be attractive because it enables us to comprehend, in a single glance, the whole structure of a graph, but, of course, drawing such pictures is only feasible if the set of vertexes is not too large. Figures 1 and 2 give simple examples.

41.

Figure 1: The smallest directed graphs: $V = \{ a \}$ with $E = \emptyset$ and $E = \{ (a, a) \}$

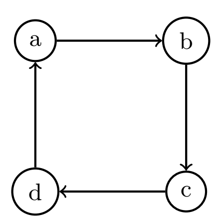


Figure 2: The graph of relation $\{ (a, b), (b, c), (c, d), (d, a) \}$

If we are only interested in the pattern of the arrows we may omit the names of the vertexes and simply draw the vertexes as dots. The resulting picture is called an "unlabeled" (picture of the) graph.

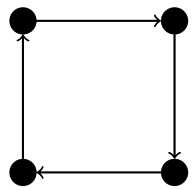


Figure 3: The same graph, unlabeled

Relation E may be such that $u\,E\,u$, for some u. In terms of graphs this means that a vertex may have an arrow from itself to itself. This is perfectly admissible, although in some applications such "auto-arrows" may be undesirable. Notice that the property "having no auto-arrows" is the directed-graph equivalent of the relational property "being irreflexive".

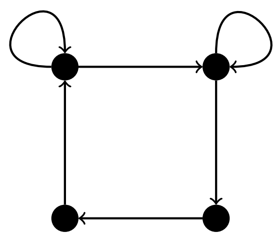


Figure 4: The unlabeled graph of relation $\{\ (a,a)\ ,\ (a,b)\ ,\ (b,b)\ ,\ (b,c)\ ,\ (c,d)\ ,\ (d,a)\ \}$

2.2 Undirected Graphs

Often we are only interested in the (symmetric) concept of nodes being connected, independent of any notion of direction. An "undirected graph" is a symmetric (endo)relation E on a set V. As before, we call the elements of V "nodes" or "vertexes". The pairs (u,v) satisfying $u\,E\,v$ are now called "edges"; we also say that such u and v are "directly connected" or "neighbors".

Relation E being symmetric means that $u\,E\,v$ is equivalent to $v\,E\,u$; hence, being neighbors is a symmetric notion: edge (u,v) is the same as edge (v,u). In this view an undirected graph just is a special case of a directed graph, with this characteristic property: the graph contains an arrow from u to v if and only if the graph contains an arrow from v to u. So, arrows occur in pairs. See Figure 5, for a simple example. A more concise rendering of an undirected graph is obtained by combining every such pair of arrows into a single, undirected edge, as in Figure 6.

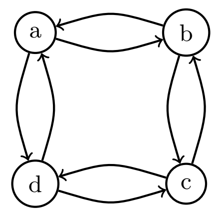


Figure 5: The graph of $\{\ (a,b)\ ,\ (b,a)\ ,\ (b,c)\ ,\ (c,b)\ ,\ (c,d)\ ,\ (d,c)\ ,\ (d,a)\ ,\ (a,d)\ \}$

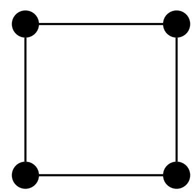


Figure 6: The same graph, with undirected edges and unlabeled

There is no fundamental reason why undirected graphs might not also contain edges connecting a node to itself. Such edges are called "auto loops". That is, if $u\,E\,u$ then u is directly connected to itself, so u is a neighbor to itself.[1] It so happens, however, that in undirected graphs auto-loops are more a nuisance than useful: many properties and theorems obtain a more pleasant form in the absence of auto-loops.

Therefore, we adopt the convention that undirected graphs contain no auto-loops. Formally, this means that an undirected graph is an *irreflexive* and symmetric relation.

In the case of finite graphs we sometimes wish to *count* the number of arrows or edges. We adopt the convention that, in an undirected graph, every pair of directly connected nodes counts as a single edge, even though this single edge corresponds to *two* arrows in the graph. This reflects the fact that, in a symmetric relation, the pairs (u,v) and (v,u) are indistinguishable. For example, according to this convention, the undirected graph in Figure 6 has four edges.

*   *   *

We have defined an undirected graph as an irreflexive and symmetric directed graph. Every directed graph can be transformed into an undirected one, just by "ignoring the directions of the arrows". In terms of relations this amounts to taking the symmetric closure of the relation and removal of the auto-arrows: in the undirected graph nodes u and v are neighbors if and only if, in the directed graph, there is an arrow from

[1] This shows that we should not let ourselves be confused by the connotations of the everyday-life word "neighbor": here the word is used in a strictly technical meaning.

u to v or from v to u (or both), provided $u \neq v$. For example, the directed graph in Figure 4 can thus be transformed into the undirected graph in Figure 6.

2.3 A more compact notation for undirected graphs

We have defined an undirected graph as an irreflexive −no edge between a node and itself− and symmetric relation. Although this is correct mathematically, it is not very practical. For example, the set of edges of the graph in Figure 5 now is $\{ (a,b), (b,a), (b,c), (c,b), (c,d), (d,c), (d,a), (a,d) \}$, in which every edge occurs *twice*: that nodes a and b, for instance, are connected is represented by the presence of both (a,b) and (b,a) in the set of edges. Yet, we do wish to consider this connection as a *single* undirected edge. It is awkward, then, to have to write down both (a,b) and (b,a) to represent this single edge. We would rather not be forced to distinguish these pairs.

We obtain a more convenient representation by using two-element[2] sets $\{u,v\}$: as set $\{u,v\}$ equals set $\{v,u\}$ we only need to write this down once. So, in the sequel, an undirected graph will be a pair (V,E), where V is the set of nodes, as usual, and where E is a set of pairs $\{u,v\}$, with $u,v \in V$ and $u \neq v$. For example, the set of edges of the graph in Figure 5 can now be written as:
$\{ \{a,b\}, \{b,c\}, \{c,d\}, \{d,a\} \}$.

In the number of edges, written as $\#E$, we do not double count the edges in two directions, so in this example we have $\#E = 4$.

Although it is usual to write $(.,.)$ for ordered pairs, in which $(a,b) \neq (b,a)$, and in sets elements have no order by which $\{a,b\} = \{b,a\}$, in the literature one often sees (a,b) to denote an edge in an undirected graph.

2.4 Additional notions and some properties

Occasionally, we use infix operators for the relations in directed and undirected graphs. That is, sometimes we write $u\,E\,v$ as $u \rightarrow v$ and we speak of directed graph $(V, \rightarrow)$ instead of (V,E). Similarly, for symmetric relations we sometimes use $u \sim v$ instead of $u\,E\,v$ and we speak of undirected graph $(V, \sim)$. So, in this nomenclature, $u \rightarrow v$ means "the graph has an arrow from u to v" and $u \sim v$ means "in the graph u and v are neighbors".

In a directed graph $(V, \rightarrow)$, for every node u the *number of* nodes v satisfying $u \rightarrow v$ is called the "out-degree" of u, whereas the number of nodes u satisfying $u \rightarrow v$ is called the "in-degree" of v, provided these numbers are *finite*. Notice that if V is finite the in-degree and out-degree of every node are finite too. An auto-arrow adds 1, both to the in-degree and the out-degree of its node.

If relation $\rightarrow$ is symmetric, so $u \rightarrow v \Leftrightarrow v \rightarrow u$ for all u, v, then the in-degree of every node equals its out-degree.

In an undirected graph $(V, \sim)$, the "degree" of a node u is its number of neighbors, that is, the number of nodes v with $u \sim v$. Thus, the degree of a node

[2] Undirected graphs contain no auto-edges, so the pair (u,u) is not an edge.

in an undirected graph equals the in-degree and the out-degree of that node in the underlying directed graph.

We write in , out , and deg for "in-degree", "out-degree", and "degree" respectively.

So for a directed graph (V,E) we have for $u,v{\in}V$:

$$\begin{aligned} in(v) &= \#\{\, u \in V \mid (u,v) \in E \,\} \\ out(u) &= \#\{\, v \in V \mid (u,v) \in E \,\}. \end{aligned}$$

By straightforward addition we obtain:

$$\textstyle\sum_{v\in V} in(v) \;=\; \#E = \;\sum_{u\in V} out(u).$$

For an undirected graph (V,E) we have

$$deg(u) \;=\; \#\{\, v \mid \{u,v\} \in E \,\}.$$

2.1 Theorem. In an undirected graph (V,E) we have

$$\sum_{v\in V} deg(v) \;=\; 2 * \#E.$$

Proof. The number of ends of edges can be counted in two ways.

In the first one one observes that every edge has two ends, and since there are $\#E$ edges, this number is $2 * \#E$.

In the second one one observes that the degree of a node is the number of ends of edges to which it is attached. Adding all these yields $\sum_{v\in V} deg(v)$, so these numbers are equal. □

* * *

With N for the size of V , so N equals the number of vertexes in the graph, we have that the degree of every node is at most $N-1$. If the degree of a node equals $N-1$ then this node is a neighbor of *all other* nodes. If every node in an undirected graph has this property, the graph is called "complete". Similarly, a directed graph is complete if it contains an arrow from every node to every node. Thus, the complete directed graph corresponds to the complete relation $\top$, whereas the complete undirected graph corresponds to the relation $\top\backslash I$ (because of the omission of auto-loops). The complete undirected graph with N nodes is called the complete N-graph. Figure 7, for example, gives a picture of the complete 5-graph.

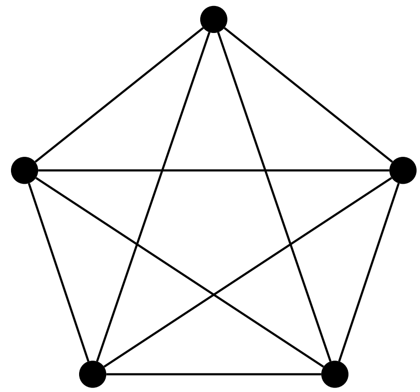


Figure 7: The complete 5-graph, unlabeled

2.5 Connectivity

2.5.1 Paths

We simultaneously consider a directed graph $(V, \rightarrow)$ and an undirected graph (with the same set of nodes) $(V, \sim)$. A *directed path from* node u to node v is a finite sequence $[\, s_0, \cdots, s_n \,]$ consisting of $n{+}1$, $0 \leq n$, nodes satisfying:

$$u = s_0 \;\wedge\; (\forall i : 0 \leq i < n : s_i \rightarrow s_{i+1}) \;\wedge\; s_n = v \quad .$$

Although this path contains $n{+}1$ nodes, it pertains to only n arrows, namely the n pairs (s_i, s_{i+1}), for all $i : 0 \leq i < n$. Therefore, we say that the *length* of this path equals n: the length of a path is the number of arrows in it. If $n = 0$ the path contains no arrows and we have $u = v$: the only paths of length 0 are the one-element sequences $[\, u \,]$ which are paths from u to u, for every node u. Paths of length 0 are called "empty" whereas paths of positive length are called "non-empty".

Similarly, in an undirected graph an *undirected path from* node u to node v is a finite sequence $[\, s_0, \cdots, s_n \,]$ consisting of $n{+}1$, $0 \leq n$, nodes satisfying:

$$u = s_0 \;\wedge\; (\forall i : 0 \leq i < n : s_i \sim s_{i+1}) \;\wedge\; s_n = v \quad .$$

Again, the length of this path is n, being the number of edges in it.

Whenever no confusion is possible, we simply use "path" instead of "directed path" or "undirected path". In any, directed or undirected graph, we call nodes u and v "connected" if the graph contains a path from u to v. Every node is connected to itself, because we have seen that for every node u a path, of length 0, exists from u to u.

In relational terms being connected means being related by the reflexive-transitive closure of the relation. In what follows, we denote the reflexive-transitive closures of relations $\rightarrow$ and $\sim$ by $\overset{*}{\rightarrow}$ and $\overset{*}{\sim}$, respectively, and we denote their transitive closures by $\overset{+}{\rightarrow}$ and $\overset{+}{\sim}$, respectively.

2.2 Lemma. In a directed graph the relation "is connected to" equals $\stackrel{*}{\rightarrow}$.

Proof. From the chapter on relations we recall the property $R^* = (\bigcup_{n:0\leq n} R^n)$; in terms of $\rightarrow$ this can be written as: $\stackrel{*}{\rightarrow} = (\bigcup_{n:0\leq n} \stackrel{n}{\rightarrow})$, where $\stackrel{n}{\rightarrow}$ denotes the equivalent of R^n . This means that $u \stackrel{*}{\rightarrow} v$ is equivalent to $(\exists n : 0 \leq n : u \stackrel{n}{\rightarrow} v)$, whereas "u is connected to v" is equivalent to
$(\exists n : 0 \leq n :$ "u is connected to v by a path of length n" $)$. We now prove the equivalence of these two characterizations term-wise; that is, for all natural n we prove that $u \stackrel{n}{\rightarrow} v$ is equivalent to "u is connected to v by a path of length n". We do so by Mathematical Induction on n :

$u \stackrel{0}{\rightarrow} v$

$\Leftrightarrow$ { definition of $\stackrel{0}{\rightarrow}$ }

$u\, I\, v$

$\Leftrightarrow$ { definition of I }

$u = v$

$\Leftrightarrow$ { definition of path }

"the path $[u]$, of length 0, connects u to v"

$\Leftrightarrow$ { definition of "connected", see below }

"u is connected to v by a path of length 0" .

As to the logical equivalence in the last step of this derivation: in the direction "$\Rightarrow$" this is just $\exists$-introduction; in the direction "$\Leftarrow$" we observe: for *every* path $[x]$, of length 0 , we have that if $[x]$ connects u to v then $x = u$, hence $[x] = [u]$. (That is, the path of length 0 connecting u to v is *unique*.)

Furthermore, we derive, for $0 \leq n$ and for nodes u, w :

$u \stackrel{n+1}{\rightarrow} w$

$\Leftrightarrow$ { definition of $\stackrel{n+1}{\rightarrow}$ }

$(\exists v :: u \stackrel{n}{\rightarrow} v \wedge v \rightarrow w)$

$\Leftrightarrow$ { Induction Hypothesis }

$(\exists v ::$ "u is connected to v by a path of length n" $\wedge\ v \rightarrow w)$

$\Leftrightarrow$ { definition of connected }

$(\exists v :: (\exists s :$ "s is a path of length n" $: u = s_0 \wedge s_n = v) \wedge v \rightarrow w)$

$\Leftrightarrow$ { $\wedge$ over $\exists$ }

$(\exists v :: (\exists s :$ "s is a path of length n" $: u = s_0 \wedge s_n = v \wedge v \rightarrow w))$

$\Leftrightarrow$ { dummy unnesting }

$(\exists s, v :$ "s is a path of length n" $: u = s_0 \wedge s_n = v \wedge v \rightarrow w)$

$\Leftrightarrow$ { if s is a path of length n then $s +\!\!+ [v, w]$ is a path of length $n{+}1$:

dummy transformation }

$(\exists t : \text{“}t \text{ is a path of length } n{+}1\text{”} : u = t_0 \wedge t_{n+1} = w\,)$

$\Leftrightarrow$ { definition of connected }

"u is connected to w by a path of length $n{+}1$" .

□

In a very similar way we can prove that the relation "is connected by a non-empty path length" is equivalent to $\stackrel{+}{\rightarrow}$. Moreover, the proof of the above lemma does not depend on particular properties of the directed relation $\rightarrow$: the lemma and its proof also are valid for undirected graphs, provided, of course, we replace $\stackrel{*}{\rightarrow}$ and $\stackrel{+}{\rightarrow}$ by $\stackrel{*}{\sim}$ and $\stackrel{+}{\sim}$ respectively.

* * *

Note that being connected in an undirected graph is a symmetric relation: u is connected to v if and only if v is connected to u, because $[\,s_0, \cdots, s_n\,]$ is a path from u to v if and only if the *reverse* of s, that is, the sequence $[\,s_n, \cdots, s_0\,]$, is a path from v to u.

In directed graphs, being connected is not necessarily symmetric, of course: the existence of a *directed path* (usually) does not imply the existence of directed path in the reverse direction.

2.5.2 Path concatenation

Let s be a directed path of length m from node u to node v, and let t be a directed path of length n from node v to node w. So, the end point of s, which is v, equals the starting point of t, that is, we have $s_m = t_0$.

From s and t we can now construct a directed path, of length $m{+}n$, from node u to node w; this is called the "concatenation" of s and t, and we denote it by $s \mathbin{+\!\!+} t$. For s and t paths of length m and n, respectively, their concatenation $s \mathbin{+\!\!+} t$ is a path of length $m{+}n$, defined as follows:

$$
\begin{aligned}
(s \mathbin{+\!\!+} t)_i &= s_i \quad , \text{for } 0 \le i \le m \\
(s \mathbin{+\!\!+} t)_{m+i} &= t_i \quad , \text{for } 0 \le i \le n
\end{aligned}
$$

Keep in mind that $s \mathbin{+\!\!+} t$ is defined *only if* $s_m = t_0$, and this is implied by this definition: on the one hand $(s \mathbin{+\!\!+} t)_m = s_m$, on the other hand $(s \mathbin{+\!\!+} t)_m = t_0$. In this case, $s \mathbin{+\!\!+} t$ is a path from u to w indeed. This we prove as follows:

$(s \mathbin{+\!\!+} t)_0$

$=$ { definition of $\mathbin{+\!\!+}$ }

s_0

$=$ { s is a path from u to v }

$$u \quad ,$$

as required; and, for $0 \leq i < m$:

$$
\begin{array}{ll}
 & (s +\!\!+ t)_i \rightarrow (s +\!\!+ t)_{i+1} \\
= & \quad \{ \text{ definition of } +\!\!+ \text{ } \} \\
 & s_i \rightarrow s_{i+1} \\
= & \quad \{ \text{ } s \text{ is a path of length } m \text{ } \} \\
 & \mathsf{true}
\end{array}
$$

as required; and, for $0 \leq i < n$:

$$
\begin{array}{ll}
 & (s +\!\!+ t)_{m+i} \rightarrow (s +\!\!+ t)_{m+i+1} \\
= & \quad \{ \text{ definition of } +\!\!+ \text{ } \} \\
 & t_i \rightarrow t_{i+1} \\
= & \quad \{ \text{ } t \text{ is a path of length } n \text{ } \} \\
 & \mathsf{true}
\end{array}
$$

as required; and, finally:

$$
\begin{array}{ll}
 & (s +\!\!+ t)_{m+n} \\
= & \quad \{ \text{ definition of } +\!\!+ \text{ } \} \\
 & t_n \\
= & \quad \{ \text{ } t \text{ is a path from } v \text{ to } w \text{ } \} \\
 & w \quad ,
\end{array}
$$

as required.

Concatenation of undirected paths is defined in exactly the same way: here concatenation is actually an operation on sequences of nodes, and the difference between $\rightarrow$ and $\sim$, that is, the difference between directed and undirected, only plays a role in the interpretation of such sequences as paths.

We now conclude that, both in directed and in undirected graphs, if a path s, say, exists from node u to node v and if a path t, say, exists from node v to node w, then also a path exists from node u to node w, namely $s +\!\!+ t$. Thus we have proved the following lemma.

2.3 Lemma. Both in directed and in undirected graphs, the relation "is connected to" is transitive.
□

2.5.3 The triangular inequality

Every path in a graph has a *length*, which is a natural number. Every non-empty set of natural numbers has a smallest element. Therefore, if node u is connected to node v we can speak of the *minimum* of the *lengths* of all paths from u to v. This we call the "distance" from u to v. Because, in undirected graphs, connectedness is symmetric, we have, in undirected graphs, that the distance from u to v is equal to the distance from v to u.

If u is *not* connected to v we define, for the sake of convenience, the distance from u to v to be ∞ ("infinity"), because ∞ can be considered, more or less, as the identity element of the minimum-operator. Note, however, that ∞ is not a natural number and that we must be very careful when attributing algebraic properties to it. For example, it is viable to define $\infty + n = \infty$, for every natural n, and even $\infty + \infty = \infty$, but $\infty - \infty$ cannot be defined in a meaningful way. An important property is:

(0) $\quad n < \infty \ \ , \ \text{for all } n \in \mathsf{Nat}$;

(1) $\quad n \leq \infty \ \ , \ \text{for all } n \in \mathsf{Nat} \cup \{\infty\}$.

We denote the distance from u to v by $dist(u,v)$. Then, function $dist$ is defined as follows, for all nodes u,v:

$$\begin{array}{lcl} dist(u,v) & = & \infty \ \ , \ \text{if } u \text{ is not connected to } v \, ; \\ dist(u,v) & = & (\mathsf{min}\, n : 0 \leq n \wedge \text{"a path of length } n \text{ exists from } u \text{ to } v\text{"} : n) \ \ , \\ & & \text{if } u \text{ is connected to } v \, . \end{array}$$

Function $dist$ now satisfies what is known in Mathematics as the "triangular inequality". This lemma holds for both directed and undirected graphs.

2.4 Lemma. All nodes u,v,w satisfy: $dist(u,w) \leq dist(u,v) + dist(v,w)$.

Proof. By (unavoidable) case analysis. If $dist(u,v) = \infty$ or $dist(v,w) = \infty$ then also $dist(u,v) + dist(v,w) = \infty$; now, by property (1), we have $dist(u,w) \leq \infty$, so we conclude, for this case: $dist(u,w) \leq dist(u,v) + dist(v,w)$, as required.

Remains the case $dist(u,v) < \infty$ and $dist(v,w) < \infty$. In this case, paths exist from u to v and from v to w. Let s be a path, of length m, from u to v and let t be a path, of length n, from v to w. Then, as we have seen in the previous subsection, $s +\!\!+ t$ is a path, of length $m+n$, from u to w. By the definition of $dist$, we conclude: $dist(u,w) \leq m+n$. As this inequality is true for *all* such paths s and t, it is true for paths of minimal length as well. Hence, also for this case we have: $dist(u,w) \leq dist(u,v) + dist(v,w)$, as required.

□

2.5.4 Connected components

A directed graph $(V, \rightarrow)$ is *strongly connected* if every node is connected to every node, that is, if there is a directed path from every node u to every node v. In relational terms, this means that $\overset{*}{\rightarrow} = \top$. The adverb "strongly" stresses the fact that, in directed graphs, strong connectedness is a symmetric notion: for every two nodes u,v there is a path from u to v *and* there is path from v to u.

An undirected graph is *connected* if every pair of nodes is connected by a path. Relationally, a graph is connected if and only if $\overset{*}{\sim} = \top$. As we have seen, in undirected graphs connectedness is symmetric. It even is an equivalence relation. A *connected component* is a *maximal subset* of the nodes of the graph that is connected: the connected components of an undirected graph are the equivalence classes of $\overset{*}{\sim}$.

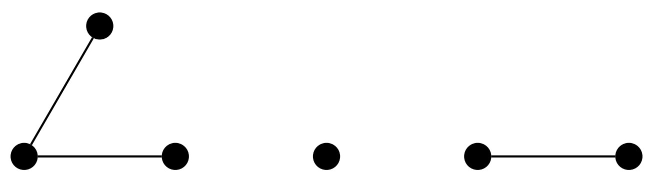


Figure 8: An undirected graph with 3 connected components

2.6 Cycles

A *cycle* in a graph is a non-trivial path from a node to itself. For undirected graphs a proper definition of 'non-trivial' needs some care. Generally, a graph may contain few cycles, many cycles, or no cycles at all. In the latter case the graph is called *acyclic*.

2.6.1 Directed cycles

In a directed graph a *cycle* is a (directed) path from a node to itself. For example, if $a \rightarrow b$ and $b \rightarrow a$ then the path $[\, a\, ,\, b\, ,\, a\,]$ is a cycle, and so is the path $[\, b\, ,\, a\, ,\, b\,]$. Although these are different paths they constitute, in a way, the same cycle. The simplest possible case of a directed cycle is $[\, a\, ,\, a\,]$, namely if $a \rightarrow a$.

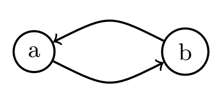


Figure 9: A simple directed cycle

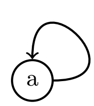


Figure 10: An even simpler cycle

2.6.2 Undirected cycles

In undirected graphs the notion of cycles is somewhat more complicated. For example, if, in undirected graph $(V, \sim)$, we have $a \sim b$ and, hence, also $b \sim a$, then $[\,a\,,\,b\,,\,a\,]$ is a path from node a to itself. Yet, we do not wish to consider this a cycle. More generally, we do not wish the pattern $[\,\cdots, a\,,\,b\,,\,a\,,\cdots\,]$ to occur anywhere in a cycle: in a cycle, every next edge should be different from its predecessor. As a consequence, in an undirected graph the smallest possible cycle involves at least *three* nodes and *three* edges. Some texts require even stronger conditions for a path to be a cycle, for instance, that no node occurs more than once. We choose for the weakest version only excluding directly going back.

These considerations give rise to the following definition.

2.5 Definition. An undirected cycle is a path $[\,s_0, \cdots, s_n\,]$, of length $n \geq 3$, for which $s_0 = s_n$ and $(\forall i : 0 \leq i \leq n{-}2 : s_i \neq s_{i+2})$ and $s_{n-1} \neq s_1$.

The first of these conditions expresses that the path's last node equals its first node – thus "closing the cycle" –, and the rest expresses that every two successive edges in the cycle are different. The conjunct $s_{n-1} \neq s_1$ really is needed here: the "last" edge, $\{\,s_{n-1}, s_n\,\}$, which is the same as $\{\,s_{n-1}, s_0\,\}$, and the "first" edge, $\{\,s_0, s_1\,\}$, are successive too, which must be different as well.

In Figure 14, for example, we have that $[\,a, b, d, b, c, a\,]$ is not a cycle, because it contains edge $\{\,b, d\}$ twice in succession. Without the conjunct $s_{n-1} \neq s_1$, however, the path $[\,d, b, c, a, b, d\,]$ would be a cycle, which is undesirable: whether or not a certain collection of nodes constitutes a cycle should not depend on which node is the first node of the path representing that cycle.

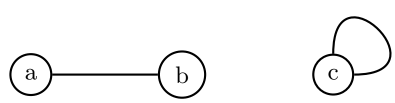


Figure 11: No cycles at all

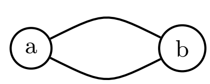


Figure 12: Not even an (undirected) graph

Thus we obtain the following lemma, which expresses that cycles are "invariant under rotation". This lemma is useful because it allows us to let any node in a cycle be the starting node of the path representing that cycle.

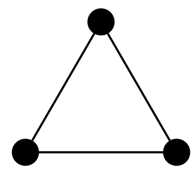


Figure 13: The smallest undirected cycle

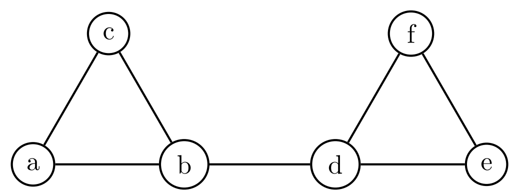


Figure 14: $[\,a, b, d, e, f, d, b, c, a\,]$ is a cycle, $[\,a, b, d, b, c, a\,]$ is not

2.6 Lemma. [Rotation Lemma] For every natural n , $3 \leq n$, a path $[\,s_0, s_1, \cdots, s_{n-1}, s_0\,]$ is a cycle if and only if the path $[\,s_1, \cdots, s_{n-1}, s_0, s_1\,]$ is a cycle.
□

In a similar way we have a lemma for reversing a cycle.

2.7 Lemma. [Reversal Lemma] For every natural n , $3 \leq n$, a path $[\,s_0, s_1, \cdots, s_{n-1}, s_0\,]$ is a cycle if and only if the path $[\,s_0, s_{n-1}, s_{n-2}, \cdots, s_1, s_0\,]$ is a cycle.
□

2.7 Euler and Hamilton cycles

2.7.1 Euler cycles

In a undirected graph a cycle with the property that it contains *every edge* of the graph exactly once is called an *Euler cycle*.

2.8 Theorem. For every connected graph $(V, \sim)$ with $\sim$ non-empty we have

$$(V, \sim) \text{ contains an Euler cycle } \Leftrightarrow (\forall v : v \in V : \mathit{deg}(v) \text{ is even}) \quad .$$

Proof. By mutual implication.

"$\Rightarrow$": We consider an Euler cycle in graph $(V, \sim)$. Let v be a node. Wherever v occurs in the Euler cycle v has a predecessor u , say, in the cycle and a successor w , say, in the cycle. This means that u, v, w are all different and $u \sim v$ and $v \sim w$. Thus, all edges associated with v occurring in the Euler cycle occur in pairs; hence, the total number of edges associated with v occurring in the Euler cycle is even.

Because the cycle is an Euler cycle *all* of v's edges occur in the Euler cycle; hence, $deg(v)$ is even.

"$\Leftarrow$": Assuming $(\forall v : v \in V : \text{“}deg(v) \text{ is even”})$ we prove the existence of an Euler cycle by sketching an algorithm for the construction of an Euler cycle. This algorithm consists of two phases. In the first phase a collection of (one or more) cycles is formed such that *every* edge of the graph occurs exactly once in exactly one of these cycles. In the second phase, the cycles in this collection are combined into larger cycles, thus reducing the number of cycles in the collection while retaining the property that *every* edge of the graph occurs exactly once in exactly one of the cycles in the collection. As soon as this collection contains only one cycle, this one cycle is a Euler cycle.

first phase: Initially all edges are white. The property $(\forall v : v \in V : \text{“}deg(v) \text{ is even”})$ will remain valid for the subgraph formed by V and the white edges only: it is an invariant of this phase. Another invariant is that all red edges form a collection of cycles with the property that *every red edge* of the graph occurs exactly once in exactly one of these cycles. Initially this is true because there are no red edges: initially the collection of red cycles is empty. If, on the other hand, all edges are red the collection of red cycles comprises all edges of the graph, and the first phase terminates. As long as the graph contains at least one white edge, the following step is executed.

Select a white edge, $\{s_0, s_1\}$, say. Because $deg(s_1)$ is even, node s_1 has a neighbor s_2, say, that differs from s_0 and such that edge $\{s_1, s_2\}$ is white as well. Repeating this indefinitely yields an infinite sequence $s_{i:0 \le i}$ of nodes, pairwise connected by white edges. As the graph is finite, this sequence contains a sub-path $[s_p, \cdots, s_q]$, for some p, q with $0 \le p < q$, that is a cycle, comprising white edges only. Now all white edges in this cycle are turned red. Because, for every node in this cycle, its associated edges occur in pairs, the number of white edges associated with any node in this cycle is even and, as a result, the degree of all nodes remains even under reddening of the white edges in this cycle. This process is repeated as long as white edges exist. Because in a undirected graph every cycle contains at least 3 edges the number of white edges thus decreases (by at least 3), this first phase will not go on forever, and will end in a situation where no white edges exist any more.

second phase: The second phase terminates if the collection of red cycles contains only one cycle. As long as this collection contains at least two cycles it takes two cycles that have a node in common. This is always possible due to the assumption that the graph is connected: if for a cycle all nodes are on none of the other cycles, this cycle is isolated and does not admit a path to any node on the other cycles, contradicting connectedness. Now these two cycles with a node v in common can be joined to a single cycle: if the one cycle is a path s from v to v and the other cycle is a path t from v to v, then the concatenation of s and t is a cycle covering both original cycles. It satisfies the cycle condition since s and t are disjoint. In this way the total number of cycles decreases, while still every edge of the original graph occurs exactly once as an edge of one of the cycles. This process is repeated until only one cycle remains and all cycles have been glued together; by construction this cycle is an Euler cycle.
$\square$

This proof of existence of an Euler cycle is constructive, and of a quite algorithmic nature. In fact, it gives rise to an algorithm to construct an Euler cycle in any connected graph in which all degrees are even, that is linear in the number of edges.

2.7.2 Hamilton cycles

In a (directed or undirected) graph a cycle with the property that it contains *every node* of the graph exactly once is called a *Hamilton cycle*.

A naive algorithm to compute whether a given graph contains a Hamilton cycle is conceptually simple: enumerate all cycles and check whether any of them is a Hamilton cycle. This naive algorithm is quite inefficient, of course, but really efficient algorithms are not (yet) known: the problem to decide whether a graph contains a Hamilton cycle is *NP-hard*, which in practice means that all algorithms will require an amount of computation time that grows exponentially with the size of the graph.

Notice the contrast in complexity between the notion of Euler and Hamilton cycles. On the one hand, Theorem 2.8 provides a simple algorithm to evaluate the existence of an Euler cycle −just calculate the degrees of the nodes−, and its proof contains a relatively straightforward algorithm for the construction of an Euler cycle. On the other hand, calculating the existence of an Hamilton cycle, let alone construction of one, is NP-hard.

Thus, two seemingly similar notions −Euler cycles and Hamilton cycles− happen to have essentially different properties.

2.7.3 A theorem on Hamilton cycles

We consider finite, undirected graphs, with at least 4 nodes. We present a theorem giving a sufficient condition for the existence of Hamilton cycles, namely if the graph contains “sufficiently many” edges. In our case the notion of “sufficiently many” and the theorem take the following shape.

2.9 Theorem. We consider an undirected graph with n nodes, $4 \leq n$. If, for every two unconnected nodes, the sum of their degrees is at least n, then the graph contains a Hamilton cycle.

□

To formalize this, let V be a (fixed) set of nodes, with $n = \#V$, $4 \leq n$. In what follows variables u, v, p, q range over V, with $p \neq q$. The set E of edges is variable; that is, as a function of E we define predicates P and H, as follows:

$$P(E) \;=\; (\forall u, v : u \neq v : \; \{u, v\} \notin E \;\Rightarrow\; deg(u) + deg(v) \geq n \;) \quad \text{, and:}$$

$$H(E) \;=\; \text{“graph } (V, E) \text{ contains a Hamilton cycle”} \quad .$$

Predicate P formalizes our particular version of “sufficiently many”: P expresses that, for every two unconnected nodes, the sum of their degrees is at least n.

Both P and H are *monotonic*, as follows:

monotonicity: For all E and for any two nodes p, q:

$$P(E) \;\Rightarrow\; P(E \cup \{\{p,q\}\}) \quad \text{, and:}$$

$$H(E) \;\Rightarrow\; H(E \cup \{\{p,q\}\}) \quad .$$

□

In addition, for the extreme cases, the empty graph $\perp$ and the complete graph $\top$, we have:

$$\neg(P(\perp)) \;\wedge\; \neg(H(\perp)) \;\wedge\; P(\top) \;\wedge\; H(\top) \quad .$$

The theorem now states that every graph satisfying predicate P contains at least one Hamilton cycle.

2.10 Theorem. $(\forall E :: P(E) \Rightarrow H(E))$.

□

We present two proofs for this theorem. These proofs are essentially the same, but they differ in their formulation. The crucial part in both proofs is the following:

Core Property: For set E of edges and for any two nodes p, q with $\neg(\{p,q\} \in E)$:

$$P(E) \wedge H(E \cup \{\{p,q\}\}) \;\Rightarrow\; H(E) \quad .$$

□

Notice that the Core Property also holds if $\{p,q\} \in E$, but in a trivial way only: then $H(E \cup \{\{p,q\}\}) = H(E)$, so in this case the property is void.

We will present a proof for the Core Property later, but first we will show how it is used in the proofs of the Theorem.

2.7.4 A proof by contradiction

The first proof runs as follows, by contradiction. That is, we suppose that the Theorem is false. Then, there exists a set F of edges such that $P(F)$ and $\neg(H(F))$. Because $\neg(H(F))$ and $H(\top)$, and because $F \subseteq \top$, there also exists a "turning point", that is, a set E of edges and a pair p, q of nodes such that:

$$F \subseteq E \;\wedge\; \neg(H(E)) \;\wedge\; H(E \cup \{\{p,q\}\}) \quad .$$

Notice that, because of $\neg(H(E)) \wedge H(E \cup \{\{p,q\}\})$, we have –Leibniz!– that $E \neq E \cup \{\{p,q\}\}$, hence $\{p,q\} \notin E$.

Because of the monotonicity of P, and because $P(F)$ and $F \subseteq E$, set E satisfies $P(E)$ too. Now, from $P(E)$ and $H(E \cup \{\{p,q\}\})$ we conclude, using the Core Property, $H(E)$. In conjunction with the assumed $\neg(H(E))$ we obtain the desired contradiction.

2.7.5 A more explicit proof

The reasoning in the previous proof is somewhat strange: the assumption $\neg(H(E))$ is not really used in the proof proper: it is only used to conclude a contradiction. Therefore, we should be able to construct a more direct proof. In addition what does "there exists a 'turning point'" really mean, mathematically speaking?

Because of the monotonicity of P we have $P(E) \Rightarrow P(E \cup \{\{p,q\}\})$; therefore, by means of elementary propositional calculus, the Core Property can be rewritten thus:

(2) $$(P(E \cup \{\{p,q\}\}) \Rightarrow H(E \cup \{\{p,q\}\})) \;\Rightarrow\; (P(E) \Rightarrow H(E)) \quad ,$$

and this smells very strongly of a proof by Mathematical Induction. As a matter of fact, this *is* Mathematical Induction, albeit in a somewhat unusual direction, namely from larger towards smaller.

Firstly, we have $H(\top)$ −the complete graph contains a Hamilton cycle, very many even−, so we also have $P(\top) \Rightarrow H(\top)$. This is the basis of the induction.

Secondly, property (2) now represents the induction step. Because every set E of edges can be obtained from a larger set $E \cup \{\{p,q\}\}$, with $\{p,q\} \notin E$, we are done.

Notice that the fact that the collection of all possibles sets of edges is *finite*[3] is of no consequence: although usually applied to infinite sets the principle of Mathematical Induction is perfectly valid in a finite setting.

2.7.6 Proof of the Core Property

We repeat the Core Property, which is the essential part of both proofs of the Theorem.

Core Property: For set E of edges and for any two nodes p,q with $\{p,q\} \notin E$:

$$P(E) \wedge H(E \cup \{\{p,q\}\}) \;\Rightarrow\; H(E) \quad .$$

□

To prove this we assume that E is a set of edges and p,q are different nodes, such that $\{p,q\} \notin E$, satisfying $P(E)$ and $H(E \cup \{\{p,q\}\})$. The latter means that the graph $(V, E \cup \{\{p,q\}\})$ contains a Hamilton cycle. If such a Hamilton cycle does *not* contain edge $\{p,q\}$, then it also is a Hamilton cycle in the graph (V,E) ; hence, $H(E)$ and in this case we are done.

So, remains the case that $(V, E \cup \{\{p,q\}\})$ contains a Hamilton cycle that does contain edge $\{p,q\}$. Now we have to prove $H(E)$, that is, we must prove that (V,E) contains a Hamilton cycle as well, that is, *without* edge $\{p,q\}$.

For this purpose, let $[\, s_0, s_1, \cdots, s_n \,]$ be a Hamilton cycle in $(V, E \cup \{\{p,q\}\})$. This means that $\{ s_i \mid 0 \le i < n \} = V$ −recall that $n = \# V$ −, that $s_n = s_0$, and that $(\forall i : 0 \le i < n : \{ s_i, s_{i+1} \} \in E \cup \{\{p,q\}\})$. We assume that this cycle contains edge $\{p,q\}$ and, without loss of generality, we assume that $s_0 = p$ and $s_1 = q$.

[3]for our *fixed*, finite set of nodes

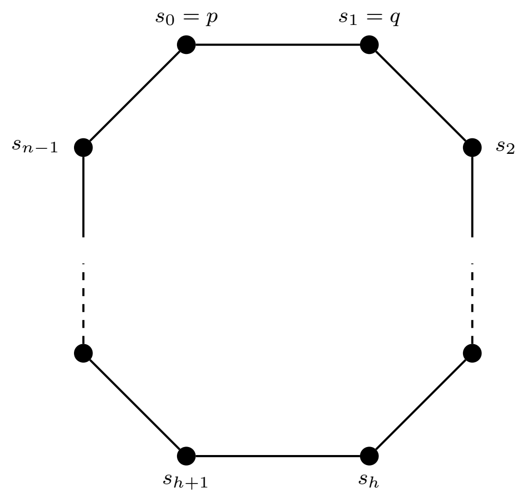


Figure 15: a Hamilton cycle, with edge $\{p, q\}$

In this setting we prove that (V, E) contains a Hamilton cycle. To construct a Hamilton cycle *not* containing edge $\{p, q\}$ we take the Hamilton cycle introduced above, containing edge $\{p, q\}$, as a starting point. Removal of edge $\{p, q\}$ destroys the cycle, and what remains is a path connecting s_1, that is q, to s_0, that is p, that still contains all nodes of the graph and all edges of which are in E.
Now we must restore the cycle by somehow reconnecting p and q, using edges in E only. We do so by selecting an index h in the interval $[2..n{-}1)$ such that both $\{p, s_h\} \in E$ and $\{q, s_{h+1}\} \in E$. To show that this is possible we need the theorem's assumption $P(E)$, which was defined as:

$$(\forall u, v : u \neq v : \ \{u, v\} \notin E \ \Rightarrow \ deg(u) + deg(v) \geq n \ ) \quad .$$

Applying this to p, q and using $\{p, q\} \notin E$ we obtain:

(3) $\qquad deg(p) + deg(q) \geq n \quad .$

Let $x = \#\{i \in [2..n{-}1) \mid \{p, s_i\} \in E\}$ and let $y = \#\{j \in [2..n{-}1) \mid \{q, s_{j+1}\} \in E\}$; now we calculate:

$$
\begin{array}{ll}
 & deg(p) + deg(q) \ \geq \ n \\
\Leftrightarrow & \qquad \{ \text{ definition of } deg \text{ (twice), using } s_0 = p \text{ and } s_1 = q \ \} \\
 & \#\{i \in [1..n) \mid \{s_0, s_i\} \in E\} + \#\{j \in [2, n] \mid \{s_1, s_j\} \in E\} \ \geq \ n \\
\Leftrightarrow & \qquad \{ \text{ split off } i = 1 \text{ and } i = n{-}1 \text{, using } \{s_0, s_1\} \notin E \text{ and } \{s_{n-1}, s_n\} \in E \ \} \\
 & 1 + \#\{i \in [2..n{-}1) \mid \{s_0, s_i\} \in E\} + \#\{j \in [2, n] \mid \{s_1, s_j\} \in E\} \ \geq \ n \\
\Leftrightarrow & \qquad \{ \text{ split off } j = 2 \text{ and } j = n \text{, using } \{s_1, s_2\} \in E \text{ and } \{s_1, s_n\} \notin E \ \}
\end{array}
$$

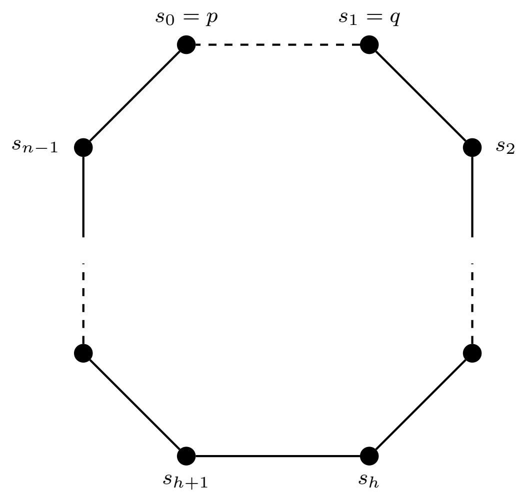


Figure 16: The remains of the cycle, after removal of edge $\{p,q\}$

$$
\begin{array}{ll}
 & 1 + \#\{ i\in[2..n{-}1) \mid \{s_0,s_i\}\in E\} + 1 + \#\{ j\in[3..n) \mid \{s_1,s_j\}\in E\} \ \geq \ n \\
\Leftrightarrow & \quad \{ \text{ dummy transformation } j:=j{+}1 \ \} \\
 & 1 + \#\{ i\in[2..n{-}1) \mid \{s_0,s_i\}\in E\} + 1 + \#\{ j\in[2..n{-}1) \mid \{s_1,s_{j+1}\}\in E\} \ \geq \ n \\
\Leftrightarrow & \quad \{ \text{ definitions of } x \text{ and } y \text{, using } s_0=p \text{ and } s_1=q \ \} \\
 & 1+x+1+y \geq n \\
\Leftrightarrow & \quad \{ \text{ calculus } \} \\
 & x+y \geq n-2 \quad .
\end{array}
$$

So, the number of indexes i in the interval $[2..n{-}1)$ for which $\{p,s_i\}\in E$ plus the number of indexes i in the range $[2..n{-}1)$ for which $\{q,s_{i+1}\}\in E$ is at least $n-2$. The size of the interval $[2..n{-}1)$, however, only is $n-3$; hence the two sets of indexes have a non-empty intersection: there exists an index h, $h\in[2..n{-}1)$, such that both $\{p,s_h\}\in E$ and $\{q,s_{h+1}\}\in E$.

For every such an index h, $[\,s_0,s_h,\cdots,s_2,s_1,s_{h+1},\cdots,s_{n-1},s_n\,]$ is a Hamilton cycle in the graph (V,E). Because we have shown the existence of such an h, we conclude the existence of a Hamilton cycle in (V,E), which was our goal.

remark: The existence of an index h in the interval $[2..n{-}1)$ implies that this interval is nonempty, that is, $2<n-1$, which boils down to $4\leq n$. Hence, the proofs of the Theorem presented here are only valid for graphs with at least 4 nodes. It can be easily verified that the Theorem also holds for $n=3$: the complete 3-graph − a "triangle" − is the only one satisfying predicate P, and a "triangle" is a Hamilton cycle. For $n<3$ the Theorem does not hold.

□

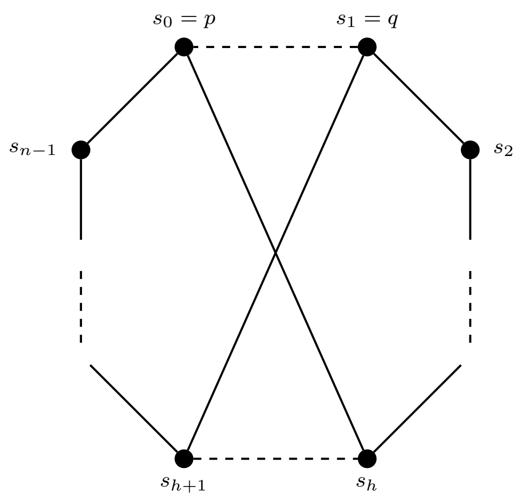


Figure 17: a Hamilton cycle, without edge $\{p, q\}$

2.8 Ramsey's theorem

2.8.1 Introduction

We are having a party at which every two guests either do know each other or do not know each other. If the number of guests at the party is "large enough" then the party has at least 5 guests all of which either do know one another or do not know one another. How large must the party be for this to be true?

F.P. Ramsey has developed some theory for the treatment of problems like this. This theory makes it possible to draw rather global conclusions about undirected graphs, independently of their actual structure.

To illustrate this we present a simple theorem that represents his work. In the above example the guests at the party can be considered the nodes of an undirected graph. Any two nodes are connected by an edge if and only if the two corresponding guests do know each other. A set of 5 guests all of which do know one another then amounts to a subgraph of size 5 that is *complete*, that is, we say that the whole graph *contains a complete* 5-*graph*. How do we formulate, on the other hand, that from a set of 5 guests every two guests do *not* know each other? Well, this means that the whole graph contains 5 nodes every two of which are *not* connected.

We might as well, however, consider the *complement* graph, in which two nodes are connected by an edge if and only if the two corresponding guests do *not* know each other. As a matter of fact, the problem as stated is *symmetric* in the notions of "knowing each other" and "not knowing each other". It is, therefore, awkward to destroy this symmetry by representing the one concept by the presence of edges and the other concept by their absence. Moreover, we have two possibilities here, the choice between which is irrelevant.

To restore the symmetry we, therefore, consider a complete undirected graph, of which the set of edges has been partitioned into two subsets – or more than two, in the more general case of Ramsey's theory – . The one subset then represents the pairs of guests who know each other and the other subset represents the pairs of guests who do not know each other.

Partitioning a set into (disjoint) subsets can be represented conveniently by *coloring*. In our case, partitioning the edges of a complete graph into two subsets can be represented by coloring each edge with one out of two colors. (And, of course, with more than two colors we can represent partitionings into more than two subsets.) Now, an edge of the one color may represent a pair of guests who do know each other, whereas an edge of the other color may represent a pair of guests who do not know each other. Thus, the symmetry between "knowing" and "not knowing" is restored.

2.8.2 Ramsey's theorem

We consider finite, complete, undirected graphs only. For the sake of brevity, we will use "k-graph" for the "complete k-graph", for any natural k, $2 \le k$. Formally, a coloring of a graph's edges is a function from the set of edges to the set of colors used, $\{\mathsf{red}, \mathsf{blue}\}$, say, if two colors are sufficient. So, a coloring is a function of type $E \rightarrow \{\mathsf{red}, \mathsf{blue}\}$, and if c is such a coloring, then for any edge $\{u, v\}$ we have either $c(\{u,v\}) = \mathsf{red}$ or $c(\{u,v\}) = \mathsf{blue}$, but not both simultaneously, as we presume that $\mathsf{red} \ne \mathsf{blue}$: every edge has only one color. In what follows we use variables c and d to denote colorings.

Again for brevity's sake, we say that the k-graph "contains a red m-graph" if the nodes of the k-graph contain a subset of m nodes such that all edges connecting these nodes are red; that is, these m nodes together with their edges constitute a completely red m-graph as a subgraph of the k-graph, for any k, m with $2 \le m \le k$.

As an example, notice that the 2-graph has two nodes only, connected by one single edge; hence, the proposition "the k-graph contains a red 2-graph" is equivalent to the proposition "the k-graph contains at least one red edge".

The proposition "the k-graph contains a red m-graph" depends on the parameters k and m, of course, but also on the actual coloring. So, it is a predicate with three parameters. Calling this predicate Rd, we define it as follows, together with a similar predicate Bl, for the color blue, for all k, c, m with $2 \le m \le k$:

$$Rd(k,c,m) \;\Leftrightarrow\; \text{"the } k\text{-graph with coloring } c \text{ contains a red } m\text{-graph"} \text{ , and:}$$

$$Bl(k,c,m) \;\Leftrightarrow\; \text{"the } k\text{-graph with coloring } c \text{ contains a blue } m\text{-graph"} \text{ .}$$

These predicates are monotonic, in the following way. Suppose $Rd(k,c,m)$, for some k, c, m. Then we also have $Rd(k{+}1, c, m)$, provided we consider the coloring of the

$(k+1)$-graph as an extension of the coloring of the k-graph $-$both colorings being denoted here by the very same $c-$, just as the $(k+1)$-graph can be viewed as an extension of the k-graph. For this purpose we consider the $k+1$ nodes of the $(k+1)$-graph as a set of k nodes, forming a k-graph, plus one additional node, which may remain anonymous. Every coloring of the $(k+1)$-graph thus induces a coloring of the k-graph; as stated, function c denotes either coloring.

Ramsey's theorem now is about a function R, say, defined as follows, for all m, n with $2 \leq m$ and $2 \leq m$:

$$\begin{array}{rcl} R(m,n) & = & \text{“the smallest of all natural numbers } k \text{ satisfying:} \\ & & (\forall c :: Rd(k,c,m) \ \vee \ Bl(k,c,n)\,)\text{ ”} \quad . \end{array}$$

The function value $R(m,n)$ is only well-defined, of course, if at least one natural number k exists satisfying $(\forall c :: Rd(k,c,m) \ \vee \ Bl(k,c,n)\,)$: only then we can speak of the smallest such number. Notice that, by definition, if $R(m,n) = p$ then for every k, $p \leq k$, the k-graph contains at least one red m-graph or contains at least one blue n-graph (or both).

The following theorem states that such natural numbers exist and provides an upper bound for $R(m,n)$.

2.11 Theorem. (Ramsey)

$$R(m,n) \ \leq \ \binom{m+n-2}{m-1} \quad \text{, for all } m,n : 2 \leq m \wedge 2 \leq n \quad .$$

□

Notice that, by definition, $R(m,n)$ is symmetric in m and n, that is, we have: $R(m,n) = R(n,m)$, because for every coloring c satisfying $Rd(k,c,m) \ \vee \ Bl(k,c,n)$ a coloring d exists $-$which one?$-$ satisfying $Rd(k,d,n) \ \vee \ Bl(k,d,m)$. The expression $\binom{m+n-2}{m-1}$ does not look symmetric, at least, not at first sight. Yet, it is, because binomial coefficients satisfy the following, general property:

$$\binom{m+n}{m} = \binom{m+n}{n} \quad \text{, for all } m,n : 1 \leq m \wedge 1 \leq n \quad ,$$

as a result of which we also have: $\binom{m+n-2}{m-1} = \binom{m+n-2}{n-1}$.

Proof of the Theorem: By Mathematical Induction on the value of $m+n$; that is, the Induction Hypothesis is:

$$R(p,q) \ \leq \ \binom{p+q-2}{p-1} \quad \text{, for all } p,q : 2 \leq p \wedge 2 \leq q \wedge p+q < m+n \quad .$$

We distinguish 3 cases.

Firstly, $2 \leq m \wedge n = 2$: We consider the m-graph. Let c be the coloring in which all edges of the m-graph are red, so this particular c yields $Rd(m,c,m)$. For every *other* coloring c we have that not all edges of the m-graph are red, so the m-graph contains at least one blue edge, which means $Bl(m,c,2)$, for all other c. Combining these cases we obtain $(\forall c :: Rd(m,c,m) \vee Bl(m,c,2))$, from which we conclude that $R(m,n) \leq m$. (Actually, we have $R(m,n) = m$ because no smaller graph contains a red m-graph, but the upper bound is all we need.) Now $m = \binom{m+2-2}{m-1}$, so we conclude $R(m,n) \leq \binom{m+2-2}{m-1}$, as required.

Secondly, $m = 2 \wedge 2 \leq n$: By symmetry with the previous case.

Thirdly, $3 \leq m \wedge 3 \leq n$: We need an additional property, to be proved later; the need of this property is inspired by a well-known property of binomial coefficients:

$$
\begin{array}{ll}
 & R(m,n) \\
\leq & \quad \{ \bullet \text{ property of } R\text{, see below, using } 3 \leq m \wedge 3 \leq n \} \\
 & R(m{-}1\,,n) + R(m\,,n{-}1) \\
\leq & \quad \{ \text{ Induction Hypothesis (twice) } \} \\
 & \binom{m+n-3}{m-2} + \binom{m+n-3}{m-1} \\
= & \quad \{ \text{ property of binomial coefficients } \} \\
 & \binom{m+n-2}{m-1} \quad .
\end{array}
$$

□

In the above proof of the Theorem we have used the following property of R, which constitutes the core of the proof.

property: $R(m,n) \ \leq \ R(m{-}1\,,n) + R(m\,,n{-}1)$, for all $m,n : 3 \leq m \wedge 3 \leq n$.

proof: Let $k \ = \ R(m{-}1\,,n) + R(m\,,n{-}1)$. To prove that $R(m,n) \leq k$ it suffices to prove $Rd(k,c,m) \vee Bl(k,c,n)$, for all colorings c. Therefore, let c be a coloring of the k-graph. Let v be a node of the k-graph and in what follows dummy u also ranges over the nodes of the k-graph. We define subsets X and Y of the nodes, as follows:

$$
\begin{array}{lll}
X & = & \{ u \in V \mid u \neq v \wedge c(\{u,v\}) = \mathsf{red} \} \quad \text{, and:} \\
Y & = & \{ u \in V \mid u \neq v \wedge c(\{u,v\}) = \mathsf{blue} \} \quad .
\end{array}
$$

Then X and Y and $\{v\}$ partition the nodes of the k-graph, so we have:

$$\#X + \#Y + 1 \;=\; R(m{-}1\,,n) + R(m\,,n{-}1) \quad .$$

From this it can be derived that $R(m{-}1\,,n) \le \#X \;\vee\; R(m\,,n{-}1) \le \#Y$, by contraposition:

$$\begin{array}{ll}
 & \#X < R(m{-}1\,,n) \;\;\wedge\;\; \#Y < R(m\,,n{-}1) \\
\Leftrightarrow & \quad \{ \text{ all values here are integers } \} \\
 & \#X \le R(m{-}1\,,n) - 1 \;\;\wedge\;\; \#Y \le R(m\,,n{-}1) - 1 \\
\Rightarrow & \quad \{ \text{ monotonicity of addition } \} \\
 & \#X + \#Y \;\le\; R(m{-}1\,,n) + R(m\,,n{-}1) - 2 \\
\Leftrightarrow & \quad \{ \text{ all values here are integers } \} \\
 & \#X + \#Y + 1 \;<\; R(m{-}1\,,n) + R(m\,,n{-}1) \\
\Rightarrow & \quad \{ \; < \text{ is irreflexive } \} \\
 & \#X + \#Y + 1 \;\ne\; R(m{-}1\,,n) + R(m\,,n{-}1) \quad ,
\end{array}$$

which settles the issue.

We now prove the required property, $Rd(k,c,m) \vee Bl(k,c,n)$, by distinguishing the two cases of this disjunction.

Case $R(m{-}1\,,n) \le \#X$: From the definition of R we conclude, for our coloring c, that either $Rd(\#X,c\,,m{-}1)$ or $Bl(\#X,c\,,n)$. If $Rd(\#X,c\,,m{-}1)$ then X contains a red $(m{-}1)$-graph. By definition of X, we also have $c(\{u,v\}) = \mathsf{red}$, for all $u \in X$; hence, $X \cup \{v\}$ contains a red m-graph, which implies $Rd(k,c,m)$ as well. If, on the other hand, $Bl(\#X,c\,,n)$ then we also have $Bl(k,c,n)$. In both cases we have $Rd(k,c,m) \vee Bl(k,c,n)$, which concludes this case.

Case $R(m\,,n{-}1) \le \#Y$: By symmetry.

□

2.8.3 A few applications

A party containing 5 guests all knowing one another or all not knowing one another can now represented as a complete graph containing a red 5-graph or a blue 5-graph. So, asking for the smallest such party is asking for the value of $R(5,5)$. As upper bound for $R(5,5)$, Ramsey's theorem now gives $\binom{8}{4}$, which equals 70. Further investigation of this problem has revealed that $R(5,5) \in [\,43\,,\,49\,]$; what is the actual value of R(5,5) still is an open problem!

*   *   *

The smallest complete graph containing, independently of the coloring, at least one *monochrome* triangle is the complete 6-graph. Ramsey's theorem yields $R(3,3) \le 6$. For the complete 5-graph a coloring exists such that the graph does *not* contain a monochrome triangle; hence, $R(3,3) \ge 6$. So, $R(3,3) = 6$.

2.9 Trees

2.9.1 Undirected trees

An *(undirected) tree* is an undirected graph that is connected and acyclic. As we will see, on the one hand trees are the *smallest* connected graphs: removal of an edge from a tree always results in a graph that is not connected anymore. On the other hand, trees are the *largest* acyclic graphs: adding an additional edge to a tree results in a graph containing at least one cycle.

Although trees may be infinite, usually only finite trees are considered. Without further notice we confine our attention to finite trees.

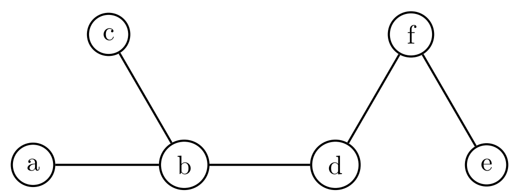


Figure 18: A (labeled) tree

In a connected graph, a *leaf* is a node with exactly one neighbor, that is, a node of degree 1. In Figure 18, for example, the leaves are a, c, e.

2.12 Lemma. Removal of a leaf and its (unique) associated edge from a connected graph yields a connected graph.

Proof. Let v be a leaf in a graph, and let u, w be nodes different from v. Then, no path connecting u and w contains v. Hence, every such path still exists in the graph resulting from removal of v and its associated edge.
□

2.13 Lemma. Every finite, acyclic graph with at least one edge contains at least one leaf.

Proof. Assume not, then every node has degree 0 or ≥ 2.

We construct an infinite sequence $s_{i:0\le i}$ of nodes, as follows. Choose $s_0 \in V$ and $s_1 \in V$ such that $\{s_0, s_1\}$ is an edge. Next, for all $i, 0 \le i$, we choose $s_{i+2} \in V$ such that $s_{i+1} \sim s_{i+2}$ and $s_i \ne s_{i+2}$. This is possible because $deg(s_{i+1}) \ge 2$, since s_{i+1} is part of an edge, so does not have degree 0.

Thus, we have defined an infinite path s, starting at s_0 and with the property that $s_i \ne s_{i+2}$, for all $i, 0 \le i$. The set V of nodes, however, is finite. Therefore[4],

[4] See the discussion on finite and infinite, in the chapter on functions.

we have $s_p = s_q$, for some p, q with $0 \le p < q$. Hence, the sub-path $[\, s_p, \cdots, s_q \,]$ is a cycle connecting s_p to itself. This contradicts the assumption of the graph being acyclic, concluding the proof.
□

A direct corollary of this lemma is that every tree with at least two nodes contains at least one leaf.

2.14 Theorem. A tree with n, $1 \le n$, nodes contains $n-1$ edges.

Proof. By Mathematical Induction on n. A tree with 1 node has 0 edges −after all, every edge connects two *different* nodes−, and $1-1=0$. Now let $(V, \sim)$ be a tree with $\#V = n+1$, where $1 \le n$. By (the corollary to) the previous lemma this tree has a leaf u, say, so $deg(u) = 1$. Hence, there is exactly one node v, say, with $u \sim v$, so the one-and-only edge involving u is $\{u, v\}$. Now let $(W, \approx)$ be the graph obtained from $(V, \sim)$ by removal of leaf u and its edge $\{u, v\}$. This means that $W = V \backslash \{u\}$ and that $w \approx x \Leftrightarrow w \sim x$, for all $w, x \in W$.

Because $v \in V$ we have $\#W = \#V - 1$, so $\#W = n$. The graph $(W, \approx)$ is a tree because removal of node u and its edge $\{u, v\}$ maintains connectedness of the remaining graph and, obviously, introduces no cycles. By Induction Hypothesis, tree $(W, \approx)$ contains $n-1$ edges, hence the original tree $(V, \sim)$ contains n edges.
□

Actually, (finite) trees can be characterized in many different ways. This is illustrated by the following theorem, of which the above theorem is a special case, but for which we do not give the proof.

2.15 Theorem. For a connected, undirected graph (V, E) the following propositions are equivalent.

(a) (V, E) is acyclic.

(b) For every $e \in E$ the graph $(V, E \backslash \{e\})$ is not connected.

(c) $\#E = \#V - 1$.

(d) For all nodes u, v a *unique* path exists connecting u to v on which every node occurs at most once.

□

2.10 Exercises

1. How many edges does the complete undirected n-graph have, for all $n \ge 1$? Prove the correctness of your answer.

2. An undirected graph (V, E) is called “regular of degree d”, for some natural number d, if $deg(v) = d$, for all $v \in V$. Prove that such a graph satisfies $d * \#V = 2 * \#E$.

3. For an undirected graph in which every node has degree 3, show that the total number of nodes is always even.

4. Let (V,E) be an undirected graph satisfying $\#V = 9$ and $\#E \geq 14$. Prove that V contains at least one node the degree of which is at least 4.

5. Given are two connected (undirected) graphs (V,E) and (W,F), such that $V \cap W = \emptyset$. Let $v \in V$ and $w \in W$. Prove that the graph $(V \cup W\,,\; E \cup F \cup \{\{v,w\}\})$ is connected.

6. Let (V,E) be a connected undirected graph, in which $V = \{v_1, v_2, \ldots, v_n\}$. Let $W = \{w_1, w_2, \ldots, w_n\}$. Prove that the undirected graph $(V \cup W, E')$ for E' defined by

   $$E' = E \cup \{(v_i, w_i) \mid i = 1, 2, \ldots, n\}$$

   is connected.

7. Let $(V, \sim)$ be a connected undirected graph such that $v, w \in V$ with the following properties: *deg(v)* and *deg(w)* are odd and *deg(u)* is even for all *other* nodes $u \in V$. Prove that the graph contains an Euler-path connecting v and w, that is, a path containing every edge of the graph exactly once.

8. For two connected undirected graphs (V_1, E_1) and (V_2, E_2) it is given that $V_1 \cap V_2 \neq \emptyset$. Prove that $(V_1 \cup V_2, E_1 \cup E_2)$ is connected.

9. Give an undirected graph having a cycle of length 3 and a cycle of length 4, but not a cycle of length 5.

10. For an undirected graph (V,E) every two non-empty subsets V_1 and V_2 of V satisfy:

    $$(V_1 \cup V_2 = V) \Rightarrow (\exists v_1, v_2 : v_1 \in V_1 \wedge v_2 \in V_2 \wedge (v_1, v_2) \in E).$$

    Prove that (V,E) is connected.

    (Hint: for a node v consider $V_1 = \{u \in V \mid$ there is a path from v to $u\}$.)

11. Let (V,E) be an acyclic undirected graph with two distinct nodes $v_1, v_2 \in V$ such that for every node $u \in V$ there is either a path from u to v_1 or a path from u to v_2, but not both. Prove that $\#E = \#V - 2$.

12. A *chain* in a directed graph $(V, \rightarrow)$ is an infinite sequence $s_{i\,:\,0 \leq i}$ of nodes – that is, a function of type $\mathbb{N} \rightarrow V$ – with the property $(\forall i : 0 \leq i : s_i \rightarrow s_{i+1})$.

    (a) Prove that finite and acyclic directed graphs do not contain chains.

    (b) As a consequence, prove that every finite and acyclic directed graph contains at least one node the out-degree of which is zero.

13. We consider a (finite) undirected graph in which the degree of every node is at least 3. Prove that this graph contains a cycle containing at least 4 nodes.

    (Hint: construct v_i for $i = 0, 1, 2, 3, \ldots$ such that $v_{i-1} \rightarrow v_i$ and $v_i \neq v_{i-1}$ for $i > 0$ and $v_i \neq v_{i-2}$ for $i > 1$)

14. Let (V, E) be a finite connected undirected graph. Let W be a finite set and $f : V \rightarrow W$ a bijective function. Prove that the undirected graph

    $$(V \cup W, E \cup \{(v, f(v)) \mid v \in V\})$$

    is connected.

15. An undirected graph contains two cycles of lengths n, m, respectively, that have exactly one edge in common. Prove that the graph also has a cycle of length $n + m - 2$.

16. We consider an (finite) undirected graph with n nodes, for $n \geq 3$. The degree of every node in this graph is at least 1 and the graph contains a node of degree $n - 2$. Prove that this graph is connected.

17. We consider two undirected trees (V, E) and (W, F), with $V \cap W = \emptyset$. Let $v_0, v_1 \in V$ and $w_0, w_1 \in W$. Prove that the graph $(V \cup W\ ,\ E \cup F \cup \{\{v_0\,, w_0\}, \{v_1, w_1\}\})$ contains a cycle.

18. Let (V, E) be an undirected tree, and $v \in V$. Choose $v' \notin V$ and define $V' = V \cup \{v'\}$ and $E' = E \cup \{\{v, v'\}\}$. Prove that (V', E') is a tree.

$*$19. We consider the complete 6-graph in which every edge has been co loured either red or blue. Prove that, independent of the chosen coloring, this graph contains at least 2 *monochrome* triangles.

20. Prove that an undirected graph with n nodes and in which the number of edges is greater than $n^2/4$ contains at least one triangle.

21. Give an example of an undirected graph containing an Euler cycle, but not containing a Hamilton cycle.

22. Give an example of an undirected graph, with at least 4 nodes, and containing a cycle that is both an Euler cycle and a Hamilton cycle.

23. Give an example of an undirected graph containing an Euler cycle and a Hamilton cycle that are different.

24. For $i = 1, 2$ let (V_i, E_i) be a finite undirected graph for which $(v_i, v_i') \in E_i$ is an edge on a Hamilton cycle of (V_i, E_i). Assume $V_1 \cap V_2 = \emptyset$. Prove that the graph

    $$(V_1 \cup V_2, E_1 \cup E_2 \cup \{(v_1, v_2), (v_1', v_2')\})$$

    admits a Hamilton cycle.

25. Give an example of a Hamilton cycle in an undirected graph in which every node has degree 3.

26. Among any group of 21 people, show that there are four people of which either every two of them once played chess together or every two of them never played chess together. (Hint: use Ramsey theory.)

27. Give an example of a connected, undirected graph with 6 nodes, in which the degree of every node equals 3. Also give an example of such a graph in which the degree of every node equals 4.

28. Give an example of an undirected graph with 7 nodes, in which the degree of every node equals 2, and consisting of exactly 2 connected components.

29. Prove that every undirected graph, with 5 nodes and in which the degree of every node equals 2, is connected.

30. Prove that every acyclic, undirected graph, with n nodes and $n-1$ edges, is connected.

31. Prove that every undirected graph, with n nodes and at least $(n^2-3*n+4)/2$ edges, is connected.

$*$32. Prove that every undirected graph, with n nodes and at least $(n^2-3*n+6)/2$ edges, contains a Hamilton cycle.

3 Functions

3.1 Functions

Functions are about the most important building blocks in mathematical reasoning. Functions are almost everywhere. Examples are the well known functions $f \in \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^2$, $f(x) = \sin(x)$, or $f(x) = \frac{1}{x^2+1}$. Actually, such functions are relations on $\mathbb{R}$: we say that $x \in \mathbb{R}$ is related to $y \in \mathbb{R}$ if and only if $f(x) = y$. Thus, every function $f \in \mathbb{R} \rightarrow \mathbb{R}$ corresponds to the relation $\{ (x,y) \mid f(x) = y \}$. This is the traditional mathematical way to define functions.

3.1 Definition. A relation R from a set B to a set V is a *function* – also called a *mapping* – if (and only if) it has the following two properties.

(a) For every $b \in B$ there is *at most one* $v \in V$ with $b\,R\,v$;

(b) For every $b \in B$ there is *at least one* $v \in V$ with $b\,R\,v$;

Requirement (a) is called the requirement of *functionality*. This can be formalized as follows: $b\,R\,u \wedge b\,R\,v \;\Rightarrow\; u = v$, for all $b \in B$ and $u, v \in V$. In words, if $b \in B$ is in relation to some element of V this element is *unique*.

Requirement (b) is called the requirement of *totality*. It states that *every* $b \in B$ is related to some element of V.

If relation R is functional but not total then R is called a *partial function*, so a (truly) partial function only satisfies (a). To emphasize that a function is not partial, functions satisfying (a) and (b) also are called *total functions*. Notice that requirements (a) and (b) together state that for every $b \in B$ there is *exactly one* $v \in V$ satisfying $b\,R\,v$.

□

By default, functions are total, unless stated otherwise. For functions we usually (but not always) use names $f, g, h, \ldots$ or $F, G, H, \ldots$. If f is a (partial or total) function from B to V we write $f(b)$ for the unique element $v \in V$ for which $b\,f\,v$, if it exists: so, $f(b) = v \;\Leftrightarrow\; b\,f\,v$.

If f is a total function we call B the *domain* of f. Now we have $f(b) \in V$ for *every* $b \in B$. If f is a partial function then f's domain is the *largest* subset of B on which f is defined. That is, subset $A : A \subseteq B$ is f's domain if and only if it satisfies both:

$$(\forall b : b \in A : (\exists v : v \in V : b\,f\,v)) \quad \text{, and:}$$

$$(\forall b : b \in B \backslash A : \neg (\exists v : v \in V : b\,f\,v)) \quad .$$

So, for partial function f from B to V with domain A we have $f(b) \in V$ for *every* $b \in A$ and $f(b)$ is *undefined* for all b not in A. Notice that every partial function from B to V with domain A is a total function from A to V.

Combining these observations we conclude that every (partial or total) function f from B to V with domain A satisfies $(\forall b : b \in A : f(b) \in V)$, and $A = B$ if and only if f is total.

The set of all functions from B to V is denoted by $B \to V$, also by V^B . The latter notation is motivated by the property $\#(V^B) = (\#V)^{\#B}$ for finite sets B, V. If f is a function in this set we also say that "f has type $B \to V$"; also, $f \in B \to V$ and $f : B \to V$ are common ways to denote this.

3.2 Example. We already have encountered numerous examples of functions. Here are some familiar ones.

(a) polynomial functions like $f \in \mathbb{R} \to \mathbb{R}$, with $f(x) = x^3$, for all $x \in \mathbb{R}$.

(b) goniometric functions like cos, sin and tan.

(c) $\sqrt{} \in \mathbb{R}_{\geq 0} \to \mathbb{R}$, mapping the non-negative reals to their square roots.

(d) $\ln \in \mathbb{R}^+ \to \mathbb{R}$, the natural logarithm.

3.2 Equality of functions

If two (total) functions with the same domain have equal values in all points of their common domain then these functions are equal, and conversely:

for sets B and V and functions $f, gB \to V$ we have $f = g$ if and only if $\forall x \in B : f(x) = g(x)$.

3.3 Monotonicity of function types

If $V \subseteq W$ then every (partial or total) function in $B \to V$ also is a (partial or total) function in $B \to W$. Hence, the set $B \to V$ of functions to V is a subset of the set $B \to W$ of functions to W .

Similarly, if $A \subseteq B$ then every function f in $B \to V$ satisfies: $f(b) \in V$ for every $b \in A$. This way, f can be considered as a function of type $A \to V$. Notice, however, that this is not true from a strictly formal point of view. Recalling that a function is a relation, function f , of type $B \to V$, contains a pair (b, v) , for every $b \in B$, so, also if $\neg(b \in A)$, whereas the functions in $A \to V$ only contain pairs (b, v) with $b \in A$. By omitting all pairs (b, v) with $\neg(b \in A)$, however, function f can be *restricted* to domain A . Calling the function thus obtained g , it is defined relationally by:

$$g \;=\; \{\, (b, v) \mid b \in A \wedge f(b) = v \,\} \quad .$$

Now function g has type $A \to V$, and it satisfies:

$$(\forall b : b \in A : g(b) = f(b)\,) \quad .$$

In practical situations, however, we usually will not introduce a separate name for this restricted function g , and we simply state that if $A \subseteq B$ then every function in $B \to V$ can be restricted to A, yielding a function in $A \to V$.

3.3 Example. Every function in $\mathbb{R} \to \mathbb{R}$ can be restricted to a function in $\mathbb{N} \to \mathbb{R}$, and every function in $\mathbb{N} \to \mathbb{N}$ also is a function in $\mathbb{N} \to \mathbb{Z}$.

3.4 Function composition

We have seen earlier that if S is a relation from set B to set V and if T is a relation from V to a set Z then their composition, as denoted by $S;T$, is a relation from B to Z. The following lemma states that relational composition of two functions itself is a function again.

3.4 Lemma. If f is a function in $B \to V$ and if g is a function in $V \to Z$ then the relation $f\,;g$ is a function in $B \to Z$.
$\square$

It is common mathematical practice to write the composition of two functions f and g as $g \circ f$, instead of as $f\,;g$. Notice, however, that the difference is purely notational, as we now have: $g \circ f \;=\; f\,;g$. So, according to the above lemma, if f has type $B \to V$ and if g has type $V \to Z$ then $g \circ f$ is a function of type $B \to Z$; it is defined by:

$$(g \circ f)(b) \;=\; g(f(b)) \quad \text{, for all } b \in B \ .$$

3.5 Properties. The following properties (b) and (c) are directly inherited from the corresponding properties of relational composition.

(a) On set B the identity relation I_B is a function from B to B, and $I_B(b) \;=\; b$, for every $b \in B$. Not surprisingly, I_B is also called the identity function on B.

(b) I is the identity of function composition: if $f \in B \to V$ then $f \circ I_B \;=\; f$ and $I_V \circ f \;=\; f$.

(c) Function composition is associative: $h \circ (g \circ f) \;=\; (h \circ g) \circ f$, for functions f, g, h of appropriate types.

3.5 Lifting a function

Let B and V be sets and let $f \in B \to V$ be a function from B to V. As stated earlier, set B is called the *domain* of f. Also, set V is called f's *codomain*.

For $b \in B$ element $f(b)$ (in V) is called the *image* of b under f, or the *value of* function f in point b. The subset of V containing all values $f(b)$, for all $b \in B$, is called the *image* of set B under f.

The notion of image can be generalized to arbitrary subsets of B. For any subset $A : A \subseteq B$ the image of A under f is a subset of V, namely:

$$\{\, f(b) \mid b \in A \,\} \ .$$

This subset depends, in a unique way, on subset A. So, we can define a function F, say, from the set of all subsets of B to the set of all subsets of V, as follows:

$$F(A) \;=\; \{\, f(b) \mid b \in A \,\} \quad \text{, for all } A : A \subseteq B \ .$$

In common mathematical language the set of all subsets of set B, also called B's *power set*, is denoted by $\mathcal{P}(B)$ or by 2^B. The latter notation is motivated by the property $\#(2^B) = 2^{\#B}$ for finite sets B. Thus, function F has type $\mathcal{P}(B) \to \mathcal{P}(V)$.

This function F also depends on f, of course. For every function f in $B \to V$ there is corresponding function F in $\mathcal{P}(B) \to \mathcal{P}(V)$, as defined above. We call F the *lifted* version of f; it has the following properties that can be proved straightforwardly.

3.6 Properties.

(a) $F(\varnothing) = \varnothing$

(b) $F(\{b\}) = \{f(b)\}$, for all $b \in B$

(c) F *distributes over* arbitrary unions; that is, for any collection Ω of subsets of B –so, $\Omega \subseteq \mathcal{P}(B)$–, we have:

$$F((\bigcup_{A:\, A \in \Omega} A)) \;=\; (\bigcup_{A:\, A \in \Omega} F(A))$$

(d) F is *monotonic*; that is, for all subsets A_0, A_1 of B:

$$A_0 \subseteq A_1 \;\Rightarrow\; F(A_0) \subseteq F(A_1)$$

(e) If F is lifted f and if G is lifted g, then $G \circ F$ is lifted $g \circ f$.

(f) For every subset $A \subseteq B$ and subset $U \subseteq V$:

$$F(A) \subseteq U \;\Leftrightarrow\; (\forall b : b \in A : f(b) \in U) \quad .$$

Notice that Property (b) shows that, in turn, function F uniquely determines function f from which F was obtained. In a (not too strict) way, F is a *generalization* of f, of which f can be considered an instance.

A function f, of type $B \to V$, and its lifted version, of type $\mathcal{P}(B) \to \mathcal{P}(V)$ and called F above, are entirely different functions. Nevertheless, it is common mathematical practice to *denote both* by the same name f; so, instead of $f(b)$ and $F(A)$ we write $f(b)$ and $f(A)$. This, so-called, *overloading* of the name f is rather harmless, but the interpretation of an expression like $f(x)$ now depends on the type of x: if $x \in B$ the expression just means $f(x)$, but if $x \subseteq B$, that is: $x \in \mathcal{P}(B)$, then the expression means $F(x)$.

We have called the set of function values $f(b)$, for all $b \in B$, the *image* or *range* of f. In terms of lifted f the image of f just is $f(B)$.

The following properties are easily checked.

3.7 Properties. Functions $f \in B \to V$ and $g \in V \to Z$ satisfy:

(a) $(g \circ f)(B) = g(f(B))$.

(b) $(g \circ f)(B) \subseteq g(V)$.

* * *

An element $b{\in}B$ satisfying $f(b)=v$, for some $v{\in}V$, is called an *original* of v under function f. As we know, because f is a function every $b{\in}B$ is related to a unique value, written as $f(b)$, in V. Conversely, it is not necessarily true that every $v{\in}V$ has a unique original in B: for any $v{\in}V$ set B may contain $0, 1$, or many elements b satisfying $f(b)=v$. The *whole set* of such elements b, however, is unique. That is, by lifting again, we can define a function G, say, of type $\mathcal{P}(V)\to\mathcal{P}(B)$, by:

$$G(U) \;=\; \{\, b \mid b{\in}B \wedge f(b){\in}U \,\} \quad \text{, for all } U : U\subseteq V \quad .$$

Set $G(U)$ is called the *pre-image* under f of set U. In particular, for any value $v{\in}V$, the set of all elements $b{\in}B$ satisfying $f(b)=v$ now is $G(\{v\})$; so, the pre-image of $\{v\}$ is the set of all originals of v.

In common mathematical notation $G(U)$ is written as $f^{-1}(U)$. As we will see later, some functions f have the property that, for every $v{\in}V$ there is a unique $b{\in}B$ with $f(b)=v$. Then, a function exists, of type $V\to B$, mapping every v to this unique b. This function is called f's *inverse* and it is denoted by f^{-1}. Function G, as defined here on sets, then is the lifted version of f^{-1}, which is why it is also written as f^{-1}. So, generally we have:

$$f^{-1}(U) \;=\; \{\, b \mid b{\in}B \wedge f(b){\in}U \,\} \quad \text{, for all } U : U\subseteq V \quad ,$$

and if function f has an inverse we have, for all $b{\in}B$ and $v{\in}V$:

$$b=f^{-1}(v) \;\Leftrightarrow\; f(b)=v \quad \text{, and:}$$

$$\{\, f^{-1}(v) \,\} \;=\; f^{-1}(\{v\}) \quad ,$$

3.8 Example.

(a) Let $f{\in}\mathbb{R}\to\mathbb{R}$ with $f(x)=x^2$ for all $x{\in}\mathbb{R}$. Then $f^{-1}([0,4]) = [-2,2]$.

(b) Consider the function $\mathsf{mod}\,8$ in $\mathbb{Z}\to\mathbb{Z}$. The originals of 3 then are the elements of the set $\{\ldots,-13,-5,3,11,19,\ldots\}$.

3.9 Theorem. Every function $f\in B\to V$ satisfies:

(a) $A\subseteq f^{-1}(f(A))$, for all $A : A\subseteq B$;

(b) $f(f^{-1}(U))\subseteq U$, for all $U : U\subseteq V$.

Proof.

(a) Let $a \in A$. The $f(a) \in f(A)$, so $a \in f^{-1}(f(A))$.

(b) Let $y \in f(f^{-1}(U))$. Then there is $x \in (f^{-1}(U))$ such that $f(x) = y$. Since $x \in (f^{-1}(U))$ we have $y = f(x) \in U$.

□

3.10 Example. Let $f:\mathbb{R}\to\mathbb{R}$ be defined by $f(x)=x^2$, for all $x\in\mathbb{R}$. Then the range $f^{-1}(f([0,1]))$ equals $[-1,1]$, which properly contains $[0,1]$. Moreover, we have $f^{-1}(f([-4,4]))=[0,4]$, which is properly contained in $[-4,4]$. This shows that we can have strict inclusions in the above theorem.

3.6 Surjective, injective, and bijective functions

Some functions have additional and useful properties. Here we define some of them.

3.11 Definition. A function $f:B\to V$ is *surjective* if every element in V is the value of f for *at least* one value in B, that is, if:

$$(\exists b: b\in B: f(b)=v) \quad \text{, for all } v\in V \quad .$$

Equivalently, we can state that f is surjective if

$$\forall v\in V: \#\{b\in B \mid f(b)=v\}\geq 1.$$

A function f in $B\to V$ is *injective* if every element in V is the value of f for *at most* one value in B, that is, if:

$$f(a)=f(b) \;\Rightarrow\; a=b \quad \text{, for all } a,b\in B \quad .$$

Equivalently, we can state that f is injective if

$$\forall v\in V: \#\{b\in B \mid f(b)=v\}\leq 1.$$

A function f in $B\to V$ is *bijective* if it is both surjective and injective. Hence, a function is bijective if every element in V is the value of f for *exactly one* value in B:

$$\forall v\in V: \#\{b\in B \mid f(b)=v\}=1.$$

□

Sometimes injection, surjection and bijection are used as shorthands for injective function, surjective function and bijective function.

3.12 Lemma. A function f in $B\to V$ is surjective if and only if $f(B)=V$.

Proof. Always holds $f(B)\subseteq V$, so it remains to prove that surjectivity is equivalent to $V\subseteq f(B)$:

f is surjective

$\Leftrightarrow$ { Definition }

$(\exists b : b \in B : f(b) = v)$ for all $v \in V$

$\Leftrightarrow$ { Definition }

$v \in f(B)$ for all $v \in V$

$\Leftrightarrow$ { Definition }

$V \subseteq f(B)$.

□

3.13 Lemma. Let $f : B \to V$ and $g : V \to Z$. Then

(a) if $g \circ f$ is injective, then f is injective;

(b) if $g \circ f$ is surjective, then g is surjective;

(c) if f and g are injective, then $g \circ f$ is injective;

(d) if f and g are surjective, then $g \circ f$ is surjective.

(e) if f and g are bijective, then $g \circ f$ is bijective.

Proof.

(a) Let $g \circ f$ is injective, we have to prove that f is injective. Let $x, x' \in B$ satisfy $f(x) = f(x')$. Then $g \circ f(x) = g(f(x)) = g(f(x')) = (g \circ f)(x')$. Since $g \circ f$ is injective we conclude $x = x'$. This proves that f is injective.

(b) Let $g \circ f$ is surjective, we have to prove that g is surjective. Let $z \in Z$, we have to find $y \in V$ such that $g(y) = z$. Since $g \circ f$ is surjective there exists $x \in B$ such that $z = (g \circ f)(x) = g(f(x)$, so choosing $y = f(x)$ does the job.

(c) Assume that f and g are injective, we have to prove that $g \circ f$ is injective. So let $x, x' \in B$ such that $(g \circ f)(x) = (g \circ f)(x')$. Since g is injective and $g(f(x)) = (g \circ f)(x) = (g \circ f)(x') = g(f(x'))$ we conclude $f(x) = f(x')$. Since f is injective we conclude that $x = x'$, proving that $g \circ f$ is injective.

(d) Assume that f and g are surjective, we have to prove that $g \circ f$ is surjective. Let $z \in Z$. Since g is surjective there exists $y \in V$ such that $g(y) = z$. Since f is surjective there exists $x \in B$ such that $f(x) = y$. Now $(g \circ f)(x) = g(f(x)) = g(y) = z$, so $g \circ f$ is surjective.

(e) Combine (c) and (d).

□

3.14 Example. This example illustrates that the “same” function is or is not surjective or injective, depending on which domain one considers.

(a) The function $\sin : \mathbb{R} \to \mathbb{R}$ is neither surjective nor injective.

(b) The function $\sin : [\,-\pi/2\,,\,\pi/2\,] \to \mathbb{R}$ is injective and not surjective.

(c) The function $\sin : \mathbb{R} \to [\,-1\,,\,1\,]$ is surjective and not injective.

(d) The function $\sin : [\,-\pi/2\,,\,\pi/2\,] \to [\,-1\,,\,1\,]$ is bijective.

□

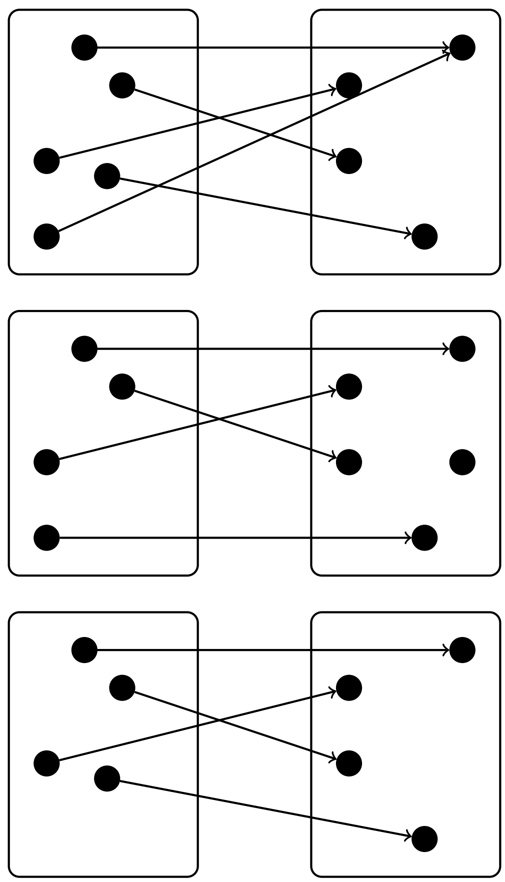


Figure 19: Surjective, injective and bijective functions

3.7 Inverse functions

In the definition of "function", in the beginning of this chapter, we have stated the requirements of "totality" and "functionality". The notion of "surjectivity" is equivalent to the notion of "totality", but with sets B and V interchanged. Similarly, the notion of "injectivity" is equivalent to the notion of "functionality", but with B and V interchanged. Recall that for every relation R from B to V its transposition R^{T} is the relation from V to B defined by:

$$v\,R^{\mathrm{T}}\,b \;\Leftrightarrow\; b\,R\,v \quad \text{, for all } b, v \quad .$$

Function f being surjective now means that relation f^{T} is total, and f being injective means that relation f^{T} is functional. From this we conclude immediately that if f is bijective relation then f^{T} is a function from V to B. This function happens to be f's *inverse*, and it is denoted by f^{-1}.

3.15 Definition. Function g in $V \to B$ is an *inverse* of function f in $B \to V$ if:

$$g \circ f \;=\; I_B \;\wedge\; f \circ g \;=\; I_V \quad .$$

3.16 Lemma. A function has *at most one* inverse, that is, if g and h both are inverses of f, then $g = h$.

Proof. Assume that g and h both are inverses of f. Then

$$g = g \circ I_V = g \circ (f \circ h) = (g \circ f) \circ h = I_B \circ h = h.$$

□

Lemma 3.16 justifies to speak about 'the' inverse of a function rather than 'an' inverse, and to fix the notation f^{-1} for it.

3.17 Lemma. Function g is the *inverse* of function f if and only if f is the inverse of g.

Proof. Directly by definition. □

3.18 Lemma. A function f has an inverse if and only if f is bijective.

Proof. First assume that $f : B \to V$ has an inverse $g : V \to B$. Let $y \in V$, then $f(g(y)) = (f \circ g)(y) = I_V(y) = y$, proving that f is surjective.

Assume that $x, x' \in B$ satisfy $f(x) = f(x')$. Then

$$x = I_B(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = I_B(x') = x',$$

proving that f is injective. So f is bijective.

Conversely, assume that $f : B \to V$ is bijective. Define $g : V \to B$ by defining $g(y)$ to be the unique element $x \in B$ such that $f(x) = y$, for every $y \in V$. Then $g(f(x)) = x$ and $f(g(y)) = y$ for all $x \in B$ and all $y \in V$, proving

$$g \circ f \;=\; I_B \;\wedge\; f \circ g \;=\; I_V,$$

hence g is the inverse of f. □

3.19 Lemma. If functions f in $B \to V$ and g in $V \to Z$ both are bijective then

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} \quad .$$

□

Proof. We have to prove that $f^{-1} \circ g^{-1}$ is the inverse of $g \circ f$. This follows from

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ I_V \circ f = f^{-1} \circ f = I_B$$

and

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ I_V \circ g^{-1} = g \circ g^{-1} = I_Z.$$

□

3.8 Finite sets and counting

The elements of finite sets can be counted. That is, we can define a function $\#$, say, that maps every finite set to its *number of elements*. So, for finite set V its number of elements $\#V$ is a natural number. We have that $\#V = n$ if and only if there is a bijection from V to $\{1, 2, \ldots, n\}$.
Without proof we collect some standard properties of $\#$.

3.20 Properties. For all finite sets U, V and value v:

(0) $\quad \#U = 0 \;\Leftrightarrow\; U = \varnothing$

(1) $\quad \#\{v\} = 1$

(2) $\quad 0 \leq \#U$

(3) $\quad \#(U \cup V) = \#U + \#V - \#(U \cap V)$

(4) $\quad \#(U \cup V) \leq \#U + \#V$

(5) $\quad \#(U \cup V) = \#U + \#V \;$, if $U \cap V = \varnothing$

(6) $\quad \#V = \#U + \#(V \setminus U) \;$, if $U \subseteq V$

(7) $\quad \#U \leq \#V \;$, if $U \subseteq V$

(8) $\quad \#U = \#V \;\Leftrightarrow\; U = V \;$, if $U \subseteq V$

□

Notice that these properties are mutually dependent. For example, property (4) follows directly from (3) and (2), property (5) is an instance of (3), and (6) is an instance of (5), whereas (7) follows from (6) and (2).

*   *   *

Functions on finite sets yield finite images. In what follows function f has type $B \to V$, where B and V are finite sets.

3.21 Lemma. $\#(f(B)) \le \#B$

Proof. By induction on the structure of B. If $B = \emptyset$ then $f(B) = \emptyset$ too, hence, in this case we even have $\#(f(B)) = \#B$. If $B = A \cup \{b\}$, for some b not in A we have:

$$
\begin{array}{ll}
 & \#(f(A \cup \{b\})) \\
= & \qquad \{\ f \text{ over } \cup\ \} \\
 & \#(f(A) \cup f(\{b\})) \\
\le & \qquad \{\ \text{property } 3.20\,(4)\ \} \\
 & \#(f(A)) + \#(f(\{b\})) \\
= & \qquad \{\ \text{definition of } f(\{b\})\ \} \\
 & \#(f(A)) + \#(\{f(b)\}) \\
= & \qquad \{\ \text{property } 3.20\,(1)\ \text{(twice)}\ \} \\
 & \#(f(A)) + \#(\{b\}) \\
\le & \qquad \{\ \text{Induction Hypothesis}\ \} \\
 & \#A + \#(\{b\}) \\
= & \qquad \{\ \text{property } 3.20\,(5)\text{, using } \neg(b \in A)\ \} \\
 & \#(A \cup \{b\})
\end{array}
$$

□

3.22 Lemma. "f is injective" $\Leftrightarrow$ $\#(f(B)) = \#B$

Proof. By mutual implication.

"$\Rightarrow$": Very similar to the proof of Lemma 3.21, using that $\#(f(A) \cup f(\{b\}))$ now is *equal* to $\#(f(A)) + \#(f(\{b\}))$, because for injective f we have $\neg(f(b) \in f(A))$ if $\neg(b \in A)$.

"$\Leftarrow$": By contraposition, that is, if f is not injective then $\#(f(B)) \ne \#B$. If f is not injective then B contains elements a, b, say, with $a \ne b$ and $f(a) = f(b)$. Now:

$$
\begin{array}{ll}
 & \#(f(B)) \\
= & \qquad \{\ a \ne b \text{ and } f(a) = f(b)\text{, so } f(B \backslash \{a\}) = f(B)\ \} \\
 & \#(f(B \backslash \{a\})) \\
\le & \qquad \{\ \text{Lemma } 3.21\ \}
\end{array}
$$

$$
\begin{array}{ll}
 & \#(B\backslash\{a\}) \\
= & \quad \{ a\in B \} \\
 & \#B - 1 \quad ,
\end{array}
$$

from which we conclude that $\#(f(B)) < \#B$, hence, also $\#(f(B)) \neq \#B$.

$\square$

3.23 Lemma. "f is injective" $\Rightarrow$ $\#B \leq \#V$

Proof.

$$
\begin{array}{ll}
 & \#B \\
= & \quad \{ f \text{ is injective: Lemma 3.22} \} \\
 & \#(f(B)) \\
\leq & \quad \{ f(B)\subseteq V\text{: property 3.20 (7)} \} \\
 & \#V
\end{array}
$$

$\square$

3.24 Lemma. "f is surjective" $\Rightarrow$ $\#V \leq \#B$

Proof.

$$
\begin{array}{ll}
 & \#V \\
= & \quad \{ f \text{ is surjective: } f(B)=V \} \\
 & \#(f(B)) \\
\leq & \quad \{ \text{Lemma 3.21} \} \\
 & \#B
\end{array}
$$

$\square$

3.25 Lemma. "f is bijective" $\Rightarrow$ $\#V = \#B$

Proof.
Since f is injective, from Lemma 3.22 we conclude $\#(f(B)) = \#B$.
Since f is surjective we conclude $f(B) = V$. So $\#V = \#B$. $\square$

Without further proofs we observe that the converses to the two latter lemmas hold as well.

Properties.

(0) $\quad \#B \leq \#V \;\Rightarrow\; (\exists f : f\in B\to V : \text{"}f \text{ is injective"})$

(1) $\quad \#V \leq \#B \;\Rightarrow\; (\exists f : f\in B\to V : \text{"}f \text{ is surjective"})$

Now we are ready for the main theorem of this subsection.

3.26 Theorem. For f a function of type $B \rightarrow V$, for finite sets B, V, and if $\#B = \#V$, we have:

$$\text{“}f\text{ is injective”} \;\Leftrightarrow\; \text{“}f\text{ is surjective”}$$

Proof.

$$\begin{array}{ll}
 & \text{“}f\text{ is injective”} \\
\Leftrightarrow & \qquad \{ \text{ Lemma 3.22 } \} \\
 & \#(f(B)) = \#B \\
\Leftrightarrow & \qquad \{ \ \#B = \#V \ \} \\
 & \#(f(B)) = \#V \\
\Leftrightarrow & \qquad \{ \ f(B) \subseteq V\text{: property 3.20 (8) } \} \\
 & f(B) = V \\
\Leftrightarrow & \qquad \{ \text{ Lemma 3.12 } \} \\
 & \text{“}f\text{ is surjective”}
\end{array}$$

$\square$

As a consequence of Theorem 3.26 we conclude that for functions from a finite set to itself, the properties injectivity and surjectivity coincide. Here finiteness is essential. For instance, the function $s : \mathbb{N} \rightarrow \mathbb{N}$ defined by $s(x) = x + 1$ for all $x \in \mathbb{N}$ is injective, but not surjective since no element maps to 0. Conversely, the function $f : \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x) = x - 1$ for all $x > 0$, and $f(0) = 0$ is surjective, but not injective since $f(0) = 0 = f(1)$.

3.27 Example. Suppose p and q are two different prime numbers. We consider the function φ in $[\,0\,..\,p\,) \rightarrow [\,0\,..\,p\,)$, defined by $\varphi(x) = (x * q) \mathsf{\ mod\ } p$, for all $x \in [\,0\,..\,p\,)$.

We prove that φ is a bijection. By Theorem 3.26 it suffices to show that φ is injective. To this end we derive, for $x, y \in [\,0\,..\,p\,)$:

$$\begin{array}{ll}
 & \varphi(x) = \varphi(y) \\
\Leftrightarrow & \qquad \{ \text{ definition of } \varphi \ \} \\
 & (x * q) \mathsf{\ mod\ } p = (y * q) \mathsf{\ mod\ } p \\
\Leftrightarrow & \qquad \{ \text{ property of } \mathsf{mod} \ \} \\
 & (\,(x - y) * q\,) \mathsf{\ mod\ } p = 0 \\
\Leftrightarrow & \qquad \{ \text{ property of } \mathsf{mod} \text{ and } \mid \ \} \\
 & p \mid (\,(x - y) * q\,) \\
\Leftrightarrow & \qquad \{ \text{ “}p\text{ is prime”: } (p\,\mid) \text{ distributes over } * \ \}
\end{array}$$

$$
\begin{array}{ll}
 & p \mid (x-y) \;\vee\; p \mid q \\
\Leftrightarrow & \quad \{ \text{“}p \text{ and } q \text{ are prime” and } p \neq q \text{, hence: } \neg(p \mid q) \;\} \\
 & p \mid (x-y) \\
\Leftrightarrow & \quad \{ \; x, y \in [\, 0 \,..\, p \,) \text{, hence } -p < x-y < p \;\} \\
 & x = y \quad .
\end{array}
$$

□

3.9 Exercises

1. Set A is given by $A = \{1, 2, 3, 4\}$. Which of the following relations are functions from A to A?

   (a) $\{(1,3), (2,4), (3,1), (4,2)\}$;
   (b) $\{(1,3), (2,4)\}$;
   (c) $\{(1,1), (2,2), (3,3), (4,4), (1,3), (2,4), (3,1), (4,2)\}$;
   (d) $\{(1,1), (2,2), (3,3), (4,4)\}$.

2. Suppose f and g are functions from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = x^2$ and $g(x) = x+1$ for all $x \in R$. What is $g \circ f$ and what is $f \circ g$?

3. Which of the following functions from $\{1, 2, 3, 4\}$ to $\{a, b, c, d\}$ is injective, surjective and/or bijective?

   (a) $\{(1,a), (2,d), (3,c), (4,b)\}$.
   (b) $\{(1,b), (2,d), (3,c), (4,b)\}$.
   (c) $\{(1,d), (2,b), (3,a), (4,c)\}$.
   (d) $\{(1,c), (2,d), (3,c), (4,b)\}$.

   For the bijective functions determine their inverses.

4. Which of the following functions is injective, surjective and/or bijective?

   (a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ for all $x \in \mathbb{R}$.
   (b) $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$, $f(x) = x^2$ for all $x \in \mathbb{R}$.
   (c) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = x^2$ for all $x \in \mathbb{R}$.

5. Suppose R and S are relations on a set V with $R\,;S = I$ and $S\,;R = I$. Prove that both R and S are bijective functions.

6. Let R be a finite relation with adjacency matrix A. Prove the following statements:

   (a) If every row of A contains exactly one non-zero entry, then R is a function.

(b) If, in addition, every column of A contains at most one entry, then function R is injective.

(c) If every row and column of A contain exactly one 1, then R is a bijection. What is the adjacency matrix of the inverse function?

7. Let B and V be sets and let R be a relation from B to V. Then, for every $v \in V$, we have defined[5] the *pre-image* of v as the set ${}_R[v]$, thus:

$$ {}_R[v] \;=\; \{\, b \in B \mid b R v \,\} \quad , $$

which, obviously, is a subset of B.

(a) Prove that the relation $\{\, (v \,,\, {}_R[v]) \mid v \in V \,\}$ is a function from V to $\mathcal{P}(B)$ (the set of all subsets of B).

(b) Prove that, if F is a function in $V \to \mathcal{P}(B)$, then the set R_F defined by $R_F \;=\; \{\, (b, v) \mid b \in F(v) \wedge v \in V \,\}$ is a relation from B to V, with ${}_{R_F}[v] = F(v)$, for all $v \in V$.

8. Given are two bijective functions f, of type $U \to V$, and g, of type $V \to W$. Prove that: $(g \circ f)^{-1} \;=\; f^{-1} \circ g^{-1}$.

9. We consider functions f, g, h, of type $U \to U$, such that both $g \circ f$ and $h \circ g$ are bijective. Prove that $h \circ g \circ f$ is bijective as well.

10. Prove that an injective function f in $B \to V$ has a *partial inverse*, that is, a partial function g from V to B such that $g \circ f \;=\; I_B$. What is the domain of g?

11. (a) Give an example of a set A and a surjective function $f : A \to A$ for which $f(a) = f(b)$ for some $a, b \in A$, $a \neq b$.

    (b) Prove that this is not possible if A is finite.

12. Let $f, g : A \to A$ for a finite set A for which $f \circ g$ is injective. Prove that both f and g are surjective.

13. (a) Give an example of two sets $A \subseteq B$ and an injective function $f : B \to A$ such that $A \neq B$.

    (b) Prove that, if $A \subseteq B$ are finite sets and $f : B \to A$ is injective, then $A = B$.

14. (a) Give an example of a set A and functions $f, g : A \to A$ such that $f \circ g = I$, but for which no $h : A \to A$ exists such that $h \circ f = I$.

    (b) Prove that this is not possible for A finite.

[5] See the chapter on relations.

4 Posets and lattices

4.1 Partial orders

Many important relations cover some idea of greater and smaller: the *partial order*s.

4.1 Definition. An (endo)relation $\sqsubseteq$ ("under") on a set P is called a *partial order* if it is reflexive, antisymmetric, and transitive. We recall that this means that, for all $x, y, z \in P$, we have:

- $x \sqsubseteq x$;
- $x \sqsubseteq y \ \wedge \ y \sqsubseteq x \ \Rightarrow \ x = y$;
- $x \sqsubseteq y \ \wedge \ y \sqsubseteq z \ \Rightarrow \ x \sqsubseteq z$.

The pair $(P, \sqsubseteq)$ is called a *partially ordered set* or, for short, a *poset*.

Two elements x and y in a poset $(P, \sqsubseteq)$ are called *comparable* if $x \sqsubseteq y$ or $y \sqsubseteq x$, otherwise they are called *incomparable*, that is, if $\neg(x \sqsubseteq y)$ and $\neg(y \sqsubseteq x)$.

A partial order is a *total order*, also called *linear order*, if every two elements are comparable.

□

4.2 Lemma. For every poset $(P, \sqsubseteq)$ and for every subset X of P, the pair $(X, \sqsubseteq)$ is a poset too.

□

4.3 Example.

- On every set, the identity relation I is a partial order. It is the *smallest* possible partial order relation on that set.
- On the real numbers $\mathbb{R}$ the relation $\leq$ is a total order: every two numbers $x, y \in \mathbb{R}$ satisfy $x \leq y$ or $y \leq x$. Restriction of $\leq$ to any subset of $\mathbb{R}$ −for example, restriction to $\mathbb{Q}, \mathbb{Z}, \mathbb{N}$ − also yields a total order on that subset.
- The power set $\mathcal{P}(V)$ of a set V, that is, the set of all subsets of V, with relation $\subseteq$ (subset inclusion), is a poset. This P contains a smallest element, namely $\emptyset$, and a largest element, namely V itself. For $\#V \geq 2$ the order is not total: if u, v are distinct then neither $\{u\} \subseteq \{v\}$ nor $\{v\} \subseteq \{u\}$, so $\{u\}$ and $\{v\}$ are incomparable.
- The relation $\mid$ ("divides") is a partial order on the positive naturals, defined by

  $$x \mid y \ \Leftrightarrow \ (\exists z : z \in \mathbb{N} : x * z = y).$$

  This order is not total, for instance, 2 and 3 are incomparable.

□

4.4 Definition. The *irreflexive part* of a partial order relation $\sqsubseteq$ is denoted by $\sqsubset$ ("strictly under") and is defined by, for all $x, y \in P$:

$$x \sqsubset y \;\Leftrightarrow\; x \sqsubseteq y \;\wedge\; x \neq y \quad .$$

□

It is straightforward to prove that the relation $\sqsubset$ is irreflexive, antisymmetric and transitive. Further, it directly follows from the definition that for all $x, y \in P$: $x \sqsubseteq y \;\Leftrightarrow\; x \sqsubset y \;\vee\; x = y$.

4.5 Lemma. If $(P, \sqsubseteq)$ is a poset, then the corresponding directed graph, with vertex set P and arrows (x, y) whenever $x \sqsubset y$, is *acyclic*.
□

If we want to draw a picture of a finite poset, with the greater elements on top and the smaller elements below, and an arrow from x to y if $x \sqsubseteq y$ holds, we usually do not draw the whole graph. Edges from a node x to itself, representing $x \sqsubseteq x$ are not drawn, and an edge from x to y with $x \sqsubseteq y$ is only drawn if there is no z, distinct from both x and y, for which we have $x \sqsubseteq z$ and $z \sqsubseteq y$. The resulting directed graph is called the *Hasse diagram* for $(P, \sqsubseteq)$, named after the German mathematician Helmut Hasse (1898-1979). Hasse diagrams are drawn in such a way that two vertexes x and y with $x \sqsubseteq y$ are connected by an edge going upwards. In Theorem 4.14 we will see that this is always possible. Consequently, the edges in Hasse diagrams do not need an arrow point to indicate the direction. For example the Hasse diagram for the poset $(\mathcal{P}(\{a, b, c\}), \subseteq)$ is drawn as in Figure 20.

The Hasse diagram is a relation itself, on the same finite set P. In fact, it is the smallest relation H of which the reflexive transitive closure H^* coincides with the given relation $\sqsubseteq$.

* * *

There are various ways of constructing new posets out of old ones. We discuss some of them. In the sequel both $(P, \sqsubseteq)$ and $(Q, \sqsubseteq)$ are posets. Notice that we use the *same* symbol, $\sqsubseteq$, for the two *different* partial order relations on sets P and Q. If confusion may arise we distinguish the two relations by using $\sqsubseteq_P$ and $\sqsubseteq_Q$, respectively.

- As already stated in Lemma 4.2, for every subset X of P the pair $(X, \sqsubseteq)$ is a poset, with relation $\sqsubseteq$ restricted to X. Thus restricted $\sqsubseteq$ is called the *induced* order on X.

- Relation $\sqsupseteq$ ("above"), defined by, for all $x, y \in P$, $x \sqsupseteq y \Leftrightarrow y \sqsubseteq x$ is a partial order too, called the *dual order to* $\sqsubseteq$; hence, $(P, \sqsupseteq)$ also is a poset.

- Let V be a set. On the set $V \to P$ of functions from V to P we can define a partial order $\sqsubseteq_{VP}$, say, as follows, for all $f, g \in V \to P$:

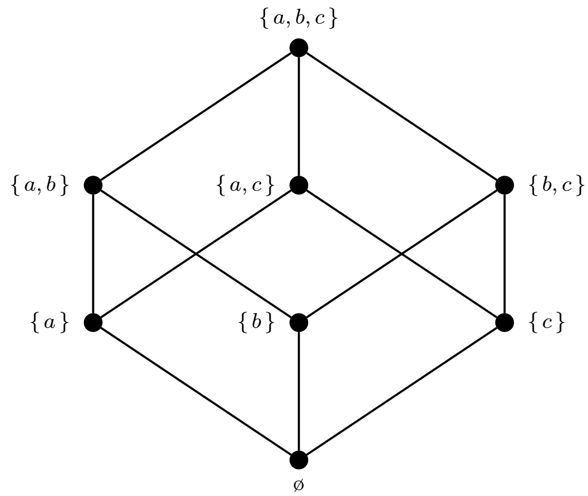


Figure 20: A Hasse diagram of $(\mathcal{P}(\{a,b,c\}), \subseteq)$

$$f \sqsubseteq_{VP} g \;\Leftrightarrow\; (\forall v : v \in V : f(v) \sqsubseteq_P g(v)) \quad .$$

Then $(V \to P, \sqsubseteq_{VP})$ is a poset.

- On the Cartesian product $P \times Q$ we can define a partial order as follows. For $(p,q), (x,y) \in P \times Q$ we define:

  $$(p,q) \sqsubseteq (x,y) \;\Leftrightarrow\; p \sqsubseteq_P x \wedge q \sqsubseteq_Q y \quad .$$

  Thus defined relation $\sqsubseteq$ is a partial order, called the *product order* on $P \times Q$.

- On the Cartesian product $P \times Q$ we also can define a partial order as follows. For $(p,q), (x,y) \in P \times Q$ we define:

  $$(p,q) \sqsubseteq (x,y) \;\Leftrightarrow\; (p \neq x \wedge p \sqsubseteq_P x) \vee (p = x \wedge q \sqsubseteq_Q y) \quad .$$

  This relation $\sqsubseteq$ is a partial order too, called the *lexicographic order* on $P \times Q$.

The notions of product order and lexicographic order can be extended to (finite) products of more than two sets.

A poset's structure is determined by its partial order relation, as denoted by $\sqsubseteq$ in the previous section. Sometimes we wish to prove equalities in a poset, and then it can be convenient if we can reformulate an equality in terms of the partial order relation: that enables us to reason in terms of the partial order.

The following lemma provides such a connection between equality and the partial order, apart from the property $x = y \Leftrightarrow (x \sqsubseteq y \wedge y \sqsubseteq x)$ that holds by reflexivity and anti-symmetry.

4.6 Lemma. In every poset $(P, \sqsubseteq)$ we have, for all $x, y \in P$:

(a) $x = y \;\Leftrightarrow\; (\forall z : z \in P : x \sqsubseteq z \Leftrightarrow y \sqsubseteq z)$;

(b) $x = y \;\Leftrightarrow\; (\forall z : z \in P : z \sqsubseteq x \Leftrightarrow z \sqsubseteq y)$.

Proof. We prove (a) only; the proof of (b) follows, mutatis mutandis, the same pattern. We do so by mutual implication.

"$\Rightarrow$": Assuming $x = y$ we may substitute x for y and vice versa wherever we like; in particular, if we substitute x for y in our demonstrandum $(\forall z : z \in P : x \sqsubseteq z \Leftrightarrow y \sqsubseteq z)$, we obtain $(\forall z : z \in P : y \sqsubseteq z \Leftrightarrow y \sqsubseteq z)$, which is true because of the reflexivity of $\Leftrightarrow$.

"$\Leftarrow$": Assuming $(\forall z : z \in P : x \sqsubseteq z \Leftrightarrow y \sqsubseteq z)$, by the instantiation $z := x$ we obtain $x \sqsubseteq x \Leftrightarrow y \sqsubseteq x$, which is equivalent to $y \sqsubseteq x$, because $\sqsubseteq$ is reflexive. Moreover, by the instantiation $z := y$ we obtain $x \sqsubseteq y \Leftrightarrow y \sqsubseteq y$, which is equivalent to $x \sqsubseteq y$. By the antisymmetry of $\sqsubseteq$ we conclude $x = y$, as required.
□

4.2 Extreme elements

4.7 Definition. For any subset X of a poset $(P, \sqsubseteq)$ we define, for all $m \in P$:

(a) m is X's *maximum*, or *largest element* if:

$m \in X \;\wedge\; (\forall x : x \in X : x \sqsubseteq m)$.

(b) m is X's *minimum*, or *least element* if:

$m \in X \;\wedge\; (\forall x : x \in X : m \sqsubseteq x)$.

(c) m is *a maximal* element of X if:

$m \in X \;\wedge\; (\forall x : x \in X : \neg(m \sqsubset x))$.

(d) m is *a minimal* element of X if:

$m \in X \;\wedge\; (\forall x : x \in X : \neg(x \sqsubset m))$.

□

Note that by definition $\neg(m \sqsubset x)$ is equivalent to $m \sqsubseteq x \;\Rightarrow x = m$, so maximality of m can be reformulated as $m \in X \;\wedge\; (\forall x : x \in X : m \sqsubseteq x \;\Rightarrow x = m)$, and similar for minimality.

Notice the difference between the notions "maximum" and "maximal". A value $m \in P$ is X's maximum if $m \in X$ and all elements in X are under m, whereas m is a maximal element of X if $m \in X$ and X contains no elements strictly above m.

A subset of a partially ordered set does not necessarily contain such extreme elements. The next lemma states that if it exists, however, the maximum of a subset is unique, and so is the minimum, if it exists. If subset X has a maximum we denote it by $\mathsf{max}\,X$, and its minimum we denote by $\mathsf{min}\,X$.

4.8 Lemma. Let X be a subset of a poset $(P, \sqsubseteq)$. If m and n both are X's maximum then $m = n$. If m and n both are X's minimum then $m = n$.
$\Box$

Proof. Assume that both m and n are a maximum of X, then by definition $m, n \in X$ and $(\forall x : x \in X : x \sqsubseteq m \wedge x \sqsubseteq n)$. So we both have $n \sqsubseteq m$ and $m \sqsubseteq n$. Since $\sqsubseteq$ is anti-symmetric we conclude $m = n$. $\Box$

A subset of a partially ordered set does not necessarily contain maximal or minimal elements. Such elements are not unique either: a subset may have many maximal or minimal elements. As a rather trivial example, consider poset (P, I_P), where the identity relation I_P is the smallest possible partial order on P: $x\, I_P\, y \Leftrightarrow x = y$. With this particular order all elements of a subset $X \subseteq P$ both are maximal and minimal.

4.9 Definition. Let $(P, \sqsubseteq)$ be a poset. If the whole set P has a minimum this is often denoted by $\perp$ ("bottom"), and if P has a maximum this is often denoted by $\top$ ("top"). If P has a minimum the minimal elements of $P \backslash \{\perp\}$ are called P's *atoms*.

4.10 Example.

- If we consider the poset of all subsets of a set V, then the empty set $\emptyset$ is the minimum of the poset, whereas the whole set V is the maximum. The atoms are the subsets of V containing just a single element.
- In the poset $(\mathbb{N}^+, \mid)$ the whole set, $\mathbb{N}^+$, has no maximum. Its minimum, however, equals 1. The atoms are the prime numbers. Surprisingly, in the poset $(\mathbb{N}, \mid)$ the whole set $\mathbb{N}$ has a maximum: the element 0, since by definition every number is a divisor of 0.
- If $(P, \sqsubseteq)$ is totally ordered then subset $\{x, y\}$ has a maximum and a minimum, for all $x, y \in P$.

$\Box$

4.11 Lemma. In a poset $(P, \sqsubseteq)$ for every subset X its maximum, if it exists, is a maximal element of X; also, its minimum, if it exists, is a minimal element of X.

Proof. Assume m is the maximum of X. Then $m \in X$ and $x \sqsubseteq m$ for all $x \in X$. Choose $x \in X$ satisfying $m \sqsubseteq x$. Then using antisymmetry and $x \sqsubseteq m$ we conclude $x = m$, so proving $m \sqsubseteq x \Rightarrow x = m$. This proves that m is maximal.

The proof for minimal/minimum is similar. $\Box$

4.12 Lemma. If a poset $(P, \sqsubseteq)$ is a total order then every subset $X \subseteq P$ has at most one maximal element, which then also is its maximum. Also, X has at most one minimal element, which then also is its minimum.

Proof. Assume that m is maximal in X and $n \in X$. Then by definition $\neg(m \sqsubset n)$, so $m = n$ or $\neg(m \sqsubseteq n)$. If $\neg(m \sqsubseteq n)$ then from totality we conclude $n \sqsubseteq m$. So in both cases we have $n \sqsubseteq m$. This proves that m is the maximum of X. If moreover n is maximal too, we similarly prove $n \sqsubseteq m$, so by antisymmetry we conclude $m = n$.

The proof for minimal/minimum is similar. □

4.13 Lemma. Let $(P, \sqsubseteq)$ be a *nonempty* and *finite* poset. Then P contains a maximal element and a minimal element.

Proof. Choose $x_1 \in P$ arbitrary. For $i = 1, 2, 3, \ldots$ choose x_{i+1} such that $x_i \sqsubset x_{i+1}$, that is, $x_i \sqsubseteq x_{i+1}$ and $x_i \neq x_{i+1}$. If at some point no such x_{i+1} exists, we have found a maximal element x_i.

Otherwise, the process goes on forever yielding an infinite sequence

$$x_1 \sqsubset x_2 \sqsubset x_3 \sqsubset x_4 \sqsubset x_5 \sqsubset \cdots .$$

Since P is finite, not all x_i can be distinct, so there is some $i < j$ such that $x_i = x_j$. So $x_i \sqsubseteq^* x_{j-i} \sqsubseteq x_j = x_i$. For a transitive relation R one easily proves by induction $R^n \subseteq R$ for $n > 0$. So if $i < j - 1$ then $x_i \sqsubseteq x_{j-1}$. If $i = j - 1$ then $x_i = x_{j-i}$, so in all cases we conclude $x_i \sqsubseteq x_{j-1}$. So $x_i \sqsubseteq x_{j-1} \sqsubseteq x_j = x_i$. Now antisymmetry yields $x_{j-1} = x_j$, contradicting the requirement $x_i \neq x_{i+1}$ in the construction for all i.

□

4.14 Theorem. [**Topological sorting**] For any finite poset $(P, \sqsubseteq)$ with $\#P = n$ there exists a bijection $f : P \to \{1, 2, \ldots, n\}$ such that $x \sqsubset y \Rightarrow f(x) < f(y)$ for all $x, y \in P$.

Proof. We prove the theorem by induction on $n = \#P$. For $n = 1$ we define $f(x) = 1$ for the single element x of P. It is clearly a bijection, and the other property holds since $x \sqsubset y$ never occurs.

For $n > 1$ we choose $p \in P$ such that p is maximal in P; this is possible by Lemma 4.13. By the induction hypothesis there exists $f' : P \setminus \{p\} \to \{1, \ldots, n-1\}$ such that $f'(x) < f'(y)$ for all $x, y \in P \setminus \{p\}$. Next we define $f : P \to \{1, \ldots, n\}$ by $f(p) = n$ and $f(x) = f'(x)$ for $x \neq p$. It is surjective since f' is surjective and $f(p) = n$; bijectivity follows from Theorem 3.26.

It remains to prove that $f(x) < f(y)$ for all $x, y \in P$ satisfying $x \sqsubset y$, which we do by case analysis:

- $x = p$ does not occur since $x \sqsubset y$ contradicts maximality of $x = p$,
- if $y = p$ then $x \in P \setminus \{p\}$, so

$$f(x) = f'(x) \leq n - 1 < n = f(p) = f(y),$$

- if $x \neq p \neq y$ then $f(x) = f'(x) < f'(y) = f(y)$.

$\square$

Topological sorting justifies the existence of Hasse diagrams: if every node x is drawn on height $f(x)$, then for every $x \sqsubset y$ the element y is drawn higher than x.

4.15 Example. Topological sorting has various applications. For example consider a (so-called) *spreadsheet*. In a spreadsheet the values in various *cells* depend on each other, but, in a correct spreadsheet, in an acyclic way only. The value in any particular cell in the spreadsheet can only be computed if the values in all cells on which this particular cell depends have been computed already. Therefore, an efficient implementation of these computations requires that they are performed in the "right" order. This gives rise to a partial order on the set of cells within a spreadsheet. By topological sorting the set of cells can be linearized in such a way that every cell precedes all cells depending on it; thus the computations of the values in the cells can be performed in a linear order.

4.3 Upper and lower bounds

4.16 Definition. For any subset X of a poset $(P, \sqsubseteq)$ we define, for all $m \in P$:

(a) m is an *upper bound* of X if: $(\forall x : x \in X : x \sqsubseteq m)$

(b) m is a *lower bound* of X if: $(\forall x : x \in X : m \sqsubseteq x)$

$\square$

4.17 Properties.

(a) If P has a maximum $\top$ then $\top$ is an upper bound of every subset of P.

(b) If P has a minimum $\bot$ then $\bot$ is a lower bound of every subset of P.

(c) Every element in P is an upper bound and a lower bound of $\emptyset$.

(d) If it exists $\mathsf{max}\, X$ is an upper bound of X, for all $X \subseteq P$.

(e) If it exists $\mathsf{min}\, X$ is a lower bound of X, for all $X \subseteq P$.

$\square$

For any subset $X \subseteq P$ we can consider the set $\{ m \in P \mid (\forall x : x \in X : x \sqsubseteq m) \}$ of *all* upper bounds of X. This set may or may not have a minimum. If it has a minimum, this minimum is called the *supremum* of X, notation $\mathsf{sup}\, X$. Alternatively, it is sometimes also called X's *least upper bound*, notation $\mathsf{lub}\, X$.

Similarly, we can consider the set $\{ m \in P \mid (\forall x : x \in X : m \sqsubseteq x) \}$ of *all* lower bounds of X. This set may or may not have a maximum. If it has a maximum, this maximum is called the *infimum* of X, notation $\mathsf{inf}\,X$. Alternatively, it is sometimes also called X's *greatest lower bound*, notation $\mathsf{glb}\,X$.

By combination of the definitions of maximum/minimum and of upper/lower bounds we can define supremum and infimum in a more direct way.

4.18 Definition. For any subset X of a poset $(P, \sqsubseteq)$ we define, for all $m \in P$:

(a) m is X's *supremum* if both:

$(\forall x : x \in X : x \sqsubseteq m)$, and:

$(\forall x : x \in X : x \sqsubseteq z) \;\Rightarrow\; m \sqsubseteq z$, for all $z \in P$.

Notice that the first requirement expresses that m is an upper bound of X, and that the second one expresses that m is under all upper bounds of X.

(b) m is X's *infimum* if both:

$(\forall x : x \in X : m \sqsubseteq x)$, and:

$(\forall x : x \in X : z \sqsubseteq x) \;\Rightarrow\; z \sqsubseteq m$, for all $z \in P$.

□

4.19 Example.

- For a set V its power set $\mathcal{P}(V)$ – the set of all subsets of V – with relation $\subseteq$ is a poset, and any subset X of $\mathcal{P}(V)$ has a supremum, namely $(\bigcup_{U : U \in X} U)$,and an infimum, namely $(\bigcap_{U : U \in X} U)$.
- The set $\mathbb{N}^+$ of positive natural numbers with relation $|$ ("divides") is a poset. The supremum of two elements $a, b \in \mathbb{N}^+$ is their *least common multiple*, that is, the *smallest* of all positive naturals m satisfying $a|m$ and $b|m$; usually, this value is denoted by $lcm(a, b)$.

  Similarly, the greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the infimum of $\{a, b\}$.

□

4.20 Lemma. For poset $(P, \sqsubseteq)$ and for $p \in P$ we have: $\mathsf{sup}\{p\} = p$ and $\mathsf{inf}\{p\} = p$.

Proof. By Definition 4.18, to prove $\mathsf{sup}\{p\} = p$ we must prove:

$$
\begin{array}{ll}
 & (\forall x : x \in \{p\} : x \sqsubseteq p) \\
\Leftrightarrow & \quad \{ \text{ definition of } \{p\} \ \} \\
 & (\forall x : x = p : x \sqsubseteq p) \\
\Leftrightarrow & \quad \{ \text{ 1-pt. rule } \} \\
 & p \sqsubseteq p \\
\Leftrightarrow & \quad \{ \sqsubseteq \text{ is reflexive } \}
\end{array}
$$

$\quad$ true ,

and, for all $z \in P$:

$$
\begin{array}{ll}
 & (\forall x : x \in \{p\} : x \sqsubseteq z) \\
\Leftrightarrow & \quad \{ \text{ same steps as above } \} \\
 & p \sqsubseteq z \quad ,
\end{array}
$$

which is the desired result.
□

4.21 Lemma. Let $(P, \sqsubseteq)$ be a poset and $X \subseteq P$.

(a) If X has a maximum m, then $\mathsf{sup}\, X = m$.

(b) If $\mathsf{sup}\, X \in X$, then $\mathsf{sup}\, X$ is the maximum of X.

(c) If X has a minimum m, then $\mathsf{inf}\, X = m$.

(d) If $\mathsf{inf}\, X \in X$, then $\mathsf{inf}\, X$ is the minimum of X.

Proof.

(a) We have to prove that m satisfies the defining properties of $\mathsf{sup}\, X$. The first is that $\mathsf{sup}\, X$ is an upper bound, which follows from the definition of maximum. For the second assume that x is an upper bound of X, we have to prove that $m \sqsubseteq x$. This follows from the fact that $m \in X$ and the definition of upper bound.

(b) Immediate from the definitions.

(c) Similar to (a).

(d) Immediate from the definitions.

□

An important difference between supremum and maximum of a set is that a set's supremum may or may not be an element of that set, whereas a set's maximum always is an element of that set. The above lemma states, however, that if a set's supremum is in that set, then this supremum also is the set's maximum.

The following lemma provides a different but equivalent characterization of supremum and infimum that occasionally turns out to be very useful.

4.22 Lemma. Let X be a subset of a poset $(P, \sqsubseteq)$. For $m \in P$ we have:

(a) m is X's *supremum* if and only if:

$$(\forall z : z \in P : m \sqsubseteq z \Leftrightarrow (\forall x : x \in X : x \sqsubseteq z)) \quad .$$

(b) m is X's *infimum* if and only if:

$$(\forall z : z \in P : z \sqsubseteq m \Leftrightarrow (\forall x : x \in X : z \sqsubseteq x)) \quad .$$

Proof. We prove (a) only; the proof for (b) follows, mutatis mutandis, the same pattern. Firstly, we let m be X's supremum according to Definition 4.18. Then, for $z \in P$ we prove the equivalence of $m \sqsubseteq z$ and $(\forall x : x \in X : x \sqsubseteq z)$, by "cyclic implication":

$$
\begin{array}{ll}
& m \sqsubseteq z \\
\Leftrightarrow & \quad \{ \text{ Definition 4.18: } m \text{ is an upper bound of } X \ \} \\
& (\forall x : x \in X : x \sqsubseteq m) \ \ \wedge \ \ m \sqsubseteq z \\
\Rightarrow & \quad \{ \ \forall \text{ introduction } \} \\
& (\forall x : x \in X : x \sqsubseteq m) \ \ \wedge \ \ (\forall x : x \in X : m \sqsubseteq z) \\
\Leftrightarrow & \quad \{ \text{ combining terms } \} \\
& (\forall x : x \in X : x \sqsubseteq m \wedge m \sqsubseteq z) \\
\Rightarrow & \quad \{ \ \sqsubseteq \text{ is transitive } \} \\
& (\forall x : x \in X : x \sqsubseteq z) \\
\Rightarrow & \quad \{ \text{ Definition 4.18: } m \text{ is under all upper bounds } \} \\
& m \sqsubseteq z \quad .
\end{array}
$$

Secondly, let m satisfy:

(2) $\qquad (\forall z : z \in P : \ m \sqsubseteq z \Leftrightarrow (\forall x : x \in X : x \sqsubseteq z)\,) \quad .$

Then we must prove that m is X's supremum. Well, m is an upper bound:

$$
\begin{array}{ll}
& (\forall x : x \in X : x \sqsubseteq m) \\
\Leftrightarrow & \quad \{ \ (2)\text{ , with } z := m \ \} \\
& m \sqsubseteq m \\
\Leftrightarrow & \quad \{ \ \sqsubseteq \text{ is reflexive } \} \\
& \mathsf{true} \quad ,
\end{array}
$$

and that m is under all upper bounds follows directly from (2), because $\Leftrightarrow$ is stronger than $\Rightarrow$.
□

4.23 Properties.

(a) If P has a maximum $\top$ then $\top = \mathsf{sup}\, P$ and $\top = \mathsf{inf}\, \varnothing$.

(b) If P has a minimum $\bot$ then $\bot = \mathsf{inf}\, P$ and $\bot = \mathsf{sup}\, \varnothing$.

□

4.4 Lattices

4.4.1 Definition

In the previous section we have introduced the notions of *supremum* – least upper bound – and *infimum* – greatest lower bound – of subsets of a poset. Generally, such a subset does not always have a supremum or an infimum, just as, generally, not every subset has a maximum or a minimum. (Recall Lemma 4.21, for the relation between supremum and maximum, and between infimum and minimum, respectively.)

Partially ordered sets in which particular subsets do have suprema and/or infima are of interest, in particular "lattices" and "complete lattices".

4.24 Definition. A poset $(P, \sqsubseteq)$ is a *lattice*, if for all $x, y \in P$ the subset $\{x, y\}$ has a supremum and an infimum. Because this pertains to two-element sets, it is customary to use infix-notation to denote their suprema and infima. For these purposes binary operators $\sqcup$ ("cup") and $\sqcap$ ("cap") are used: the supremum of $\{x, y\}$ then is written as $x \sqcup y$ and its infimum as $x \sqcap y$.
□

4.25 Example. Here are some examples of lattices we already encountered before.

- $(\mathbb{R}, \leq)$ is a lattice. For $x, y \in \mathbb{R}$ we have: $x \sqcup y = x \,\mathsf{max}\, y$ and $x \sqcap y = x \,\mathsf{min}\, y$.
- For a set V the poset $(\mathcal{P}(V), \subseteq)$ is a lattice, with $\sqcup = \cup$ and $\sqcap = \cap$.
- The poset $(\mathbb{N}^+, |)$ is a lattice, with $a \sqcup b = lcm(a, b)$, the least common mulitple, and $a \sqcap b = gcd(a, b)$, the greatest common divisor.

□

The following lemma actually is a special case of Lemma 4.22, namely for nonempty subsets with *at most two* elements; that is, this is Lemma 4.22 with $X := \{x, y\}$.

4.26 Lemma. In every lattice $(P, \sqsubseteq)$ we have, for all $x, y, z \in P$:

(a) $x \sqcup y \sqsubseteq z \;\Leftrightarrow\; x \sqsubseteq z \wedge y \sqsubseteq z$;

(b) $z \sqsubseteq x \sqcap y \;\Leftrightarrow\; z \sqsubseteq x \wedge z \sqsubseteq y$.

□

Actually, this lemma can serve as an *alternative definition* of $\sqcup$ and $\sqcap$, as the original definition follows from it. As a special case, we obtain the following lemma, expressing that $x \sqcup y$ is an upper bound and that $x \sqcap y$ is a lower bound.

4.27 Lemma. In every lattice $(P, \sqsubseteq)$ we have, for all $x, y \in P$:

(a) $x \sqsubseteq x \sqcup y \wedge y \sqsubseteq x \sqcup y$;

(b) $x \sqcap y \sqsubseteq x \wedge x \sqcap y \sqsubseteq y$.

Proof. Instantiate Lemma 4.26 with $z := x \sqcup y$ and $z := x \sqcap y$, respectively.
□

4.28 Lemma. In every lattice $(P, \sqsubseteq)$ we have, for all $x, y \in P$:

(a) $x \sqsubseteq y \;\Leftrightarrow\; x \sqcup y = y$;

(b) $x \sqsubseteq y \;\Leftrightarrow\; x \sqcap y = x$.

Proof. We prove (a) only, by calculation:

$$
\begin{array}{ll}
 & x \sqcup y = y \\
\Leftrightarrow & \quad \{ \sqsubseteq \text{ is reflexive and antisymmetric } \} \\
 & x \sqcup y \sqsubseteq y \;\wedge\; y \sqsubseteq x \sqcup y \\
\Leftrightarrow & \quad \{ x \sqcup y \text{ is an upper bound of } y \} \\
 & x \sqcup y \sqsubseteq y \\
\Leftrightarrow & \quad \{ \text{Lemma 4.26, with } z := y \} \\
 & x \sqsubseteq y \;\wedge\; y \sqsubseteq y \\
\Leftrightarrow & \quad \{ \sqsubseteq \text{ is reflexive } \} \\
 & x \sqsubseteq y
\end{array}
$$

□

4.4.2 Algebraic properties

The lattice operators have interesting algebraic properties, as reflected by the following theorem.

4.29 Theorem. Let $(P, \sqsubseteq)$ be a lattice. Then for all $x, y, z \in P$ we have:

(a) $x \sqcup x = x$ and $x \sqcap x = x$: $\sqcup$ and $\sqcap$ are *idempotent*;

(b) $x \sqcup y = y \sqcup x$ and $x \sqcap y = y \sqcap x$: $\sqcup$ and $\sqcap$ are *commutative*;

(c) $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$ and $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$: $\sqcup$ and $\sqcap$ are *associative*;

(d) $x \sqcup (x \sqcap y) = x$ and $x \sqcap (x \sqcup y) = x$: *absorption*.

Proof.

(a) See Lemma 4.20.

(b) By symmetry: set $\{x, y\}$ equals set $\{y, x\}$.

(c) By (Lemma 4.6), for all $w \in P$:

$$
\begin{array}{ll}
 & x \sqcup (y \sqcup z) \ \sqsubseteq \ w \\
\Leftrightarrow & \quad \{ \text{ Lemma 4.26 } \} \\
 & x \sqsubseteq w \ \wedge \ y \sqcup z \sqsubseteq w \\
\Leftrightarrow & \quad \{ \text{ Lemma 4.26 } \} \\
 & x \sqsubseteq w \ \wedge \ y \sqsubseteq w \ \wedge \ z \sqsubseteq w \\
\Leftrightarrow & \quad \{ \text{ Lemma 4.26 } \} \\
 & x \sqcup y \sqsubseteq w \ \wedge \ z \sqsubseteq w \\
\Leftrightarrow & \quad \{ \text{ Lemma 4.26 } \} \\
 & (x \sqcup y) \sqcup z \ \sqsubseteq \ w \quad .
\end{array}
$$

(d) We prove $x \sqcup (x \sqcap y) \ = \ x$ only, by calculation:

$$
\begin{array}{ll}
 & x \sqcup (x \sqcap y) \ = \ x \\
\Leftrightarrow & \quad \{ \text{ Lemma 4.28 } \} \\
 & x \sqcap y \ \sqsubseteq \ x \\
\Leftrightarrow & \quad \{ \ x \sqcap y \text{ is a lower bound of } x \ \} \\
 & \mathsf{true} \quad .
\end{array}
$$

□

Conversely, the following theorem expresses that every structure with operators having the above algebraic properties “is” −can be extended into− a lattice.

4.30 Theorem. Let P be a set with two binary operators $\sqcup$ and $\sqcap$; that is, these operators have type $P \times P \to P$. Let these operators have algebraic properties (a) through (d), as in the previous theorem. Then the relation $\sqsubseteq$, on P and defined by $x \sqsubseteq y \ \Leftrightarrow \ x \sqcup y = y$ for all $x, y \in P$, is a partial order, and $(P, \sqsubseteq)$ is a lattice.
□

A direct consequence of Theorem 4.29, particularly of the associativity of the operators, is that every *finite* and *non-empty* subset of a lattice has a supremum and an infimum. Notice that the requirement “non-empty” is essential here: in a lattice the empty set may not have a supremum or infimum.

4.31 Theorem. Let $(P, \sqsubseteq)$ be a lattice. Then every finite and non-empty subset of P has a supremum and an infimum.

Proof. By Mathematical Induction on the size of the subsets, and using Theorem 4.29.
□

4.4.3 Distributive lattices

The prototype example of a lattice is the poset of all subsets of a set V, with $\subseteq$ as the partial order relation. As already mentioned, in this lattice set union, $\cup$, and intersection, $\cap$, are the binary lattice operators. In this particular lattice, the operators have an additional algebraic property, namely (mutual) *distributivity*; that is, "$\cup$ distributes over $\cap$" and "$\cap$ distributes over $\cup$", respectively:

$$X \cup (Y \cap Z) \;=\; (X \cup Y) \cap (X \cup Z) \quad \text{, for all } X,Y,Z \subseteq V \quad ;$$

$$X \cap (Y \cup Z) \;=\; (X \cap Y) \cup (X \cap Z) \quad \text{, for all } X,Y,Z \subseteq V \quad .$$

Generally, lattices do *not* have these properties. They do satisfy, however, a weaker version of these properties, namely "in one direction" only.

4.32 Theorem. Let $(P, \sqsubseteq)$ be a lattice. Then for all $x,y,z \in P$ we have:

(a) $x \sqcup (y \sqcap z) \;\sqsubseteq\; (x \sqcup y) \sqcap (x \sqcup z)$;

(b) $(x \sqcap y) \sqcup (x \sqcap z) \;\sqsubseteq\; x \sqcap (y \sqcup z)$.

Proof.

(a) By calculation:

$$\begin{array}{ll}
 & x \sqcup (y \sqcap z) \;\sqsubseteq\; (x \sqcup y) \sqcap (x \sqcup z) \\
\Leftrightarrow & \qquad \{ \text{ Lemma 4.26(b) } \} \\
 & x \sqcup (y \sqcap z) \sqsubseteq x \sqcup y \quad \wedge \quad x \sqcup (y \sqcap z) \sqsubseteq x \sqcup z \\
\Leftrightarrow & \qquad \{ \text{ Lemma 4.26(a) (twice) } \} \\
 & x \sqcup x \sqcup y \;\wedge\; y \sqcap z \sqsubseteq x \sqcup y \;\wedge\; x \sqsubseteq x \sqcup z \;\wedge\; y \sqcap z \sqsubseteq x \sqcup z \\
\Leftrightarrow & \qquad \{ \text{ Lemma 4.27(a) (twice) } \} \\
 & y \sqcap z \sqsubseteq x \sqcup y \;\wedge\; y \sqcap z \sqsubseteq x \sqcup z \\
\Leftarrow & \qquad \{ \sqsubseteq \text{ is transitive (twice) } \} \\
 & y \sqcap z \sqsubseteq y \;\wedge\; y \sqsubseteq x \sqcup y \;\wedge\; y \sqcap z \sqsubseteq z \;\wedge\; z \sqsubseteq x \sqcup z \\
\Leftrightarrow & \qquad \{ \text{ Lemma 4.27(a) (twice) and Lemma 4.27(b) (twice) } \} \\
 & \mathsf{true} \quad .
\end{array}$$

(b) By duality.

□

As we have seen, some lattices –like $(\mathcal{P}(V), \subseteq)$– do satisfy the distribution properties. Such lattices are called "distributive".

4.33 Definition. A *distributive lattice* is a lattice $(P, \sqsubseteq)$ in which $\sqcup$ and $\sqcap$ distribute over each other; that is, for all $x, y, z \in P$:

(a) $x \sqcup (y \sqcap z) \;=\; (x \sqcup y) \sqcap (x \sqcup z)$;

(b) $x \sqcap (y \sqcup z) \;=\; (x \sqcap y) \sqcup (x \sqcap z)$.

□

4.34 Example. Not every lattice is distributive. The smallest example illustrating this has 5 elements $\top, a, b, c, \bot$, say, with this partial order: $\bot$ is under all elements, a, b, c are under $\top$ and are mutually incomparable. (See the Hasse diagram in Figure 21.) In this lattice $a \sqcup (b \sqcap c) \;=\; a$ whereas $(a \sqcup b) \sqcap (a \sqcup c) \;=\; \top$.

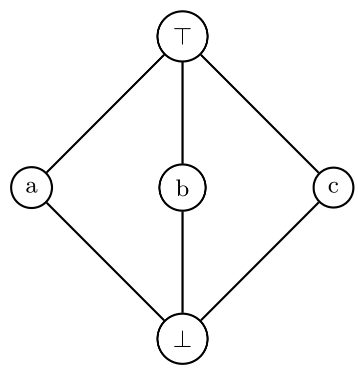


Figure 21: The smallest non-distributive lattice

4.4.4 Complete lattices

4.35 Definition. A *complete lattice* is a partial order in which *every* subset has a supremum and an infimum. In particular, the whole set has a supremum and an infimum, usually denoted by $\top$ and $\bot$, respectively. Notice that $\top$ and $\bot$ also are the lattice's maximum and minimum. (Recall Property 4.23.)
□
In computer science complete lattices are often used to give precise definitions of several concepts, like semantics of a programming language. A key result that we do not present here is that in a complete lattice every *monotone fucntion* $f : P \to P$, that is, $x \sqsubseteq y \Rightarrow f(x) \sqsubseteq f(y)$, has a *least fixed point*, that is, $\{x \mid f(x) = x\}$ has a minimum.

4.36 Lemma. Every *finite* lattice is complete.

Proof. Let $(P, \sqsubseteq)$ be a finite lattice. By Theorem 4.31 this lattice is *almost* complete already: every non-empty subset has a supremum and an infimum, so all we must do is prove that $\emptyset$ has a supremum and an infimum. From Property 4.23 we know that

$\mathsf{sup}\,\emptyset\ =\ \bot$ and $\mathsf{inf}\,\emptyset\ =\ \top$.

□

4.37 Example. The power set $(\mathcal{P}(V)\,,\subseteq)$ of all subsets of a set V is a complete lattice. The supremum of a set X of subsets of V is the union of all sets in X, which is $(\bigcup_{U:U\in X} U)$; its infimum is the intersection of all its elements, which is $(\bigcap_{U:U\in X} U)$.

□

4.38 Example. The poset $(\mathbb{R}, \leq)$ is a lattice, but it is not complete, but every *closed* interval $[\,a\,,b\,]$, with $a\leq b$ and with the same partial order $\leq$, is a complete (sub)lattice.

□

Completeness is a strong property, so strong, actually, that we only have to prove half of it: if every subset has an infimum then it also has a supremum, so if every subset has an infimum the partial order is a complete lattice. This is stated in the next theorem.

4.39 Theorem. Let $(P, \sqsubseteq)$ be a poset. Then:

(a) "Every subset of P has an infimum" $\Rightarrow$ "$(P, \sqsubseteq)$ is a complete lattice" ;

(b) "Every subset of P has a supremum" $\Rightarrow$ "$(P, \sqsubseteq)$ is a complete lattice" .

Proof. We prove (a) only. To prove this we assume that every subset of P has an infimum. Then, to prove that $(P, \sqsubseteq)$ is complete we only must prove that every subset of P has a supremum. So, let X be a subset of P. We define a subset Y by $Y\ =\ \{\,y\in P \mid (\forall x : x\in X : x\sqsubseteq y)\,\}$, that is, Y is the set of all upper bounds of X. Now let $m = \mathsf{inf}\,Y$. We prove that this m is X's supremum.

"m is an upper bound of X":

$$
\begin{array}{ll}
 & (\forall x : x\in X : x\sqsubseteq m) \\
\Leftarrow & \quad \{\ m \text{ is } Y\text{'s } \textit{greatest} \text{ lower bound}\ \} \\
 & (\forall x : x\in X : (\forall y : y\in Y : x\sqsubseteq y)\,) \\
\Leftrightarrow & \quad \{\ \text{exchanging dummies}\ \} \\
 & (\forall y : y\in Y : (\forall x : x\in X : x\sqsubseteq y)\,) \\
\Leftrightarrow & \quad \{\ \text{definition of } Y\ \} \\
 & (\forall y : y\in Y : y\in Y) \\
\Leftrightarrow & \quad \{\ \text{predicate calculus}\ \} \\
 & \mathsf{true}\ \ .
\end{array}
$$

"m is under all upper bounds of X": For any $y\in P$ we derive:

$$
\begin{array}{ll}
 & (\forall x : x\in X : x \sqsubseteq y) \\
\Leftrightarrow & \quad \{ \text{ definition of } Y \ \} \\
 & y \in Y \\
\Rightarrow & \quad \{ \ m \text{ is a lower bound of } Y \ \} \\
 & m \sqsubseteq y \quad .
\end{array}
$$

□

remark: In the proof of this theorem we introduced set Y as the set of *all* upper bounds of X. It is possible that X has no upper bounds, in which case Y is *empty*. This is harmless, because if *every* subset has an infimum then so has the empty set. Thus, this proof crucially depends on the property that also the empty set has an infimum. Recall that in a non-complete lattice the empty set does not need to have an infimum or supremum. (Also see the discussion preceding Theorem 4.31.)

□

4.5 Exercises

1. Consider the poset $(\mathbb{N}^+, \mid)$. Let $A = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
   (a) Establish all minimal and maximal elements of A.
   (b) Give a subset of four elements of A that has a maximum.
   (c) Give a subset of four elements of A that has a minimum.
2. Give an example of a poset that has exactly one maximal element, but not a maximum element.
3. Draw the Hasse diagram of
   $$\{X \subseteq \{1, 2, 3, 4\} \mid 2 \in X \vee 3 \notin X\}$$
   with respect to the partial order $\subseteq$.
4. Let $(P, \sqsubseteq)$ be a poset. Recall that for all $x, y \in P$:
   $$x \sqsubset y \ \Leftrightarrow \ x \sqsubseteq y \ \wedge \ x \neq y \quad .$$
   Prove that the relation $\sqsubset$ is irreflexive, antisymmetric, and transitive.
5. Let $(P, \sqsubseteq)$ be a poset. Prove that for all $x, y \in P$:
   (a) $x \sqsubseteq y \ \Leftrightarrow \ (\forall z : z\in P : x \sqsubseteq z \Leftarrow y \sqsubseteq z)$;
   (b) $x \sqsubseteq y \ \Leftrightarrow \ (\forall z : z\in P : z \sqsubseteq x \Rightarrow z \sqsubseteq y)$.

6. Let $(P, \sqsubseteq)$ be a poset and X a subset of P. Prove that an element $m \in X$ is maximal if and only if for all $x \in X$ we have $m \sqsubseteq x \Rightarrow m = x$.

7. A poset $(U, \sqsubseteq)$ is given with two subsets X and Y for which $\sup(X)$ and $\sup(Y)$ exist, and $\sup(X) \in Y$. Prove that $\sup(Y)$ is an upper bound of X.

8. Let $(U, \sqsubseteq)$ be a poset and $f : U \to U$ a function. Define the relation $\leq$ on U by

$$x \leq y \iff f(x) \sqsubseteq f(y).$$

   (a) Prove that $(U, \leq)$ is a poset if f is injective.
   (b) Give an example of a poset $(U, \sqsubseteq)$ and a non-injective function $f : U \to U$ such that $(U, \leq)$ is not a poset.

9. Consider the poset $(\mathbb{N}^+, \mid)$.

   (a) Establish the supremum and the infimum of $\{1, 2, 3, 4, 5\}$.
   (b) Establish the supremum and the infimum of $\{1, 2, 3, 4, 6, 12\}$.
   (c) Establish the supremum and the infimum of $\{3, 4, 5, 15, 20, 60\}$.
   (d) Establish the supremum and the infimum of $\{3, 4, 5, 12\}$.
   (e) Establish the supremum and the infimum of the set of all even numbers.

   For all set also establish whether the set has a minimum and/or a maximum.

10. Let $(U, \sqsubseteq)$ be a poset. Two sets $A, B \subseteq U$ are given, for which $\sup(A)$ exists, and for which $b \in B$ is minimal in B and $\sup(A) \sqsubseteq b$. Prove that $A \cap B \subseteq \{b\}$.

11. Let $(P, \sqsubseteq)$ be a lattice and $x, y, z \in P$. Prove that:

   (a) $x \sqsubseteq y \;\Rightarrow\; x \sqcup z \sqsubseteq y \sqcup z$;
   (b) $x \sqsubseteq z \;\Rightarrow\; z \sqcup (x \sqcap y) = z$.

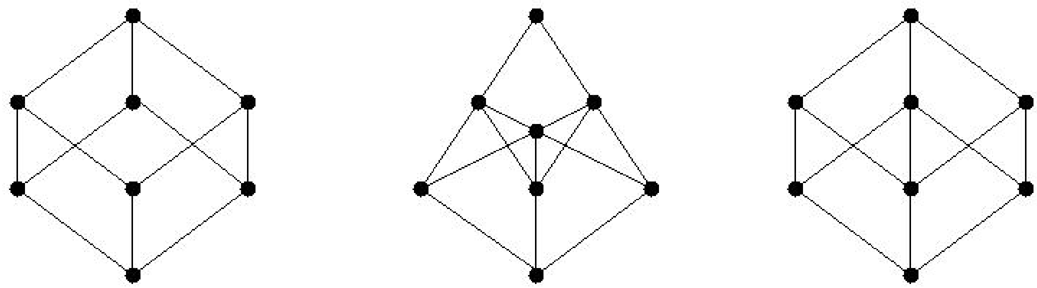
12. We consider the poset $(\mathbb{Q}, \leq)$.

   (a) Prove that the set $\{x \in \mathbb{Q} \mid x < 1\}$ has no maximum.
   (b) Prove that this set has a supremum.

13. We consider a poset $(P, \sqsubseteq)$; let X and Y be subsets of P such that $\mathsf{sup}\, X$ and $\mathsf{inf}\, Y$ both exist. In addition it is given that $x \sqsubseteq y$, for all $x \in X$ and $y \in Y$. Prove that $\mathsf{sup}\, X \sqsubseteq \mathsf{inf}\, Y$.

14. We consider a poset $(P, \sqsubseteq)$; let X be a subset of P.

   (a) Prove that if X contains two (different) maximal elements then X has no maximum.
   (b) Prove that if $(\forall x, y : x, y \in X : x \sqsubseteq y \vee y \sqsubseteq x)$ and if X contains a maximal element then X has a maximum.



15. In the figure below you see three diagrams. Which of these diagrams are Hasse diagrams? Which of these diagrams represents a lattice?
16. Show that every lattice with *at most* 4 elements is distributive.
17. Is the poset $(\mathbb{N}^+, |)$ a complete lattice? How about $(\mathbb{N}, |)$?
18. Suppose $(P, \sqsubseteq)$ is a lattice and $a, b \in P$ with $a \sqsubseteq b$. Prove that $([a,b], \sqsubseteq)$ is a lattice too. Here $[a,b]$ denotes the interval from (and including) a upto (and including) b; how would you define this interval?
19. Let $(P, \sqsubseteq)$ be a lattice. Prove that if $\sqcup$ distributes over $\sqcap$ then $\sqcap$ also distributes over $\sqcup$.
20. Prove that, in a complete lattice $(P, \sqsubseteq)$, the extreme element $\top$ is the identity element of $\sqcap$ and a zero element of $\sqcup$. Similarly, show that $\perp$ is the identity of $\sqcup$ and a zero of $\sqcap$.

5 Monoids and Groups

5.1 Operators and their properties

We consider a set V. A *binary operator on* V is a function of type $V \times V \rightarrow V$, so such a function maps pairs of elements of V to elements of V. Very often, applications of a binary operator are written in *infix-notation*, that is, the function's name is written *in between* the arguments.

In this chapter we use $*$ to denote any operator on a set V. Using infix-notation, we write the application of $*$ to pair $(x, y) \in V \times V$ as $x * y$ (instead of the more standard *prefix-notation* $*(x, y)$).

Sometimes binary operators have special properties, which deserve to be named.

5.1 Definition. Let $*$ be a binary operator on a set V. Then $*$ is called:

- *idempotent*, if for all $x \in V$ we have: $x * x = x$;
- *commutative*, if for all $x, y \in V$ we have: $x * y = y * x$;
- *associative*, if for all $x, y, z \in V$ we have: $(x * y) * z = x * (y * z)$;

□

5.2 Examples.

(a) On $\mathbb{N}$ addition, $+$, and multiplication, $*$, are binary operators; both are commutative and associative but not idempotent.

(b) On $\mathbb{Z}$ addition, $+$, and subtraction, $-$, are binary operators. Subtraction is neither idempotent, nor commutative, nor associative.

(c) On $\mathbb{Z}$ maximum, max, and minimum, min, are binary operators; both are idempotent, commutative, and associative.

(d) On the set of finite lists concatenation, $+\!\!+$, is a binary operator; it is neither idempotent nor commutative but it is associative.

(e) On the set of all relations relation composition, $;$, is an associative binary operator; as a special case, so is function composition, $\circ$, on the set of all functions.

□

For an associative operator $*$, the expressions $(x * y) * z$ and $x * (y * z)$ are equal and, therefore, we may safely omit the parentheses and write $x * y * z$ instead. Thus we do not only save a little writing, we also avoid the choice between two forms that are equivalent. Therefore, particularly with associative operators it pays to use infix-notation. With prefix-notation no parentheses can be omitted and we are always forced to decide whether to write $*(x, *(y, z))$ or $*(*(x, y), z)$: a rather irrelevant choice!

More important than the possibility to omit parentheses, however, is that associativity offers a *manipulative* opportunity in proofs: if we have a formula of the shape $(x*y)*z$ and if $*$ is associative then we may reposition the parentheses and obtain $x*(y*z)$ (and vice versa). So, even if we have omitted the parentheses we better stay aware of their (hidden) presence and of the opportunity to reposition them. We will see examples of this.

5.3 Definition. Let $*$ be a binary operator on a set V. An element $I{\in}V$ is called $*$'s *identity (element)* if it satisfies, for all $x{\in}V$:

$$x*I = x \;\wedge\; I*x = x \quad .$$

□

Not every binary operator has an identity element but every operator has *at most one* identity element; that is, if it exists an operator's identity element is unique.

5.4 Lemma. Let I and J both be identity elements of binary operator $*$ on a set V. Then $I=J$.

Proof. By calculation:

$$\begin{array}{ll} & I \\ = & \quad \{\ J \text{ is identity element, with } x := I\ \} \\ & I*J \\ = & \quad \{\ I \text{ is identity element, with } x := J\ \} \\ & J \quad . \end{array}$$

□

5.5 Examples.

(a) On $\mathbb{N}$ and $\mathbb{Z}$ the identity element of $+$ is 0, and the identity of $*$ is 1.

(b) On $\mathbb{N}^+$ operator $+$ has no identity element.

(c) On $\mathbb{Z}$ operator $-$ has no identity element.

(d) On $\mathbb{Z}$ operators max and min have no identity elements; on $\mathbb{N}$, however, the identity element of max is 0 whereas min still has no identity element.

(e) On the set of finite lists the identity element of $+\!\!+$ is $[\,]$ −the *empty* list−.

(f) The identity element of both relation composition and function composition is the identity relation/function, I.

□

Sometimes we are interested in the relation between two (or even more) binary operators. Although we do not elaborate this in this text, we mention one property that already has been used extensively in previous chapters.

5.6 Definition. Let $*$ and $+$ (say) be binary operators on a set V. Then we say that $*$ *distributes (from the left) over* $+$ if, for all $x,y,z \in V$:

$$x*(y+z) \;=\; (x*y)+(x*z) \quad .$$

Similarly, $*$ *distributes (from the right) over* $+$ if, for all $x,y,z \in V$:

$$(y+z)*x \;=\; (y*x)+(z*x) \quad .$$

Of course, if $*$ is commutative the distinction between "left" and "right" disappears and we just say "distributes over". (This is the case for almost all examples we have seen, with relation composition as the most notable exception.)
□

5.7 Examples.

(a) On $\mathbb{N}$ and $\mathbb{Z}$ multiplication, $*$, distributes over addition, $+$, but addition does not distribute over multiplication.

(b) On $\mathbb{Z}$ operator max distributes over min and min distributes over max.

(c) On $\mathbb{Z}$ operator $+$ distributes over both max and min.

(d) On $\mathbb{N}$ operator $*$ distributes over both max and min, whereas this is not true on $\mathbb{Z}$.

(e) Set union, $\cup$, distributes over set intersection, $\cap$, and vice versa.

(f) Relation composition, $;$, distributes, from the left and from the right, over union of relations, $\cup$. (Recall that composition is not commutative.)

□

5.2 Semigroups and monoids

So-called *algebraic structures* are sets with operators having particular properties. The simplest such structure is called a *semigroup*, which is just a set with an associative operator.

5.8 Definition. Let $*$ be a binary operator on a set V. The pair $(V,*)$ is a *semigroup* if $*$ is associative.
□

If the operator in a semigroup has an identity element the structure already becomes a little more interesting.

5.9 Definition. A *monoid* is a triple $(V, *, I)$, where $*$ is an associative binary operator on set V, so $(V, *)$ is a semigroup, and I, $I \in V$, is the identity element of $*$.
□

5.10 Examples.

(a) $(\mathbb{N}, +, 0)$ is a monoid, whereas $(\mathbb{N}^+, +)$ is a semigroup but not a monoid.

(b) both $(\mathbb{N}, *, 1)$ and $(\mathbb{N}^+, *, 1)$ are monoids.

(c) Let $\mathcal{L}_*$ denote the set of all finite lists, and let $\mathcal{L}_+$ denote the set of all non-empty finite lists. Then $(\mathcal{L}_*, +\!\!+, [\,])$ is a monoid, whereas $(\mathcal{L}_+, +\!\!+)$ only is a semigroup.

(d) All relations on a set with operator $;$ and identity relation I form a monoid. Similarly, all functions on a set, with function composition and the identity function form a monoid too.

□

5.11 Definition. Let $(V, *, I)$ be a monoid. For all $x \in V$ and for all $n \in \mathbb{N}$ we define x^n recursively, as follows:

$$x^0 = I \ \wedge \ x^{n+1} = x * x^n \quad .$$

□

5.12 Lemma. Let $(V, *, I)$ be a monoid. For every $x \in V$ and for all $m, n \in \mathbb{N}$ we have: $x^{m+n} = x^m * x^n$.

Proof. The proof of this lemma was already given in the proof of Lemma 1.31 in the chapter on relations. In fact Lemma 1.31 is a special case of the current lemma for the monoid consisting of all relations on a set U and the monoid operation ';'. Since the proof of Lemma 1.31 only uses the monoid properties (identity and associativity) of ';', the same proofs holds for arbitrary monoids. □

5.13 Definition. Let $(V, *, I)$ be a monoid. For every $x \in V$ an element $y \in V$ is called an *inverse* of x (with respect to $*$) if and only if: $x * y = I \wedge y * x = I$.
□

An element of a monoid does not necessarily have inverses, but if it has an inverse, it is unique. This is stated by the following lemma.

5.14 Lemma. Let $(V, *, I)$ be a monoid. Let $x, y, z \in V$ satisfy:

$$y * x = I \ \wedge \ x * z = I \quad .$$

Then $y = z$.

Proof. By calculation:

$$
\begin{array}{ll}
 & y \\
= & \quad \{ \ I \text{ is identity of } * \ \} \\
 & y * I \\
= & \quad \{ \ x * z = I \ \} \\
 & y * (x * z) \\
= & \quad \{ \ * \text{ is associative } \} \\
 & (y * x) * z \\
= & \quad \{ \ y * x = I \ \} \\
 & I * z \\
= & \quad \{ \ I \text{ is identity of } * \ \} \\
 & z \quad .
\end{array}
$$

□

Notice that in the proof of this lemma we have only used $x * z = I$ $-z$ is a *right-inverse* of $x-$ and $y * x = I$ $-y$ is a *left-inverse* of $x-$, so, actually, we have proved that all left-inverses are equal to all right-inverses.

5.3 Groups

Algebraically, life becomes really interesting with *groups*. A group is a monoid in which every element has an inverse (with respect to the binary operator).

5.15 Definition. A *group* is a monoid $(V, *, I)$ satisfying, for all $x \in V$:

(3) $\qquad (\exists y : y \in V : x * y = I \wedge y * x = I) \quad .$

An *Abelian group* is a group in which, in addition, operator $*$ is commutative.
□

As a matter of fact requirement (3) is stronger than strictly necessary: either of the two conjuncts, $x * y = I$ or $y * x = I$, can be dropped without affecting the definition. It is only for practical reasons, and because we do not wish to destroy the symmetry, that we have included both.

5.16 Lemma. Let $(V, *, I)$ be a monoid satisfying, for all $x \in V$:

(4) $\qquad (\exists y : y \in V : x * y = I) \quad .$

Then $(V, *, I)$ is a group.

Proof. To prove that $(V, *, I)$ is a group we must prove (3) for all $x \in V$, while using (4) for all $x \in V$. So, let $x \in V$ and let, using (4), element $y \in V$ satisfy $x * y = I$. Now to prove (3) for this particular x it suffices to show that y also satisfies $y * x = I$. Let, using (4) once more but with $x := y$, element $z \in V$ satisfy $y * z = I$. Now we calculate:

$$
\begin{array}{ll}
 & x \\
= & \quad \{ \ I \text{ is identity of } * \ \} \\
 & x * I \\
= & \quad \{ \ y * z = I \ \} \\
 & x * (y * z) \\
= & \quad \{ \ * \text{ is associative } \} \\
 & (x * y) * z \\
= & \quad \{ \ x * y = I \ \} \\
 & I * z \\
= & \quad \{ \ I \text{ is identity of } * \ \} \\
 & z \ .
\end{array}
$$

So, we have $x = z$; now z satisfies $y * z = I$, and substituting x for z in this we obtain $y * x = I$, as required.
□

The definition of groups states that every element of the set has an inverse. From Lemma 5.14 we already know that, if an element has an inverse, this inverse is unique. The inverse of an element, of course, depends on that element. Therefore, from now onwards we denote the inverse of every element $x \in V$ by x^{-1}.

5.17 Definition. Let $(V, *, I)$ be a group. For every $x \in V$ its inverse, x^{-1}, satisfies:

$$x * x^{-1} = I \ \wedge \ x^{-1} * x = I \ .$$

□

In the proof of Lemma 5.16 we have introduced y as the inverse of x, and z as the inverse of y, and then we have proved $z = x$. So, as an additional result, we obtain the following lemma stating that the inverse of the inverse of an element is that element itself.

5.18 Lemma. Let $(V, *, I)$ be a group. Every $x \in V$ satisfies: $(x^{-1})^{-1} = x$.
□

5.19 Lemma. Let $(V, *, I)$ be a group. All $x, y \in V$ satisfy: $(x * y)^{-1} = y^{-1} * x^{-1}$.

Proof. Using associativity several times we obtain

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * I * x^{-1} = x * x^{-1} = I$$

and

$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * I * y = y^{-1} * y = I,$$

so $y^{-1} * x^{-1}$ is the inverse of $x * y$. □

5.20 Examples.

(a) Let $V = \{\mathsf{i}\}$ and let binary operator $*$ on V be defined by $\mathsf{i} * \mathsf{i} = \mathsf{i}$. Then $(V, *, \mathsf{i})$ is a group; this is the *smallest possible* group.

(b) $(\mathbb{Z}, +, 0)$ is an (Abelian) group.

(c) $(\mathbb{Q}^+, *, 1)$ and $(\mathbb{Q}\backslash\{0\}, *, 1)$ are (Abelian) groups.

(d) For any set V we consider the set of all *bijections* from V to V, here denoted by $V \leftrightarrow V$. Then $((V \leftrightarrow V), \circ, I)$ is a group; it is not Abelian. If V is *finite* the bijections in $V \leftrightarrow V$ are also called *permutations* and the group is called a *permutation group*.

(e) For a fixed positive natural number n we define operator $\oplus$, of type $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, by $x \oplus y = (x+y) \,\mathsf{mod}\, n$, for all $x, y \in \mathbb{Z}$. Then this operator also has type $[0..n) \times [0..n) \to [0..n)$, and $([0..n), \oplus, 0)$ is an Abelian group.

□

A group $(V, *, I)$ has the property that, for all $a, b \in V$, equations of the shape $x : a * x = b$ can be solved. The solution of such an equation even is unique:

$$
\begin{array}{ll}
 & a * x = b \\
\Rightarrow & \quad \{ \text{ Leibniz } \} \\
 & a^{-1} * (a * x) = a^{-1} * b \\
\Leftrightarrow & \quad \{ * \text{ is associative } \} \\
 & (a^{-1} * a) * x = a^{-1} * b \\
\Leftrightarrow & \quad \{ a^{-1} \text{ is } a\text{'s inverse } \} \\
 & I * x = a^{-1} * b \\
\Leftrightarrow & \quad \{ I \text{ is identity of } * \} \\
 & x = a^{-1} * b \quad ,
\end{array}
$$

which shows that every solution to the equation is equal to $a^{-1} * b$. Conversely, it also is easy to show that $a^{-1} * b$ is a solution indeed, because $a * (a^{-1} * b)$ is, indeed, equal to b.

This is the characteristic property of groups: a group is the simplest possible structure in which all equations of the shape $x : a * x = b$ can be solved.

5.21 Lemma. Let $(V, *, I)$ be a group. For all $x \in V$ and $n \in \mathbb{N}$ we have:

$$(x^{-1})^n = (x^n)^{-1}$$

Proof. We have to prove that $(x^{-1})^n * x^n = I = x^n * (x^{-1})^n$, for all n. We do this by induction on n.

For $n = 0$ this holds since $(x^{-1})^0 = I = x^0$. For the induction step assume the induction hypothesis $(x^{-1})^n * x^n = I = x^n * (x^{-1})^n$. Leaving associativity implicit, we obtain:

$$\begin{array}{rcll} (x^{-1})^{n+1} * x^{n+1} & = & (x^{-1})^n * x^{-1} * x * x^n & \text{(definition, Lemma 5.12)} \\ & = & (x^{-1})^n * I * x^n & \\ & = & (x^{-1})^n * x^n & \\ & = & I & \text{(induction hypothesis)} \end{array}$$

and

$$\begin{array}{rcll} x^{n+1} * (x^{-1})^{n+1} & = & x^n * x * x^{-1} * (x^{-1})^n & \text{(definition, Lemma 5.12)} \\ & = & x^n * I * (x^{-1})^n & \\ & = & x^n * (x^{-1})^n & \\ & = & I & \text{(induction hypothesis).} \end{array}$$

□

5.22 Definition. Let $(V, *, I)$ be a group. For all $x \in V$ and $n \in \mathbb{N}$ we define x^{-n} by:

$$x^{-n} = (x^{-1})^n$$

□

5.23 Lemma. Let $(V, *, I)$ be a group. For every $x \in V$ and for all $m, n \in \mathbb{Z}$ we have:

$$x^{m+n} = x^m * x^n$$

Proof. We give the proof by case analysis.

- If $m \geq 0$ and $n \geq 0$ the lemma coincides with Lemma 5.12.
- If $m \leq 0$ and $n \leq 0$ write $m' = -m \geq 0$ and $n' = -n \geq 0$, we obtain:

$$\begin{array}{rcll} x^{m+n} & = & x^{-(m'+n')} & \\ & = & (x^{m'+n'})^{-1} & \text{(Lemma 5.21)} \\ & = & (x^{n'} * x^{m'})^{-1} & \text{(Lemma 5.12)} \\ & = & (x^{m'})^{-1} * (x^{n'})^{-1} & \text{(Lemma 5.19)} \\ & = & x^{-m'} * x^{-n'} & \text{(Lemma 5.21)} \\ & = & x^m * x^n. & \end{array}$$

- If $m \geq 0$ and $n < 0$ we apply induction on m. For $m = 0$ it was already proved in the former case. The induction step proceeds as follows. In case $n = -1$ we obtain $x^{(m+1)+n} = x^m = x^m * I = x^m * x^{n+1}$, in case $n < -1$ then by the induction hypothesis we also obtain $x^{(m+1)+n} = x^{m+(n+1)} = x^m * x^{n+1}$. So writing $n' = -n > 0$ we derive

$$\begin{array}{rcll} x^{(m+1)+n} & = & x^m * x^{n+1} & \text{(just derived)} \\ & = & x^m * x^{1-n'} & \\ & = & x^m * (x^{-1})^{n'-1} & \text{(Lemma 5.21)} \\ & = & x^m * x * x^{-1} * (x^{-1})^{n'-1} & (x * x^{-1} = I) \\ & = & x^{m+1} * (x^{-1})^{n'} & \\ & = & x^{m+1} * x^{-n'} & \text{(Lemma 5.21)} \\ & = & x^{m+1} * x^n. & \end{array}$$

- If $m < 0$ and $n > 0$ we have $x^{-m-n} = x^{-n} * x^{-m}$ by the former case, yielding

$$\begin{array}{rcll} x^{m+n} & = & ((x^{m+n})^{-1})^{-1} & \text{(Lemma 5.18)} \\ & = & (x^{-m-n})^{-1} & \text{(Lemma 5.21)} \\ & = & (x^{-n} * x^{-m})^{-1} & \text{(observed above)} \\ & = & (x^{-m})^{-1} * (x^{-n})^{-1} & \text{(Lemma 5.19)} \\ & = & x^m * x^n & \text{(Lemma 5.21).} \end{array}$$

□

5.4 Subgroups

5.24 Definition. Let $(V, *, I)$ be a group and let U be a subset of V. If $(U, *, I)$ is a group this is called a *subgroup* of $(V, *, I)$.
□

To verify that $(U, *, I)$ is a subgroup we do not have to verify that $*$ is associative, that I is the identity element, and that group elements have inverses: these properties remain valid. But, we do have to verify that subset U is *closed* under the group operations, that is, to prove that $(U, *, I)$ is a subgroup we must prove the following three properties:

$(\forall x, y : x, y \in U : x * y \in U)$, and:

$I \in U$, and:

$(\forall x : x \in U : x^{-1} \in U)$.

5.25 Definition. Let $(V, *, I)$ be a group.

(a) If $a^i = I$ for some $a \in V$ and $i > 0$, then the smallest $i > 0$ for which $a^i = I$ is called the *order* of a.

(b) If $a \in V$ we define the subset U_a by $U_a = \{a^i \mid i \in \mathbb{Z}\}$. Then $(U_a, *, I)$ is a subgroup of $(V, *, I)$, called the subgroup *generated by* a.

(c) The group is called *cyclic* if V contains an element a such that the subgroup generated by a is the whole group, that is, $\{a^i \mid i \in \mathbb{Z}\} = V$.

□

5.26 Examples.

(a) In $(\mathbb{Z}, +, 0)$ the subset of the *even* integers, with $+$ and 0, form a subgroup. More generally, for any natural number n the subset of all *multiples of* n, with $+$ and 0, form a subgroup.

(b) $(\mathbb{Q}^+, *, 1)$ is a subgroup of $(\mathbb{Q} \backslash \{0\}, *, 1)$.

(c) Actually, in $(\mathbb{Z}, +, 0)$ the subgroup of all multiples of n, for some natural n, is the subgroup generated by n.

$\square$

5.27 Definition. A group $(V, *, I)$ is finite if its set V of elements is finite. For a finite group $(V, *, I)$ the *order* of the group $(V, *, I)$ is $\#V$.
$\square$

5.28 Examples.

(a) Let group $(V, *, I)$ be finite of order N and let this group be cyclic. Then V contains an element a, say, such that $V = \{ a^i \mid 0 \leq i < N \}$ and $a^N = I$.

(b) For positive natural n, the group $([0..n), \oplus, 0)$, with $\oplus$ as defined in Example 5.20 (e), has order n. This group is cyclic, as it is generated by 1.

$\square$

5.5 Cosets and Lagrange's Theorem

5.29 Definition. Let $(V, *, I)$ be a group and let $(U, *, I)$ be a subgroup. Then for every $a \in V$ the *left coset* of a is the subset $\{ a * y \mid y \in U \}$ and the *right coset* of a is the subset $\{ x * a \mid x \in U \}$. The left and right cosets of a are denoted by $a * U$ and $U * a$, respectively.
$\square$

Notice that U is a (left and right) coset too, because $I * U = U$ and $U * I = U$.

If $(V, *, I)$ is a group with subgroup $(U, *, I)$ and for fixed $a \in V$, we can define a function $\varphi : U \to V$ by $\varphi(x) = a * x$, for all $x \in U$. Then, the left coset $a * U$ just is the image of U under function φ, that is, in terms of lifted functions, we have $a * U = \varphi(U)$.

5.30 Lemma. Let $(V, *, I)$ be a group and let $(U, *, I)$ be a subgroup. For fixed $a \in V$ the function $\varphi : U \to a * U$, defined by $\varphi(x) = a * x$, for all $x \in U$, is bijective.

Proof. Because $a * U = \varphi(U)$ function φ is surjective. That φ is injective as well follows from, for all $x, y \in U$:

$$
\begin{array}{ll}
 & \varphi(x) = \varphi(y) \\
\Leftrightarrow & \quad \{ \text{ definition of } \varphi \ \} \\
 & a * x = a * y \\
\Rightarrow & \quad \{ \text{ Leibniz } \} \\
 & a^{-1} * (a * x) = a^{-1} * (a * y) \\
\Leftrightarrow & \quad \{ \ * \text{ is associative; definition of inverse; identity element } \} \\
 & x = y \quad .
\end{array}
$$

□

All subsets of a finite set are finite as well. Therefore, in a finite group $(V, *, I)$ every subgroup $(U, *, I)$ is finite too, and so are all (left and right) cosets of this subgroup. In this case we arrive at an important consequence of the above lemma.

Corollary: In a finite group $(V, *, I)$ with subgroup $(U, *, I)$ we have, for all $a \in V$, that $\#(a * U) = \#U$ and $\#(U * a) = \#U$. In words: in a finite group with a subgroup all cosets have the same size as the subgroup from which they are derived.

□

Because $I \in U$ we have $a \in a * U$, for all $a \in V$. For $a, b \in V$ one may well wonder how the cosets $a * U$ and $b * U$ are related. By careful analysis we can derive that these cosets either are disjoint or are the same, and it so happens that $a * U = b * U$ if and only if $a^{-1} * b \in U$. This gives rise to the following lemma.

5.31 Lemma. Let $(V, *, I)$ be a group and let $(U, *, I)$ be a subgroup. On V we define a relation $\sim$ by, for all $a, b \in V$: $a \sim b \Leftrightarrow a^{-1} * b \in U$. Then:

(a) $\sim$ is an equivalence relation;

(b) The left cosets $a * U$, for all $a \in V$, are the equivalence classes of $\sim$.

Proof. First we prove that $\sim$ is a equivalence relation:

- reflexive: for $a \in V$ we have $a^{-1} * a = I \in U$, so $a \sim a$.
- symmetric: for $a, b \in V$ satisfying $a \sim b$ we have $a^{-1} * b \in U$, so $b^{-1} * a = (a^{-1} * b)^{-1} \in U$, so $b \sim a$.
- transitive: for $a, b, c \in V$ satisfying $a \sim b$ and $b \sim c$ we have $a^{-1} * b \in U$ and $b^{-1} * c \in U$, so

  $$a^{-1} * c = a^{-1} * I * c = a^{-1} * (b * b^{-1}) * c = (a^{-1} * b) * (b^{-1} * c) \in U,$$

  so $a \sim c$.

Next we derive

$$\begin{aligned} x \in a * U \quad &\Leftrightarrow \quad (\exists u \in U : x = a * u) \\ &\Leftrightarrow \quad (\exists u \in U : a^{-1} * x = u) \\ &\Leftrightarrow \quad a^{-1} * x \in U \\ &\Leftrightarrow \quad a \sim x \\ &\Leftrightarrow \quad x \in [a], \end{aligned}$$

so $[a] = a * U$, proving (b). □

Now we are ready for our final theorem, which is due to the famous mathematician Joseph Louis Lagrange.

5.32 Theorem. [**Lagrange**] The order of every subgroup of a finite group is a divisor of the order of the whole group.

Proof. Let M be the order of the group and let N be the order of the subgroup. The equivalence classes of relation $\sim$, as defined in Lemma 5.31 , form a partitioning of V . Each of these classes – the left cosets – has size N due to Lemma 5.30 and Lemma 3.25. Because V is finite there are only finitely many such cosets: let K be the number of left cosets. Because these sets are mutually disjoint and because their union equals V we have $M = K * N$, hence N is a divisor of M .
□

5.6 Permutation Groups

5.6.1 Function restriction and extension

In this section we will be studying functions on intervals of the shape $[\,0\,..\,n\,)$, for positive naturals n . If f is a function on the interval $[\,0\,..\,n\,)$, then we wish to speak of the *restriction of* f to the interval $[\,0\,..\,m\,)$, for any naturals $m,n : 1 \leq m \leq n$; this is a function with domain $[\,0\,..\,m\,)$, and on this domain it has the same values as f . We denote this restriction as $f\lceil m$ – "f take m" –.

5.33 Definition. For function f on $[\,0\,..\,n\,)$ and for m with $1 \leq m \leq n$ the function $f\lceil m$, on $[\,0\,..\,m\,)$, is defined by:

$$(f\lceil m)\,(i) \;=\; f(i) \quad \text{, for all } i : 0 \leq i < m \quad .$$

□

Property: If f , on $[\,0\,..\,n\,)$, is injective then so is $f\lceil m$, for all $m,n : 1 \leq m \leq n$.
□

* * *

As a converse to function restriction we also have need of the possibility of *function extension*. If f is a function on $[\,0\,..\,n\,)$ then we wish to define a new function, on $[\,0\,..\,n{+}1\,)$, that coincides with f on $[\,0\,..\,n\,)$ and for which the value in n equals a pre-specified value v , say. We denote this function as $f \triangleleft v$ – "f snoc v" –.

5.34 Definition. For function f on $[\,0\,..\,n\,)$ and for any value v , the function $f \triangleleft v$, on $[\,0\,..\,n{+}1\,)$, is defined by:

$$\begin{aligned} (f \triangleleft v)\,(i) \;&=\; f(i) \quad \text{, for all } i : 0 \leq i < n \\ (f \triangleleft v)\,(n) \;&=\; v \end{aligned}$$

□

5.35 Lemma. Function f , on $[\,0\,..\,n{+}1\,)$, satisfies:

$$f \;=\; (f\lceil n) \triangleleft f(n) \quad ,$$

and function f, on $[\,0\,..\,n\,)$, and value v satisfy:

$$(f \triangleleft v)\lceil n \;=\; f \quad .$$

□

5.6.2 Continued Compositions

For any finite list fs of functions, all of the same type $V \to V$, we define the *continued composition* of (the functions in) list fs. Informally, if list fs has length k then the continued composition of fs is:

$$fs_0 \circ fs_1 \circ \cdots \circ fs_{k-1} \quad .$$

Formally, the continued composition of (finite) lists of functions can be defined as a function $\mathcal{C}$, say, such that $\mathcal{C}(fs)$ is the composition of the functions in fs. Function $\mathcal{C}$ can be defined recursively as follows, for all lists fs, gs of functions and for function f, all of type $V \to V$.

5.36 Definition.

$$\begin{array}{lll} \mathcal{C}([\,]) & = & I_V \\ \mathcal{C}([\,f\,]) & = & f \\ \mathcal{C}(fs +\!\!+ gs) & = & \mathcal{C}(fs) \circ \mathcal{C}(gs) \quad . \end{array} \tag{5}$$

□

Notice that we have defined $\mathcal{C}([\,]) = I_V$ here because I_V is the identity element of function composition: thus, we guarantee that rule (5) also holds if either fs or gs equals $[\,]$. Also notice that rule (5) is ambiguous: the decomposition of a list of functions as a concatenation $fs +\!\!+ gs$ of two lists fs and gs of functions is not unique, but, fortunately, this is harmless, because of the associativity of function composition: the result will be the same, independently of this decomposition. As a matter of fact, *lists* are the appropriate data structure here, because of this associativity and because function composition is *not* commutative.

5.6.3 Bijections

We recall that a *bijection* on a set V is a function in $V \to V$ that is both *injective* and *surjective*. Informally, this means that, for every $v \in V$, there is *exactly one* $u \in V$ satisfying $f(u) = v$: that f is injective means that, for every v, there is *at most one* such u, and that f is surjective means that, for every v, there is *at least one* such u. For any given set V, the bijections on V have the following properties:

- The identity function I_V is a bijection on V;
- If f and g are bijections on V then so is their composition $f \circ g$;

- If f is a bijection on V, then f has an inverse, f^{-1}, and f^{-1} is a bijection on V too.

From this we conclude that the bijections on V, with $\circ$ and I, form a group.

5.6.4 Permutations

For *finite* set V the bijections on V are also called *permutations of* V. In what follows we will restrict our attention to finite sets of a very particular shape, namely, initial segments of the natural numbers. That is, we consider nonempty intervals of the shape $[0..n)$, for $n:1\leq n$. In this section we denote the identity permutation on $[0..n)$ as I_n. Notice that there is only *one* permutation of $[0..1)$, namely I_1.

* * *

We will use $\mathcal{P}_n$ to denote the set of all permutations of $[0..n)$, for $n:1\leq n$. So, $\mathcal{P}_n$ is the subset of those functions in $[0..n)\rightarrow[0..n)$ that are bijections. In what follows, the requirement $1\leq n$ is left implicit. Hence, as permutations are bijections, we now have that $(\mathcal{P}_n, \circ, I_n)$ is a group, for every n.

* * *

Every permutation in $\mathcal{P}_n$ can be represented compactly by enumerating its values in a list of length n. That is, if $s\in\mathcal{P}_n$ then it is represented by the list $[s_0, s_1, \cdots, s_{n-2}, s_{n-1}]$. Notice that, because every permutation is a bijection, this list contains each of the naturals $i:0\leq i<n$ exactly once. For example $[0,1,2,3]$ is the identity permutation of $[0..4)$, and $[3,0,1,2]$ is the permutation that "rotates the elements of $[0..4)$ one place to the left".

If $s\in\mathcal{P}_{n+1}$ then s is a permutation of $[0..n{+}1)$; so, s is injective and, therefore, $s\lceil n$ also is injective on $[0..n)$. Function s also is surjective and if, in addition, $s_n=n$, then $s\lceil n$ also is surjective in $[0..n)\rightarrow[0..n)$. Hence, if (and only if) $s_n=n$ then $s\lceil n$ is a permutation in $\mathcal{P}_n$ as well. This is expressed by the following lemma.

5.37 Lemma. $(\forall s: s\in\mathcal{P}_{n+1} : s_n=n \Rightarrow s\lceil n\in\mathcal{P}_n)$.

□

Conversely, every permutation in $\mathcal{P}_n$ can be extended to a permutation in $\mathcal{P}_{n+1}$ in a simple way, namely by extending the function with value n.

5.38 Lemma. $(\forall s: s\in\mathcal{P}_n : s\triangleleft n\in\mathcal{P}_{n+1})$.

□

corollary: As a result of these lemmas and of Lemma (5.35) we have:

$$(\forall s: s\in\mathcal{P}_{n+1} : s_n=n \Rightarrow s=(s\lceil n)\triangleleft n) \quad ,$$

and:

$$(\forall s : s\in\mathcal{P}_n : s = (s\triangleleft n)\lceil n\,) \quad .$$

□

This shows that the subset of those permutations in $\mathcal{P}_{n+1}$ that map n to n is *isomorphic* to $\mathcal{P}_n$: the functions $(\lceil n)$ and $(\triangleleft\, n)$ are the bijections from that subset to $\mathcal{P}_n$ and back, respectively.

In what follows, therefore, we will identify the subset of the permutations in $\mathcal{P}_{n+1}$ that map n to n and $\mathcal{P}_n$, that is, we will leave the application of the bijections implicit. Thus, for every permutation $s\in\mathcal{P}_{n+1}$ with $s_n = n$ will also say that $s\in\mathcal{P}_n$ and, conversely, we consider every permutation in $\mathcal{P}_n$ to be a permutation in $\mathcal{P}_{n+1}$ as well.

5.6.5 Swaps

For $p,q\in[\,0\,..\,n\,)$ we define the permutation $p\leftrightarrow q$ – "p swap q" – as follows:

$$\begin{array}{lcll}
(p\leftrightarrow q)(p) & = & q & , \\
(p\leftrightarrow q)(q) & = & p & , \\
(p\leftrightarrow q)(i) & = & i & , \quad \text{for all } i : i\in[\,0\,..\,n\,) \wedge i\neq p \wedge i\neq q \quad .
\end{array}$$

So, $p\leftrightarrow q$ is the permutation that interchanges p and q and leaves everything else in place. Obviously, if $p=q$ then $p\leftrightarrow q = I_n$, so, if $p=q$ then $p\leftrightarrow q$ is not a true "swap", but it is a permutation nevertheless: it equals I_n . We are mainly interested in *proper* swaps, which are swaps $p\leftrightarrow q$ with $p\neq q$. In the literature proper swaps are also known as "transpositions".

convention: Because of the isomorphism discussed in the previous section we consider $p\leftrightarrow q$ to be a permutation in $\mathcal{P}_n$, for every n satisfying $p,q\in[\,0\,..\,n\,)$, without distinguishing these swaps notationally.

□

Property: Swapping p and q is symmetric in p and q , that is: $(p\leftrightarrow q) = (q\leftrightarrow p)$, for all p,q . Usually, we will, however, represent swaps uniquely, by confining ourselves to swaps $(p\leftrightarrow q)$ with $p<q$.

□

5.39 Lemma. Every swap is its own inverse; that is, for all $p,q\in[\,0\,..\,n\,)$ we have:

$$(p\leftrightarrow q)\circ(p\leftrightarrow q) \quad = \quad I_n \quad .$$

proof: Directly from the definitions of $\circ$ and $\leftrightarrow$.

□

The following property shows the effect of the composition of a permutation and a swap: the permutation $s\circ(p\leftrightarrow q)$ differs from s only in that s_p and s_q are interchanged.

Property (6) : For $s \in \mathcal{P}_n$ and for $p, q \in [\,0\,..\,n\,)$ we have:

$$\begin{array}{lcll} (\,s\circ(p\leftrightarrow q)\,)\,(p) & = & s_q & , \\ (\,s\circ(p\leftrightarrow q)\,)\,(q) & = & s_p & , \\ (\,s\circ(p\leftrightarrow q)\,)\,(i) & = & s_i & , \text{ for all } i : i\in[\,0\,..\,n\,) \wedge i\neq p \wedge i\neq q \quad . \end{array}$$

proof: Directly from the definitions of $\circ$ and $\leftrightarrow$.

□

5.40 Lemma. Every permutation is the continued composition of a finite sequence of swaps.

proof: The lemma states that, for every $n : 1\leq n$ and for every permutation in $\mathcal{P}_n$, there exists a finite list of swaps, the continued composition of which equals s . We prove this by Mathematical Induction on n .

base: The only permutation in $\mathcal{P}_1$ is I_1 , and I_1 , being the identity element of function composition, is the continued composition of $[\,]$.

step: Let $s\in\mathcal{P}_{n+1}$. Let p , $0\leq p<n$, be such that $s_p = n$. Then we have, by property (6) , that $(\,s\circ(p\leftrightarrow n)\,)\,(n) = n$, from which we conclude, using Lemma (5.37) , that $s\circ(p\leftrightarrow n) \in \mathcal{P}_n$. By Induction Hypothesis, let ss be a (finite) list of swaps the continued composition of which equals $s\circ(p\leftrightarrow n)$; so, we have: $\mathcal{C}\,(\,ss\,) = s\circ(p\leftrightarrow n)$. Now we derive:

$$\begin{array}{ll} & s \\ = & \quad \{\ I_n \text{ is identity of } \circ\text{; Lemma (5.39)}\ \} \\ & s\circ(p\leftrightarrow n)\circ(p\leftrightarrow n) \\ = & \quad \{\ \text{definition of } ss\ \} \\ & \mathcal{C}\,(\,ss\,)\circ(p\leftrightarrow n) \\ = & \quad \{\ \text{definition of } \mathcal{C}\ \} \\ & \mathcal{C}\,(\,ss\,)\circ\mathcal{C}\,(\,[\,(p\leftrightarrow n)\,]\,) \\ = & \quad \{\ \text{definition of } \mathcal{C}\ \} \\ & \mathcal{C}\,(\,ss \mathbin{+\!\!+} [\,(p\leftrightarrow n)\,]\,) \quad , \end{array}$$

from which we conclude that permutation s is the continued composition of the list $ss \mathbin{+\!\!+} [\,(p\leftrightarrow n)\,]$ of swaps.

□

The proof of this lemma also provides some information on the *length* of the list of swaps. The permutation I_1 is the continued composition of $[\,]$, which has length 0 , that is, $1-1$. If we now, by Induction Hypothesis, assume that list ss has length $n-1$, then list $ss \mathbin{+\!\!+} [\,(p\leftrightarrow n)\,]$ has length $(n+1)-1$. Thus, we conclude that every permutation in $\mathcal{P}_n$ is the composition of $n-1$ swaps.

Notice that, in the above proof, we have *not* distinguished the cases $p=n$ and $p\neq n$, as this is unnecessary: the given proof is valid for either case. If, however,

$p = n$ then $(p \leftrightarrow n)$ equals the identity and can, therefore, be omitted. As a result, we conclude that every permutation in $\mathcal{P}_n$ is the composition of *at most* $n-1$ swaps.

Finally, we note that the representation of a permutation by a list of swaps is not *unique*: every finite list of swaps represents some permutation, and one and the same permutation may be represented by very many different lists of swaps. In the following section, however, we will prove quite a surprising result: the permutations can be partitioned into two classes, which we will call "even permutations" and "odd permutations", and every swap changes the class of the permutation; that is, the composition of a permutation and a swap always is in the other class than the original permutation. As a consequence, every permutation is even if and only if it is the composition of an even number of swaps, *independently* of the actual composition!

5.6.6 Neighbor swaps

A special case of swaps are the, so-called, "neighbor swaps", which are swaps of the form $(p \leftrightarrow (p+1))$. As we will see, these provide useful stepping stones in the analysis of even and odd permutations, in the next subsection.

Just as every permutation can be composed from swaps, every swap, in turn, can be composed from neighbor swaps. To prove this we need the following lemma first.

5.41 Lemma. For every p, q with $0 \leq p < q$ we have:

$$(p \leftrightarrow (q+1)) \;=\; (q \leftrightarrow (q+1)) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q+1)) \quad .$$

proof: We prove this by showing that $(p \leftrightarrow (q+1))(i)$ is equal to $((q \leftrightarrow (q+1)) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q+1)))(i)$, for all $i : 0 \leq i$. This requires distinction of 4 cases: $i = p$, $i = q$, $i = q+1$, and all other values of i. We illustrate this for the case $i = q+1$; the other cases can be verified similarly:

$$
\begin{array}{ll}
 & ((q \leftrightarrow (q+1)) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q+1)))(q+1) \\
= & \qquad \{ \text{ Property (6) } \} \\
 & ((q \leftrightarrow (q+1)) \circ (p \leftrightarrow q))(q) \\
= & \qquad \{ \text{ Property (6) } \} \\
 & ((q \leftrightarrow (q+1)))(p) \\
= & \qquad \{ \text{ definition of } \leftrightarrow, \text{ using } p < q, \text{ so } p \neq q \text{ and } p \neq q+1 \ \} \\
 & p \\
= & \qquad \{ \text{ definition of } \leftrightarrow \ \} \\
 & ((p \leftrightarrow (q+1)))(q+1) \quad .
\end{array}
$$

□

This lemma shows that the swap $(p \leftrightarrow (q+1))$ can be defined recursively as the composition of $(p \leftrightarrow q)$ and 2 neighbor swaps $(q \leftrightarrow (q+1))$. As a result we obtain the following lemma, which turns out useful in the next subsection.

5.42 Lemma. Every swap $(p \leftrightarrow q)$, for p,q with $0 \le p < q$, is the continued composition of exactly $2*k+1$ neighbor swaps, where $k = q-1-p$. Notice that the number $2*k+1$ is *odd*.

proof: We prove this by Mathematical Induction on the value of k. The basis of the induction, of course, is the swap $(p \leftrightarrow (p+1))$, so $k=0$, which all by itself is a *single* neighbor swap. For p,q with $0 \le p < q$, the swap $(p \leftrightarrow (q+1))$ is, by Lemma (5.41), the composition of $(p \leftrightarrow q)$ and 2 neighbor swaps $(q \leftrightarrow (q+1))$. Hence, if, by Induction Hypothesis, $(p \leftrightarrow q)$ is the composition of $2*k+1$ neighbor swaps then $(p \leftrightarrow (q+1))$ is the composition of $2*(k+1)+1$ neighbor swaps.

□

Aesthetic aside: Because $(q \leftrightarrow (q+1)) = ((q+1) \leftrightarrow q)$, the formula in Lemma (5.41) can be rendered in a more *symmetric* way as:

$$(p \leftrightarrow (q+1)) \;=\; ((q+1) \leftrightarrow q) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q+1)) \quad .$$

For p,q with $0 \le p < q$, Lemma (5.42) can now be rendered, informally, as:

$$\begin{aligned}(p \leftrightarrow q) \;=\; & (q \leftrightarrow (q-1)) \circ ((q-1) \leftrightarrow (q-2)) \circ \cdots \circ ((p+2) \leftrightarrow (p+1)) \circ \\ & (p \leftrightarrow (p+1)) \circ \\ & ((p+1) \leftrightarrow (p+2)) \circ \cdots \circ ((q-2) \leftrightarrow (q-1)) \circ ((q-1) \leftrightarrow q) \quad .\end{aligned}$$

□

*   *   *

We are now ready to harvest the results of the above labor. To start with, we observe that the actual number of inversions in a permutation does not give much information, but this number being even or odd does. This we call the *parity* of a permutation.

5.43 Definition. For $s \in \mathcal{P}_n$ the *parity* of s is:

$$(\#i,j : 0 \le i < j < n : s_j < s_i) \;\mathsf{mod}\; 2 \quad .$$

□

If the parity of a permutation equals 0 we also call the permutation “even” and if its parity equals 1 we also call the permutation “odd”. Now the above analysis boils down to the following lemma.

5.44 Lemma. Composition of a permutation with a proper swap changes its parity.

□

By “repeated application” −that is, of course, by Mathematical Induction− of this lemma we obtain the following theorem.

5.45 Theorem. If a permutation equals the continued composition of a sequence of proper swaps, then its parity equals the parity of the number of swaps.

proof: By Mathematical Induction on the length of the sequences, using the previous lemma.
□

Notice that this theorem pertains to *all possible* ways in which a given permutation equals the continued composition of a sequence of proper swaps. As a consequence, if two different such sequences represent the same permutation, then their lengths have equal parities. So, an even permutation can only be composed from an even number of swaps and an odd permutation can only be composed from an odd number of swaps, independently of *how* the permutation is composed from swaps.

Having the same parity is an equivalence relation. This relation partitions $\mathcal{P}_n$ into two equivalence classes, containing the even and the odd permutations in $\mathcal{P}_n$, respectively. Recalling that $(\mathcal{P}_n, \circ, I_n)$ is a group, we now also obtain the following additional result.

5.46 Theorem. In the group $(\mathcal{P}_n, \circ, I_n)$ the subset of the even permutations, with $\circ$ and I_n, form a subgroup of $(\mathcal{P}_n, \circ, I_n)$. This means that:

a) I_n is even;

b) if s and t are even then so is $s \circ t$;

c) if s is even then so is s^{-1}.

proof: Left as an exercise.
□

5.7 Exercises

1. Prove that every group $(V, *, I)$ satisfies: $I^{-1} = I$.
2. Describe all groups with exactly 2 elements, with 3 elements, and with 4 elements.
3. Why is $(\mathbb{N}, +, 0)$ not a group?
4. Prove that in every group $(V, *, I)$ we have, for all $x \in V$ and $n \in \mathbb{N}$:
   $x^n = I \;\Leftrightarrow\; x^{-n} = I$.
5. Let $(M, *, I)$ be a monoid and let $a, b \in M$ satisfy $a^2 = b^3 = I$. Prove that $(a * b * a)^6 = I$.
6. For a fixed natural number p, $2 \leq p$, we define operator $\otimes$, of type $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, by $x \otimes y = (x * y) \,\mathsf{mod}\, p$, for all $x, y \in \mathbb{Z}$. Prove that:
   (a) $([0..p), \otimes, 1)$ is a monoid;
   (b) $([0..p), \otimes, 1)$ is not a group;
   (c) $([1..p), \otimes, 1)$ is a group if and only if p is a prime number.

7. What is, in a group $(V, *, I)$, the subgroup generated by I?

8. What is, in the group $(\mathbb{Q}\backslash\{0\}, *, 1)$, the subgroup generated by 2?

9. Why is $(\mathbb{Q}^-, *, 1)$ *not* a subgroup of $(\mathbb{Q}\backslash\{0\}, *, 1)$?

10. Show that $(\mathbb{Z}, +, 0)$ is cyclic.

11. We consider a group $(V, *, I)$. Prove that, for every non-empty subset $U \subseteq V$, the structure $(U, *, I)$ is a subgroup of $(V, *, I)$ if and only if:

$$(\forall x, y : x, y \in U : x * y^{-1} \in U) \quad .$$

12. We consider, for some positive natural n, the group $([0..n), \oplus, 0)$, with $\oplus$ as defined in Example 5.20 (e).

    (a) Prove that, for all positive natural m, the subgroup generated by m is the whole group if and only if m and n are relatively prime.

    (b) Identify all subgroups of this group.

13. Let $(G, *, I)$ be a group and let $a \in G$. Let $f : G \to G$ be the function defined by $f(x) = x * a$ for all $x \in G$. Prove that f is bijective.

14. Compute the order of each of the following permutations on $\{a, b, c, d, e\}$:

    (a) $\{(a, d), (b, e), (c, c), (d, a), (e, b)\}$.

    (b) $\{(a, a), (b, e), (c, b), (d, d), (e, c)\}$.

    (c) $\{(a, d), (b, b), (c, e), (d, c), (e, a)\}$.

    (d) $\{(a, b), (b, e), (c, a), (d, c), (e, d)\}$.

    (e) $\{(a, d), (b, e), (c, b), (d, a), (e, c)\}$.

15. Prove that there is no permutation on $\{a, b, c, d, e\}$ of order 8.

16. Prove that there is a permutation on $\{a, b, c, d, e, f, g, h\}$ of order 15.

17. (Warning: this exercise is quite hard) We consider a monoid $(M, *, I)$ with exactly 8 elements. M contains an element g, say, *of order* 7. This means that $g^7 = I$ and that $g^i \neq I$, for all $i : 1 \leq i < 7$.

    (a) Prove that M contains an element h, say, that is not a power of g.

    (b) Prove that such h satisfies $h * g = h$.

18. Identify all subgroups of the group of permutations on $\{1, 2, 3\}$.

19. Give an example showing that composition of swaps usually is not commutative. That is, give example values for k, l, p, q such that:
$(k \leftrightarrow l) \circ (p \leftrightarrow q) \neq (p \leftrightarrow q) \circ (k \leftrightarrow l)$.

20. Let a, b be elements of a group. Let a have order $n < \infty$. Prove that $b * a * (b^{-1})$ has order n.

21. Let f be a permutation on a finite set A, for which $a, b \in A$ exist such that $a \neq b$, $f(a) = b$ and $f(b) = a$. Prove that the order of f is even.

22. Let a, b be elements of a finite group. Prove that $a * b$ and $b * a$ have the same order.

6 Combinatorics: the Art of Counting

6.1 Introduction

Combinatorics is the branch of Mathematics in which methods to solve counting problems are studied. Here is a list of questions that are considered combinatorial problems. As we will see, some of these problems in this list may *look* different but actually happen to be (instances of) the *same* problem.

1. What is the number of sequences of length n and constructed from the symbols 0 and 1 only, for any given natural n?
2. What is the number of sequences of length n and constructed from the symbols 0 and 1 only, but containing no two 0's in succession, for any given natural n?
3. What is the number of subsets of a given finite set?
4. What is the number of elements of the Cartesian product of two given finite sets?
5. What is the number of possible Hungarian license plates for cars? (A Hungarian license plate contains three letters followed by three digits.)
6. What is the number of relations on a given finite set?
7. What is the number of sequences of length n and containing each of the numbers $0, 1, \cdots, n-1$ (exactly) once, for given $n: 1 \le n$?
8. What is the number of sequences of length n and containing different objects chosen from a given collection of m different objects, for given $n, m: 1 \le n \le m$?
9. What is the number of ways to select n objects from a given collection of m objects, for given $n, m: 1 \le n \le m$?
10. What is the number of numbers, in the decimal system, the digits of which are all different?
11. What is the number of "words" consisting of 5 letters?
12. What is the number of ways in which 5 pairs can be formed from a group of 10 persons?
13. What is the number of $n \times n$ matrices, all elements of which are 0 or 1? How many of these matrices have an odd determinant?
14. What is the number of steps needed to sort a given finite sequence?
15. What is the minimal number of "yes/no"-questions needed to determine which one out of a given (finite) set of possibilities is actually the case?

16. In a digital signaling system 8 wires are used, each of which may or may not carry a voltage. For the transmission of a, so-called, "code word" via these wires exactly 4 wires carry a voltage (and the other 4 wires carry no voltage). How many code words are thus possible?

To provide some flavor of the theory needed to answer these questions in a systematic way, we discuss some of these questions here, not necessarily to solve them already but, at least, to shed some light on them.

question 1:

What is the number of sequences of length n and constructed from the symbols 0 and 1 only, for any given natural n? Well, a sequence of n symbols has n positions, each of which may contain a 0 or a 1. So, each position admits 2 possibilities, and the choice at each position is *independent* from the choice at every other position. For $n=2$, for instance, we have a total of $2*2$ choices, whereas for $n=3$ we have a total of $2*2*2$ possibilities. Generally, for arbitrary n the number of possibilities is 2^n.

This is about the simplest possible counting problem. A systematic way to solve it, which is also applicable to more difficult problems, is by means of induction on n. The only sequence of length 0 is the "empty" sequence, of which there is only one. So, for $n=0$ the number of sequences equals 1. (And, if one wishes to avoid the notion of the empty sequence, one starts with $n=1$ and finds the answer 2, because there are only 2 sequences of length 1, namely consisting of a single symbol 0 or 1.) Next, a sequence of length $n+1$ can be viewed as the *extension* of a sequence of length n with an additional symbol, being 0 or 1. So, such an extension is possible in two ways, each yielding a new sequence. Hence, the number of sequences of length $n+1$ is twice the number of sequences of length n. Thus, we also arrive at the conclusion that the number of sequences of length n equals 2^n: for $n=0$, the number is 2^0, and each extension doubles the answer, with $2^n * 2 = 2^{n+1}$.

question 2:

What is the number of sequences of length n and constructed from the symbols 0 and 1 only, but containing no two 0's in succession, for any given natural n? This question is harder than the previous one, because of the restriction that the sequences contain no two 0's in succession: now different positions in the sequence are not independent anymore, and the question is not as easily answered as the previous one. As an abbreviation, we call the sequences constructed from the symbols 0 and 1 only, but containing no two 0's in succession, "admissible".

To answer this question it pays to introduce a *variable* – a name – for the answer. Because the answer depends on variable n, the parameter of the problem, we let this variable depend on n; that is, we make it a function on $\mathbb{N}$, as $n\in\mathbb{N}$. So, we say: let a_i be the number of admissible sequences of length i, for all $i\in\mathbb{N}$. Then a is the function, with type $\mathbb{N}\to\mathbb{N}$. This enables us to try to formulate an equation for a which, hopefully, we can solve.

For our current problem we reason as follows. The one and only sequence of length 0 is the empty sequence, and it is admissible: as it contains no 0's at all, it certainly contains no two 0's in succession. Thus, we decide that $a_0 = 1$. Next, for $i \in \mathbb{N}$, a sequence of length $i+1$ can now be obtained in two different ways: either by extending an admissible sequence of length i with a symbol 1, always resulting in an admissible sequence, or by extending an admissible sequence of length i with a symbol 0; this, however, yields an admissible sequence *only if* the sequence thus extended does not end with a 0 itself: if it did we would obtain two 0's in succession!

Hence, a new kind of sequences enter the game, namely "admissible sequences not ending with a symbol 0". Therefore, we introduce yet another name b, say: let b_i be the number of admissible sequences not ending with a symbol 0, for all $i \in \mathbb{N}$. Using b, we can now complete our equation for a; we obtain: $a_{i+1} = a_i + b_i$. Notice that, in this formula, a_i is the number of admissible sequences of length $i+1$ obtained by extending an admissible sequence with a symbol 1, and that b_i is the number of admissible sequences of length $i+1$ obtained by extending an admissible sequence, not ending in a 0, with a symbol 0; their sum, then, is the total number of admissible sequences of length $i+1$.

Thus we obtain the following equation for our function a:

$$\begin{array}{lcl} a_0 & = & 1 \\ a_{i+1} & = & a_i + b_i \quad \text{, for all } i \in \mathbb{N} \end{array}$$

This equation contains our new variable b and to be able to solve the equation we also need a similar equation for b. By means of precisely the same kind of reasoning we decide that the only admissible sequence, not ending in a 0, of length 0 is the empty sequence; hence, $b_0 = 1$. And, the only way to obtain an admissible sequence, not ending in a 0, of length $i+1$ is by extending an admissible sequence of length i with a symbol 1; so, $b_{i+1} = a_i$. Thus we obtain the following equation for our function b:

$$\begin{array}{lcl} b_0 & = & 1 \\ b_{i+1} & = & a_i \quad \text{, for all } i \in \mathbb{N} \end{array}$$

These two equations can now be combined into one set of equations for a and b together. Actually, they constitute a *recursive definition* for a and b, because, for any given $n \in \mathbb{N}$, they can be used as rewrite rules to calculate the values of a_n and b_n in a finite number of steps. Nevertheless, we also call this an "equation" because it does not give *explicit* expressions for a and b.

$$\begin{array}{lcl} a_0 & = & 1 \\ a_{i+1} & = & a_i + b_i \quad \text{, for all } i \in \mathbb{N} \\ b_0 & = & 1 \\ b_{i+1} & = & a_i \quad \text{, for all } i \in \mathbb{N} \end{array}$$

Because these equations pertain to functions on $\mathbb{N}$, and because of their recursive nature, they are also called *recurrence relations*. Recurrence relations of this and similar forms can be solved in a systematic way. This is the subject of a separate section.

question 3:

What is the number of subsets of a given finite set? Well, every element may or may not be an element of a subset: for every element of the given set we have a choice out of 2 possibilities, independently of (the choices for) the other elements. Therefore, if the given set has n elements, we have n independent choices out of 2 possibilities; hence, the number of subsets of a set with n elements equals 2^n .

Actually, this is the very same problem as the one in question 1. The elements of any finite set can be ordered into a finite sequence, and now every subset of it can be represented as a sequence of length n consisting of symbols 0 and 1 : a 1 in a given position encodes that the corresponding – according to the order chosen – element of the given set is an element of the subset, and a 0 in a given position encodes that the corresponding element of the given set is not an element of the subset. Thus, there is a one-to-one correspondence – that is: a bijection – between the set of all subsets of a given set of size n and the set of all sequences of length n consisting of symbols 0 and 1 . Thus, question 3 and question 1 are essentially the same, and so are their answers.

question 4:

What is the number of elements of the Cartesian product of two given finite sets? Let V and W be finite sets with m and n elements, respectively. The Cartesian product $V\times W$ is the set of all pairs (v,w) with $v\in V$ and $w\in W$. Because v can be chosen out of m elements, and because, independently, w can be chosen out of n elements, the number of possible pairs equals $m\times n$. So, we have: $\#(V\times W) = \#V * \#W$.

Similarly, the number of elements of the Cartesian product of *three* finite sets is the product of the *three* sizes of these sets: $\#(U\times V\times W) = \#U * \#V * \#W$, and so on. The following two questions contain applications of this.

question 5:

What is the number of possible Hungarian license plates for cars? (A Hungarian license plate contains three letters followed by three digits.) Each letter is chosen from the alphabet of 26 letters, and each digit is one out of 10 decimal digits. Actually, with A for the alphabet and with D for the set of decimal digits, a Hungarian license plate number is an element of the Cartesian product $A\times A\times A\times D\times D\times D$; hence, the number of possible combinations equals $\#A * \#A * \#A * \#D * \#D * \#D$, that is: $26^3 * 10^3$.

question 6:

What is the number of relations on a given finite set? A relation on a set V is a subset of the Cartesian product $V\times V$, so the number of relations on V equals the number of subsets of $V\times V$. If V has n elements then $V\times V$ has n^2 elements, so the number of relations equals 2^{n^2} .

question 7:

What is the number of sequences of length n and containing each of the numbers $0, 1, \cdots, n{-}1$ (exactly) once? Notice that the requirement "containing each of the numbers $0, 1, \cdots, n{-}1$ (exactly) once" is rather *over specific*: that it is about the numbers $0, 1, \cdots, n{-}1$ is not very relevant, all that matters is that the sequence contains n given *different* objects. The element in the first position can be chosen out of n possible objects, and this leaves only $n-1$ objects for the remainder of the sequence. Hence, the second element can be chosen out of these $n-1$ objects, and this, in turn, leaves $n-2$ objects for the (next) remainder of the sequence; and so on, until we are left with exactly one object to choose from for the last element of the sequence. Hence, the number of possible such sequences equals $n*(n{-}1)*(n{-}2)*\cdots*2*1$; this quantity is usually denoted as $n!$ – "n factorial" – .

Here, too, a recursive characterization is possible. The number of sequences of length 1, and containing one given object exactly once, equals 1. And, for any $n{\in}\mathbb{N}$, a sequence of length $n{+}1$ containing each of $n{+}1$ different objects exactly once can be constructed, firstly, by choosing one of these objects, which can be done in $n{+}1$ ways, and, secondly, by constructing a sequence of length n containing each of the remaining n objects exactly once; finally, the sequence thus obtained is extended with the single object chosen in the first step. We conclude that the number of sequences of length $n{+}1$ equals $n{+}1$ times the number of sequences of length n. Thus we arrive at this, well-known, recursive definition of $n!$:

$$\begin{array}{lcl} 1! & = & 1 \\ (n{+}1)! & = & (n{+}1)*n! \quad \text{, for all } n{\in}\mathbb{N}^+ \end{array}$$

question 8:

What is the number of sequences of length n and containing different objects chosen from a given collection of m different objects, for given $n, m : 1{\le}n{\le}m$? One way to approach this problem is to observe that the m given objects can be arranged into a sequence in $m!$ ways, as we have seen in the previous question. The first n objects of such a sequence then constitute a sequence of length n and containing different objects chosen from the given collection of m objects. The order of the remaining $m-n$ objects (in the sequence of length m), however, is completely irrelevant: these remaining objects can be ordered in $(m{-}n)!$ ways, so there are actually $(m{-}n)!$ sequences of length n, that all begin with the same n objects in the same order, and that only differ in the order of their last $m-n$ elements. So, to count the number of sequences of length n we have to *divide* the number of sequences of length m by $(m{-}n)!$. Thus we obtain as answer to our question: $m!/(m{-}n)!$.

question 9:

What is the number of ways to select m objects from a given collection of n objects, for given $m, n : 1{\le}m{\le}n$? One may well wonder if, and if so how, this question differs from the previous one. Well, the previous question was about *sequences*, whereas this question is about *sets*. The question can be rephrased as: What is the number of subsets of size n of a given set of size m, for given $n, m : 1 \le n \le m$? Well, every sequence of length n of the kind in the previous question represents such a subset, albeit that the order in which the objects occur in the sequence now is irrelevant. That is, every two sequences, of length n, containing the *same* objects in possibly *different* orders now represent the *same* subset. Actually, for every selection of n objects there are $n!$ sequences containing these objects and all representing the same subset. Hence, the number of ways to form a subset of size m from a given set of size n equals the answer to the previous question divided by $n!$. Thus we obtain: $m!/((m-n)! * n!)$. This quantity is called a *binomial coefficient* and it is usually denoted as $\binom{m}{n}$, which is defined by:

$$\binom{m}{n} \;=\; \frac{m!}{(m-n)! * n!} \quad .$$

Binomial coefficients happen to have interesting properties which we will study later.

question 10:

What is the number of numbers, in the decimal system, the digits of which are all different? Obviously, such a number consists of *at most* 10 digits. It is questionable whether we allow such a number to start with the digit 0: on the one hand, "0123" does represent a number in the decimal system, on the other hand, we usually do not write down such leading zeroes because they are meaningless: "0123" represents the same number as "123". So, let us *decide* to exclude meaningless leading zeroes. Then, the only number starting with the digit 0 is "0".

In this case, the problem is most easily solved by distinguishing the possible numbers according to their length. We have already observed that the length of our numbers is at most 10. For numbers consisting of a single digit we have 10 possibilities, as each of the 10 decimal digits is permitted. For numbers of length $n+1$, $1 \le n \le 9$, we can choose the first digit in 9 ways, 0 having been excluded as the first digit. Independently of how this first digit has been chosen we still have 9 digits left for the remaining n digits of the number, because now digit 0 is included again. So, for these remaining n digits the question becomes: what is the number of sequences of n digits, chosen from a set of 9 different digits? This question, however, is an instance of problem 8, with $m := 9$; hence, the answer to this question is $9!/(9-n)!$. Thus, we conclude that the number of numbers, in the decimal system, the digits of which are all different, is 10 single-digit numbers, and $9 * 9!/(9-n)!$ numbers consisting of $n+1$ digits, for $1 \le n \le 9$.

question 11:

What is the number of "words" consisting of 5 letters? This depends on what one considers a "word". If we are asking for the number of 5-letter words in a specific language the question is a linguistic question, not a mathematical one. So, let us decide that a “word” is just an arbitrary sequence consisting of letters from the 26-letter alphabet. Then, for every position in the sequence we have an independent choice out of 26 possibilities, so the number of 5-letter words equals 26^5.

Notice that this question is very similar to questions 1 and 4.

question 12:

What is the number of ways in which 5 pairs can be formed from a group of 10 persons? This question does not admit a simple, straightforward answer. Therefore, as in the discussion of question 2, we introduce a variable to represent it: let a_i be the number of ways in which i pairs can be formed from a group of $2*i$ persons, for all $i \in \mathbb{N}^+$. The original question, then, amounts to asking for the value of a_5.

For a group of 2 persons, the answer is quite simple: only one pair can be formed, so $a_1 = 1$. For a group of $2*(i{+}1)$ persons, which is equal to $2*i{+}2$, one person can be matched to $2*i{+}1$ other persons, and the remaining $2*i$ persons can then be arranged into pairs in a_i ways. Thus we obtain: $a_{i+1} = (2*i{+}1)*a_i$. Combining these results we obtain the following recurrence relations for a:

$$\begin{array}{lcl} a_0 & = & 1 \\ a_{i+1} & = & (2*i{+}1)*a_i \quad \text{, for all } i \in \mathbb{N}^+ \end{array}$$

So, informally, we have: $a_i = (2{*}i{-}1)*(2{*}i{-}3)*\cdots*3*1$, and the answer for a group of 10 persons is $9*7*5*3*1$. In some textbooks, the expression for a_i is denoted as $(2{*}i{-}1)!!$.

question 13:

What is the number of $n \times n$ matrices, all elements of which are 0 or 1? How many of these have an odd determinant? The first question has no relation to linear algebra. An $n \times n$ matrix has n^2 elements, each of which may be 0 or 1. Hence, the number of such matrices equals 2^{n^2}. This answer is the same as the answer to question 6, and this is no coincidence. Why?

The problem posed in the second question does belong to linear algebra. The answer, which we shall not explain here, is that the number of $n \times n$ $0/1$-matrices with an odd determinant is given by this nice formula:

$$(\Pi i : 0 \le i < n : 2^n - 2^i) \quad .$$

For $n = 3$, for example, we thus find 168 matrices with an odd determinant, and 344, namely: $2^{3^2} - 168$, with an even determinant.

question 16:

In a digital signaling system 8 wires are used, each of which may or may not carry a voltage. For the transmission of a, so-called, “code word” via these wires exactly 4 wires carry a voltage (and the other 4 wires carry no voltage). How many code words are thus possible? Every code words corresponds to a particular selection of 4 wires from the 8 available wires, so the number of possible code words equals the number of ways to select 4 objects out of a collection of 8. This is exactly question 9, with $n := 4$ and $m := 8$. Hence, the answer is $8!/(4!*4!)$, which equals 70.

6.2 Recurrence Relations

6.2.1 An example

In the introduction we have discussed this question: What is the number of sequences of length n and constructed from the symbols 0 and 1 only, but containing no two 0's in succession, for any given natural n? For the sake of brevity we have called such sequences "admissible".

To solve this problem we have introduced two functions, a and b, on $\mathbb{N}$, with the following interpretation, for all $i \in \mathbb{N}$:

$$
\begin{array}{lcl}
a_i & = & \text{“the number of admissible sequences of length } i \text{”} \text{, and:} \\
b_i & = & \text{“the number of admissible sequences of length } i \text{,} \\
 & & \text{not ending with a } 0 \text{”} \text{.}
\end{array}
$$

The answer to the above question then is a_n, and we already have formulated the following set of equations for a and b, also called *recurrence relations*:

$$
\begin{array}{lrcl}
(0) & a_0 & = & 1 \\
(1) & a_{i+1} & = & a_i + b_i \text{ , for all } i \in \mathbb{N} \\
(2) & b_0 & = & 1 \\
(3) & b_{i+1} & = & a_i \text{ , for all } i \in \mathbb{N}
\end{array}
$$

These recurrence relations form equations for *two* unknowns, namely a and b. We can, however, use (2) and (3) to *eliminate* b from equation (1): after all, we can view (2) and (3) as a definition for b in terms of a. Because of the case distinction between b_0 and b_{i+1} we must apply a similar case distinction to (1); that is, we must split (1) into separate equations for a_1 and a_{i+2}. In the equation for a_1 we can now substitute 1 for b_0 (and 1 for a_0), and in the equation for a_{i+2} we can now substitute a_i for b_{i+1}. Thus we obtain a new set of equations for a in which b does not occur anymore:

$$
\begin{array}{lrcl}
(4) & a_0 & = & 1 \\
(5) & a_1 & = & 2 \\
(6) & a_{i+2} & = & a_{i+1} + a_i \text{ , for all } i \in \mathbb{N}
\end{array}
$$

Thus, we have obtained a recurrence relation for a in isolation –that is, without b–; the "old" equations (2) and (3) can now be used to define b in terms of a, if so desired. That is to say, if we are able to derive an explicit –that is, non-recursive– definition for a then (2) and (3) provide an equally explicit definition for b in terms of a. Notice, however, the proviso "if so desired": we may very well be interested in b too, but our original problem was about a, and we have only introduced b as an additional, auxiliary variable to be able to formulate equation (1).

*   *   *

Equations (4) through (6) can be used to calculate as many values a_i as we like, preferably in the order of increasing i. For example, the first 7 values are:

i	a_i
0	1
1	2
2	3
3	5
4	8
5	13
6	21

We see that the values a_i, as a function of i, increase rather quickly. This is not so strange: equation (6) is very similar to the following, only slightly different, equation.

$$a_{i+2} \;=\; a_{i+1} + a_{i+1} \quad \text{, for all } i \in \mathbb{N} \quad ,$$

which is equivalent to $a_{i+2} = 2 * a_{i+1}$. Now for this equation, together with (4) and (5), it is quite easy to *guess* that the solution might be $a_i = 2^i$, for all $i \in \mathbb{N}$, and, once we have guessed this, it requires only ordinary Mathematical Induction to prove that our guess is correct.

In our case, however, we have to deal with equation (6). Because of the smaller index, i instead of $i{+}1$, in one of the terms of the right-hand side, we suspect that the solution does not increase as quickly as 2^i, but, perhaps, it still increases exponentially? This idea deserves further investigation. Notice that we have tacitly decided to confine our attention to equation (6), and to ignore, at least for the time being, equations (4) and (5).

6.2.2 The characteristic equation

The last considerations give rise to the idea to investigate solutions of the form $\gamma * \alpha^i$ (for a_i), for some, non-zero, constants γ and α yet to be determined. To investigate this we substitute this expression for a_i in equation (6), such that we can try to calculate solutions for γ and α:

$$\gamma * \alpha^{i+2} \;=\; \gamma * \alpha^{i+1} + \gamma * \alpha^i \quad \text{, for all } i \in \mathbb{N} \quad .$$

Firstly, we observe that, unless $\gamma = 0$, which would make the equation useless, this equation does not really depend on γ; for every $\gamma \neq 0$, this equation is equivalent to the following one:

$$\alpha^{i+2} = \alpha^{i+1} + \alpha^i \quad \text{, for all } i \in \mathbb{N} \quad .$$

Although this equation has to be met, for one-and-the-same α, for *all* natural i, this is not as bad as it may seem; for $\alpha \neq 0$, this equation, in turn, is equivalent to the following one, in which i does not occur anymore:

$$\alpha^2 = \alpha^1 + \alpha^0 \quad .$$

Using that $\alpha^0 = 1$ and bringing all terms to one side of the equality we rewrite the equation into this form:

(7) $$\alpha^2 - \alpha^1 - 1 = 0 \quad .$$

This is called the *characteristic equation* of recurrence relation (6). What we have obtained now is the knowledge that if the solution to (6) is to be of the shape $\gamma * \alpha^i$ then α must satisfy (7).

Equation (7) is a quadratic one with two solutions α_0 and α_1, say, given by:

(8) $$\alpha_0 = (1+\sqrt{5})/2 \text{ and: } \alpha_1 = (1-\sqrt{5})/2 \quad .$$

Apparently, we have two possibilities for α here, so $a_i = \alpha_0^i$ and $a_i = \alpha_1^i$ are both solutions to our original equation (6), but there is more. We recall equation (6):

(6) $$a_{i+2} = a_{i+1} + a_i \quad \text{, for all } i \in \mathbb{N} \quad .$$

As we will discuss more extensively later, this is a so-called *linear* and *homogeneous* recurrence relation, which has the property that any *linear combination* of solutions is a solution as well. In our case, this means that for all possible constants γ_0 and γ_1, the definition:

(9) $$a_i = \gamma_0 * \alpha_0^i + \gamma_1 * \alpha_1^i \quad \text{, for all } i \in \mathbb{N} \quad ,$$

provides a solution to equation (6). In fact, it can be proved that *all* solutions have this shape, so now we have obtained *all* solutions to equation (6).

Recurrence relations (4) through (6), however, which also constitute a recursive definition for a, suggest that the solution should be *unique*. After all, we are able to construct a table containing the values a_i, for increasing i, as we did in the previous section. So, which one out of the infinitely many solutions of the shape given by (9) is the one we are looking for? This means: what should be the values of constants γ_0 and γ_1 such that we obtain the correct solution? To answer this question we have to consider equations (4) and (5) again, the ones we have temporarily ignored:

(4) $$a_0 = 1$$
(5) $$a_1 = 2$$

If we now instantiate (9), with $i := 0$ and $i := 1$, and using that $\alpha^0 = 1$ and $\alpha^1 = \alpha$, for any α, we obtain these two special cases:

$$a_0 = \gamma_0 + \gamma_1 \text{ and: } a_1 = \gamma_0 * \alpha_0 + \gamma_1 * \alpha_1 \quad .$$

By substituting these values for a_0 and a_1 into equations (4) and (5) we obtain the following two new equations, in which γ_0 and γ_1 are the unknowns now:

$$\begin{aligned} \gamma_0 + \gamma_1 &= 1 \\ \gamma_0 * \alpha_0 + \gamma_1 * \alpha_1 &= 2 \end{aligned}$$

With γ_0 and γ_1 as the unknowns, these are just two linear equations that can be solved by standard algebraic means. In this case we obtain:

$$\gamma_0 \;=\; (2-\alpha_1)/(\alpha_0-\alpha_1) \quad \text{and:} \quad \gamma_1 \;=\; (\alpha_0-2)/(\alpha_0-\alpha_1) \quad ,$$

where α_0 and α_1 are given, above, by definition (8). Thus we obtain, for all $i\in\mathbb{N}$:

(10) $$a_i \;=\; ((3+\sqrt{5}\,)/2\sqrt{5}\,)*((1+\sqrt{5}\,)/2)^i \;+\; ((\sqrt{5}-3)/2\sqrt{5}\,)*((1-\sqrt{5}\,)/2)^i \;.$$

The sequence $f_0, f_1, f_2, \ldots$ defined by

$$f_0 = 0, f_1 = 1, f_{n+2} = f_{n+1} + f_n \;\text{ for } n \geq 0$$

is usually called the *Fibonacci sequence*, named after Fibonacci, also called Leonardo from Pisa, who lived from around 1170 to around 1250. This sequence has many applications in computer science. It is closely related to the sequence a_i inverstigated above, in fact $a_i = f_{i+2}$ for all $i \geq 0$. In the same way as above one derives

$$f_i \;=\; \frac{(1+\sqrt{5}/2)^i - (1-\sqrt{5}/2)^i}{\sqrt{5}}$$

for all $i \geq 0$. Note that $(1+\sqrt{5}\,)/2 \approx 1.618$ and $(1-\sqrt{5}\,)/2 \approx -0.618$, so $(1-\sqrt{5}/2)^i$ converges very quickly to 0, and up to a constant f_i is roughly equal to $(1.618)^i$ for larger i, which grows exponentially.

6.2.3 Linear recurrence relations

The recurrence relation studied in the previous section belongs to a class of recurrence relations known as *linear recurrence relations* with *constant coefficients*. They are called linear because function values, like a_{i+2}, are defined as linear combinations of other function values, like a_{i+1} and a_i in (6). Notice that equation (6) can be written, slightly more explicitly, as:

$$a_{i+2} \;=\; 1*a_{i+1} + 1*a_i \quad \text{, for all } i\in\mathbb{N} \quad .$$

Any formula of the shape $c_0*x_0 + c_1*x_1 + c_2*x_2 + \cdots$ is called a linear combination of the xs, with the cs being the coefficients. In the case of recurrence relations, we speak of constant coefficients if they *do not depend* on i. For example, in our example the coefficients, of a_{i+1} and a_i, are 1 and 1, respectively, which, indeed, do not depend on i.

The general shape of a linear recurrence relation with constant coefficients is the following one, in which the c_j are the coefficients, for all $j : 0 \leq j < k$, $c_0 \neq 0$, and in which k is a constant called the *order* of the recurrence relation:

(11) $$a_{i+k} \;=\; c_{k-1}*a_{i+k-1} + \cdots + c_1*a_{i+1} + c_0*a_i \quad \text{, for all } i\in\mathbb{N}.$$

So, in a k-th order recurrence relation value a_{i+k} is defined recursively in terms of its k direct predecessors, which are $a_{i+k-1}, \cdots, a_{i+1}, a_i$, only.

Relation (11) defines a_{i+k} recursively in terms of $a_{i+k-1}, \cdots, a_{i+1}, a_i$, as a linear combination, for all $i \in \mathbb{N}$, but it does not define the first k elements of function a; that is, relation (11) gives no information on the values $a_{k-1}, \cdots, a_1, a_0$. These values, therefore, may be, and must be, defined separately. So, a complete k-th order recurrence relation consists of relation (11) together with k separate definitions for the values a_i, for all $i : 0 \le i < k$. These definitions also are known as the *initial conditions* of the recurrence relation.

* * *

Relation (11) is *homogeneous*, which means that if α_i is a solution for a_i, then so is $\gamma * \alpha_i$, for any constant γ. Relation (11) is *linear*, which means that if α_i and β_i both are solutions for a_i, then so is $\alpha_i + \beta_i$. Combining these two observations we conclude that any linear combination of solutions to (11) is a solution as well. Note that this conclusion *only* pertains to equation (11) in isolation, so without regard for the initial conditions. If the initial conditions are taken into account the recurrence relation has only one, unique, solution.

As in the example before, we now investigate to what extent equation (11) admits solutions of the shape α^i for a_i. Notice that, because of the homogeneity, we do not need to incorporate a constant coefficient: as was the case with the solution to the example −Section 6.2.2−, this coefficient will drop out of the equation anyhow. Substitution of α^i for a_i in (11) transforms it into the following equation for α:

$$\alpha^{i+k} \;=\; c_{k-1} * \alpha^{i+k-1} + \cdots + c_1 * \alpha^{i+1} + c_0 * \alpha^i \quad \text{, for all } i \in \mathbb{N} \quad .$$

As we are looking for solutions with $\alpha \neq 0$, this equation can be further simplified into this, equivalent, form:

$$(12) \qquad \alpha^k - c_{k-1} * \alpha^{k-1} \;\cdots\; - c_1 * \alpha - c_0 * 1 \;=\; 0 \quad .$$

Now α^i is a solution for a_i in equation (11) if and only if α is a solution to equation (12), which, as before, is called the *characteristic equation* of the recurrence relation. Notice that this is an algebraic equation of the same order as the order of the recurrence relation.

* * *

The simplest case arises when the k-th order characteristic equation has k *different* real roots, α_j, say, for $j : 0 \le j < k$. Then, any linear combination of the powers of these roots, that is, for all possible coefficients γ_j, with $0 \le j < k$, function a defined by:

$$(13) \qquad a_i \;=\; (\Sigma j : 0 \le j < k : \gamma_j * \alpha_j^i) \quad \text{, for all } i \in \mathbb{N} \quad ,$$

is a solution to (11). Moreover, not only does this yield just *a* solution to (11), it can even be proved that *all* solutions are thus characterized.

As stated before, when the k initial conditions, that is, the defining relations for a_i, for $0 \le i < k$, are taken into account, the solution to the recurrence relation is unique. This means that if the values for a_i, for $0 \le i < k$, have been given, and once the α_j, for $0 \le j < k$ haven been solved from (11), definition (13), for all $i : 0 \le i < k$, is not a definition anymore but a *restriction* on the possible values for γ_j. That is, the set of relations:

$$(\Sigma j : 0 \le j < k : \gamma_j * \alpha_j^i) \;=\; a_i \quad \text{, for all } i : 0 \le i < k \quad ,$$

now constitutes a system of k linear equations with unknowns γ_j, with $0 \le j < k$, from which these can be solved by means of standard linear-equation solving techniques.

* * *

A somewhat more complicated situation arises if the characteristic equation has *multiple* roots. A simple example of this phenomenon is the equation:

$$\alpha^2 - 2.8 * \alpha + 1.96 \;=\; 0 \quad ,$$

which can be rewritten as:

$$(\alpha - 1.4)^2 \;=\; 0 \quad .$$

This means that both roots α_0 and α_1 are equal to 1.4.

In a general k-th order algebraic equation a root may have a, so-called, multiplicity upto k. It can now be proved that, if a certain root α_p, say, has, multiplicity q, say, then α_p^i, $i * \alpha_p^i$, $i^2 * \alpha_p^i$, $\cdots$, $i^{q-1} * \alpha_p^i$ are q independent solutions for a_i in equation (11). These q different solutions account for the multiplicity, also q, of root α_p. Thus, in total we still obtain k different basis solutions from which linear combinations can be formed to obtain, again, *all* solutions of the recurrence relation.

As a simple example, the characteristic equation:

$$\alpha^2 - 2.8 * \alpha + 1.96 \;=\; 0 \quad ,$$

has a single root, 1.4, with multiplicity 2. Hence, all solutions to the (homogeneous) recurrence relation of which this is the characteristic equation are of the form $\gamma_0 * 1.4^i + \gamma_1 * i * 1.4^i$.

* * *

The situation becomes even more complicated if the characteristic equation has less than k, possibly multiple, roots in $\mathbb{R}$: then the equation still has k roots, but some (or all) of them are complex numbers. A very simple example is the equation:

$$\alpha^2 - \alpha + 1 \;=\; 0 \quad .$$

As the determinant, namely $1-4$, of this equation is negative, this equation has no roots in $\mathbb{R}$ at all, but it has two complex numbers as its roots: $(1+\sqrt{-3})/2$ and $(1-\sqrt{-3})/2$, which are usually written as –with $i=\sqrt{-1}$ –: $(1+i*\sqrt{3})/2$ and $(1-i*\sqrt{3})/2$.

These complex roots can be used, in the same way as described earlier, to obtain all solutions to the recurrence relation. Although, definitely, there is quite some mathematical beauty in this, such solutions are not very useful from a practical point of view. In Subsection **??** we present a more computational way to cope with such situations.

6.2.4 Summary

Summarizing, for solving a recurrence relation of the shape

$$a_0 = n_0, a_1 = n_1, a_{i+2} = c_1 a_{i+1} + c_0 a_i \text{ for all } i \in \mathbb{N}$$

for given numbers n_0, n_1, c_0, c_1, we have the following approach:

- First ignore the requirements $a_0 = n_0, a_1 = n_1$ and try to find a solution of $a_{i+2} = c_1 a_{i+1} + c_0 a_i$ of the shape $a_i = \alpha^i$ for all i. This yields the characteristic equation $\alpha^2 = c_1\alpha + c_0$.
- Find the two solutions α_0 and α_1 of this equation, now for every two numbers A, B, the expression $a_i = A\alpha_0^i + B\alpha_1^i$ is a solution of the equation. The numbers α_0 and α_1 may be real or complex numbers. In case $\alpha_0 = \alpha_1$, then the expression $a_i = A\alpha_0^i + Bi\alpha_0^i$ is a solution of the equation.
- Finally, find values for A, B such that $a_0 = n_0, a_1 = n_1$ hold.

We observe that if $n_0, n_1, c_0, c_1 \in \mathbb{N}$ then we will obtain $a_i \in \mathbb{N}$ for all i. In particular, this holds for counting problems as in our introduction, which are only about natural numbers. For integer n_0, n_1, c_0, c_1 the result will always be integer. In the mean time we have obtained a solution of the form (10), in which both α_0, α_1, and the coefficients A, B are defined in terms of true –non-integer, even irrational– real numbers like $\sqrt{5}$, or even complex numbers. Apparently, however complicated the resulting formula is, its value is a natural number nevertheless. Isn't that strange?

We conclude that even for problems that are purely about natural or integer numbers, it turns out to be fruitful to make an excursion into $\mathbb{R}$ or $\mathbb{C}$ to be able to find a closed expression for the solution of the problem.

6.3 Binomial Coefficients

6.3.1 Factorials

We already have seen that the product $n*(n-1)*(n-2)*\cdots*2*1$ is denoted as $n!$ –"n factorial"–, for any $n \in \mathbb{N}^+$. Even for $n=0$ this product is meaningful: then it is the *empty* product, consisting of 0 factors, for which the best possible definition is the identity element of multiplication, that is: 1. A recursive definition for $n!$ is:

$$
\begin{array}{lcl}
0! & = & 1 \\
(n{+}1)! & = & (n{+}1) * n! \quad \text{, for all } n{\in}\mathbb{N}
\end{array}
$$

Factorials occur in solutions to many counting problems. In Section 6.1 we already have argued that the number of ways to arrange n given, different objects into a sequence of length n equals $n!$. Here we repeat the argument, in a slightly more precise way. We do this recursively; for this purpose, we introduce a function a on $\mathbb{N}$ with the idea that:

$$
\begin{array}{ll}
a_i = & \text{“the number of sequences of length } i \text{, containing } i \text{ different objects”} \text{ ,} \\
& \text{for all } i{\in}\mathbb{N} \text{ .}
\end{array}
$$

The number of ways to arrange 0 different objects into a sequence of length 0 equals 1, because the only sequence of length 0 is the empty sequence, and it contains 0 objects. So, we conclude: $a_0 = 1$. Next, to arrange $i{+}1$ different objects into a sequence of length $i{+}1$ we can, firstly, select one object that will be the first element of the sequence, and, secondly, arrange the remaining i objects into a sequence of length i. The first object can be selected in $i{+}1$ different ways and, independently, the remaining i objects can be arranged in a_i ways into a sequence of length i. So, we obtain: $a_{i+1} = (i{+}1) * a_i$. Thus, we obtain as recurrence relation for a:

$$
\begin{array}{lcl}
a_0 & = & 1 \\
a_{i+1} & = & (i{+}1) * a_i \quad \text{, for all } i{\in}\mathbb{N}
\end{array}
$$

The solution to this recurrence is $a_i = i!$, for all $i{\in}\mathbb{N}$.

Notice that, while we are speaking here of “different objects”, their actual nature is irrelevant: all that matters is that they are different. Actually, we even have used this tacitly in the above argument: after we have selected one object from a collection of $i{+}1$ different objects, the remaining collection, after removal of the object selected, is a collection of i different objects, independently of which object was selected to be removed.

* * *

A slightly more complicated problem we also have discussed in Section 6.1 was: what is the number of ways to select and arrange n different objects from a given collection of m different objects into a sequence of length n, for given $n, m : 0{\leq}n{\leq}m$?

One way to approach this problem is to observe that, as we now know, the m given objects can be arranged into a sequence in $m!$ ways. The first n objects of such a sequence then constitute a sequence of length n that contains n different objects chosen from the given collection of m objects. The order of the last $m{-}n$ objects (in the sequence of length m), however, is completely irrelevant: these remaining objects can be ordered in $(m{-}n)!$ ways without affecting the first n objects in the sequence, so there are actually $(m{-}n)!$ sequences of length n, that all begin with the same n objects in the same order, and that only differ in the order of their last $m{-}n$ elements. So, to count the number of sequences of length n we have to *divide* the number of sequences of length m by $(m{-}n)!$. Thus we obtain as solution: $m!/(m{-}n)!$.

6.3.2 Binomial coefficients

The number of ways to select an (unordered) *collection* – instead of an (ordered) *sequence* – of n different objects from a given collection of m different objects, for $n, m : 0 \leq n \leq m$, can be determined by the following argument. The number of ways to arrange n different objects into a sequence is, as we know, $n!$. If we are only interested in a collection of such objects, their order is irrelevant, and this means that all $n!$ such arrangements are equivalent. So, to obtain the number of possible collections we must, again, divide the answer to the previous problem by $n!$. Thus, we obtain as solution:

$$\frac{m!}{n! * (m-n)!} \quad .$$

It so happens that this is an important quantity that has many interesting properties. These quantities are called *binomial coefficients*, and we introduce a notation for it, which is pronounced as "m over n":

$$\binom{m}{n} \;=\; \frac{m!}{n! * (m-n)!} \quad \text{, for all } n, m : 0 \leq n \leq m \quad .$$

* * *

For example, we consider all sequences of length m consisting of (binary) digits – "bits", for short – 0 or 1. As every bit in such a sequence is either 0 or 1 – so, one out of two possibilities –, independently of the other bits in the sequence, the total number of bit sequences of length m equals 2^m. If we number the positions in such a sequence from and including 0 and upto and excluding m, a one-to-one correspondence – that is, a bijection – exists between the collection of all subsets of the interval $[0..m)$ and the collection of all bit sequences of length m: number i is in a given subset if and only if the corresponding sequence contains a bit 1 at position i, for all $i \in [0..m)$.

The collection of bit sequences of length m can be *partitioned* into $m+1$ disjoint classes, according to the number of bits 1 in the sequence. That is, we consider the bit sequences, of length m, containing exactly n bits 1, for $n, m : 0 \leq n \leq m$. In the subset $\leftrightarrow$ bit-sequence correspondence every bit sequence containing exactly n bits 1 now corresponds to a subset with exactly n elements.

We already know that the number of subsets containing exactly n elements chosen from a given collection of m elements equals $\binom{m}{n}$. Hence, because of the one-to-one correspondence, the number of bit sequences of length m and containing exactly n bits 1 also equals $\binom{m}{n}$.

Because the bit sequences of length m and containing exactly n bits 1, for all n with $0 \leq n \leq m$, together are all bit sequences of length m, we obtain the following, quite interesting result:

$$(\Sigma n : 0 \leq n \leq m : \tbinom{m}{n}) \;=\; 2^m \quad \text{, for all } m \in \mathbb{N} \quad .$$

* * *

Binomial coefficients satisfy an interesting recurrence relation, which is also known as *Pascal's triangle*. As a basis for the recurrence we have, for all $m \in \mathbb{N}$:

$$\binom{m}{0} = 1 \text{ and: } \binom{m}{m} = 1 \quad ,$$

and for all n, m with $1 \le n \le m$ we have:

$$\binom{m+1}{n} = \binom{m}{n} + \binom{m}{n-1} \quad .$$

This latter property is proved as follows:

$$\begin{aligned}
\binom{m}{n} + \binom{m}{n-1} &= \tfrac{m!}{n!*(m-n)!} + \tfrac{m!}{(n-1)!*(m-n+1)!} \\
&= \tfrac{m!*(m-n+1)}{n!*(m-n+1)!} + \tfrac{m!*n}{n!*(m-n+1)!} \\
&= \tfrac{m!*(m-n+1)+m!*n}{n!*(m-n+1)!} \\
&= \tfrac{m!*(m+1)}{n!*(m-n+1)!} \\
&= \tfrac{(m+1)!}{n!*(m-n+1)!} \\
&= \binom{m+1}{n}.
\end{aligned}$$

By means of these relations the binomial coefficients can be arranged in an (infinite) table of triangular shape − hence the name “Pascal's triangle” −, such that, for any $m \in \mathbb{N}$, row m in the table contains the $m+1$ binomial coefficients $\binom{m}{n}$ in the order of increasing n. For instance, here are the first 7 rows of this triangular table:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

6.3.3 The Shepherd's Principle

Sometimes it is difficult to count the things we wish to count directly, and it may be easier to count the elements of a larger set that is so tightly related to our set of interest that we can obtain the count we want by means of a straightforward correction.

This is known as the *Shepherd's Principle*, because of the following metaphor. To count the number of sheep in a flock of sheep may be difficult: when the sheep stick closely together one observes a single, cluttered mass of wool in which no individual sheep can be distinguished easily. But, knowing – and assuming! – that every sheep has 4 legs, we can count the legs in the flock and conclude that the number of sheep equals this number of legs divided by 4.

As a matter of fact, we have already applied this technique, in Subsection 6.3.1: to count the number of sequences of length n and containing n different objects from a given collection of m different objects – the sheep –, we have actually counted the number of sequences of length m – the legs – and divided this by the number of ways the irrelevant $m-n$ remaining objects can be ordered – the number of legs per sheep – .

*   *   *

To demonstrate the Shepherd's Principle we discuss a few simple examples. Firstly, the number of anagrams of the word "FLIPJE" just equals the numbers of ways in which the 6 different letters can be arranged into a sequence of length 6. This is simple because the 6 letters are different, and the answer just is $6!$.

Secondly, what is the number of anagrams of the word "SHEPHERD"? As this word contains 8 letters there would be, if all letters would be different, $8!$ ways to arrange them into an anagram. But the letters are not different: the word contains 2 letters "H" and 2 letters "E"; here we assume, of course, that the 2 letters "H" are indistinguishable and also that the 2 letters "E" are indistinguishable. Well, we make them different *temporarily*, by *tagging* them, for example, by means of subscripts: "$\mathrm{SH_0E_0PH_1E_1RD}$". Now all letters are different, and the number of anagrams of this word – the legs – equals $8!$. The number of legs per sheep now is the number of ways in which the tagged letters can be arranged: $\mathrm{E_0}$ and $\mathrm{E_1}$ can be arranged in $2!$ ways and, similarly, $\mathrm{H_0}$ and $\mathrm{H_1}$ can be arranged in $2!$ ways. So, the number of legs per sheep equals $2!*2!$, and, hence, the number of anagrams of "SHEPHERD" – the number of sheep – equals $8!/(2!*2!)$.

Thirdly, what is the number of anagrams of the word "HAHAHAH"? Well, this 7-letter word contains 4 letters "H" and 3 letters "A"; so, on account of the Shepherd's Principle, the answer is $7!/(4!*3!)$, which equals $\binom{7}{4}$. Is this a surprise? No, because the word is formed from only 2 two different letters, "H" and "A"; so, the number of anagrams of "HAHAHAH" is equal to the number of 7-letter words, formed from letters "H" and "A" only and containing exactly 4 letters "H".

As the exact nature of the objects is irrelevant – it really does not matter whether we use "H" and "A" or "1" and "0" –, this last question is the same as the question for the number of 7-bit sequences containing exactly 4 bits 1. Hence, the answers are the same as well.

6.3.4 Newton's binomial formula

In subsection 6.3.2 we have derived the following relation for binomial coefficients:

$$(\Sigma n : 0 \leq n \leq m : \tbinom{m}{n}) \ = \ 2^m \quad \text{, for all } m \in \mathbb{N} \ .$$

Actually, this is an instance of the following, more general relation, for all – integer, rational, real, ... – numbers x, y:

$$(14) \qquad (x+y)^m \ = \ (\Sigma n : 0 \leq n \leq m : \tbinom{m}{n} * x^n * y^{m-n}) \quad \text{, for all } m \in \mathbb{N} \ .$$

This is known as *Newton's binomial formula*, although it appears to be much older than Newton. Newton, however, has generalized the formula by not restricting m to the naturals but by allowing it even to be a complex number.

We will not elaborate this here; instead we confine ourselves to the observation that there is a connection between the recurrence relation for binomial coefficients we have seen earlier:

$$\binom{m+1}{n} \ = \ \binom{m}{n} + \binom{m}{n-1} \quad ,$$

and relation (14), by means of the recurrence relation for exponentiation when applied to $(x+y)$:

$$(x+y)^{m+1} \ = \ (x+y) * (x+y)^m \quad .$$

6.4 A few examples

We conclude this chapter with a few more examples, some of which we have already solved, albeit in a slightly different form.

example 1:

A vase contains m balls which have been numbered $0, 1, \cdots, m{-}1$. From this vase we draw, at random, n balls, for some $n : 0 \leq n \leq m$. What is the number of possible results if the order in which the balls are drawn is relevant?

Notice that, although the balls themselves may not be distinguishable by their shapes, the fact that they have been numbered makes them distinguishable. So, what matters here is that we have a collection of m different objects. The problem at hand now is the same as a question we have already answered earlier: What is the number of sequences of length n and containing different objects chosen from a given collection of m different objects, for given $n, m : 1 \leq n \leq m$? As we have seen, the answer to this question is: $m! / (m{-}n)!$.

example 2:

A vase contains m balls which have been numbered $0, 1, \cdots, m{-}1$. From this vase we draw, at random, n balls, for some $n : 0 \leq n \leq m$. What is the number of possible results if the order in which the balls are drawn is *not* relevant? We recall that this question is equivalent to the question: What is the number of subsets of size n of a given finite set of size m? As we have seen, the answer is $\dbinom{m}{n}$.

We also have seen that an alternative way to answer this question is to apply the Shepherd's Principle: the n balls drawn from the vase can be ordered in $n!$ ways; as this order is irrelevant we have to divide the answer to the previous question by this very $n!$; as a result, we obtain the same answer, of course: $\binom{m}{n}$.

example 3:

A vase contains m balls which have been numbered $0, 1, \cdots, m{-}1$, for some positive natural m. From this vase we draw, at random, n balls, for some $n{\in}\mathbb{N}$, but now every ball drawn is placed back into the vase immediately, that is, before any next balls are drawn. What is the number of possible results if the order in which the balls are drawn is relevant? (Notice that in this example we do not need the restriction $n{\leq}m$.) The result of this game simply is a sequence, of length n, of numbers in the range $[0..m)$, and the numbers in this sequence are mutually independent. Hence, the answer is: m^n.

example 4:

A vase contains m balls which have been numbered $0, 1, \cdots, m{-}1$, for some positive natural m. From this vase we draw, at random, n balls, for some $n{\in}\mathbb{N}$, but now every ball drawn is placed back into the vase immediately, that is, before any next balls are drawn. What is the number of possible results if the order in which the balls are drawn is *not* relevant? This example is new, and more difficult that the previous ones.

An effective technique to solve this and similar problems is to choose the "right" *representation* of the possible results of the experiment, namely in such a way that these results can be counted. In the current example, we might write the down the numbers of the balls drawn, giving rise to sequences, of length n, and containing numbers in the range $[0..m)$. In this case, however, this representation is not *unique*, because the order of these numbers is irrelevant. For instance, the sequence "3011004" is a possible result, but so are the sequence "4011030" and "0001134"; because the order of the numbers in the sequences is irrelevant and because these three sequences contain the same numbers, albeit in different orders, these sequences actually represent only *one* result, which should be counted only once. So, we need a *unique* representation, because only then the number of possible results is equal to the number of possible representatives of these results.

We obtain a unique representation by writing down the numbers of the balls drawn in *ascending order*: then every result corresponds in a unique way to an ascending sequence, of length n, and containing numbers in the range $[0..m)$. For instance, from the three example sequences "3011004", "4011030", and "0001134", the last one is ascending: it uniquely represents the, one-and-only, common result corresponding to these sequences.

So, the answer to our original question equals the number of *ascending sequences*, of length n, and containing numbers in the range $[0..m)$. To be able to count these smoothly, yet another representation happens to be convenient, based on the following observation. The sequence "0001134", for instance, consists of 3 numbers 0, followed by 2 numbers 1, followed by 0 numbers 2, followed by 1 numbers 3, followed by 1 numbers 4, followed by 0 numbers 5, where we have assumed $m=6$ and $n=7$. So, by counting, for every number in the range $[0..m)$, how often it occurs in the ascending sequence we can also represent the result of the experiment. For the sequence "0001134", for instance, the corresponding sequence of counts is "320110": it contains m numbers, namely one count for every number in the range $[0..m)$; each count itself is a number in the range $[0, m]$ and the sum of all counts equals n, which was the length of the ascending sequence.

The restriction that the sum of the counts equals n is a bit awkward but can be made more manageable by means of the following *coding trick*: we represent each count by a sequence of as many zeroes as the count −in the *unary* representation, so to speak− and we separate these sequences of zeroes by means of a digit 1. For instance, again with $m=6$, the counts of the original ascending sequence "0001134" are 3, 2, 0, 1, 1, and 0, which in the zeroes-encoding become "000", "00", " ", "0", "0", and " ". Concatenated and separated by digits 1 we obtain: "000100110101". This is a bit sequence containing exactly n digits 0, because now the sum of the counts simply equals the total number of zeroes, and containing exactly $m-1$ digits 1, because we have m counts separated by $m-1$ digits 1. Consequently, the length of this bit sequence is $m-1+n$.

Generally, every ascending sequence of length n and containing numbers in the range $[0..m)$ can be represented *uniquely* by a bit sequence of length $m-1+n$ containing exactly n digits 0 and $m-1$ digits 1. So, also the results of our balls drawing experiment are uniquely represented by these bit sequences. Therefore, the number of all possible results equals the number of these bit sequences, which is: $\binom{m-1+n}{n}$.

6.4.1 Summary

Summarizing, for counting the number of possibilities to draw k copies from a set of n objects, there are four possible results, depending on the context:

- If every copy is drawn from the full set, so the drawn copies are put back, and drawings in a different order are considered to be different, then the number of possibilities is

$$n^k.$$

- If every copy is drawn from the remaining set, and no copies are put back, and drawings in a different order are considered to be different, then the number of possibilities is

$$n(n-1)(n-2)\cdots(n-k+1) \;=\; n!/(n-k)! \;=\; k!\binom{n}{k}.$$

- If every copy is drawn from the remaining set, and no copies are put back, and drawings in a different order are considered to be the same, then the number of possibilities is

$$\binom{n}{k}.$$

- If every copy is drawn from the full set, so the drawn copies are put back, and drawings in a different order are considered to be the same, then the number of possibilities is

$$\binom{n-1+k}{k}.$$

6.5 Exercises

1. Let V be a finite set with n elements.
   (a) What is the number of functions in $V \to \{0,1\}$?
   (b) What is the number of functions in $V \to \{0,1,2\}$?
   (c) What is the number of functions in $V \to W$, with $\#W = m$?

2. (a) What is the number of "words" consisting of 5 *different* letters?
   (b) What is the number of *injective* functions in $\{0,1,2,3,4\} \to \{a,b,c,\cdots,z\}$?
   (c) What is the number of *injective* functions in $V \to W$, with $\#V = n$ and $\#W = m$?

3. Let w_i be the number of sequences, of length i, consisting of letters from $\{a,b,c\}$, in which each two successive letters are different, for all $i \in \mathbb{N}$.
   (a) Formulate a recurrence relation for w.
   (b) Derive an explicit definition for w.

4. Let v_i be the number of sequences, of length i, consisting of letters from $\{a,b,c\}$, in which no two letters a occur in direct succession, for all $i \in \mathbb{N}$. It is given that $v_{i+2} = 2 * v_{i+1} + 2 * v_i$, for all $i \in \mathbb{N}$.
   (a) Determine v_0 and v_1.
   (b) Values c_0, c_1, α_0, and α_1 exist such that $v_i = c_0 * \alpha_0^i + c_1 * \alpha_1^i$, for all $i \in \mathbb{N}$. Determine c_0, c_1, α_0, and α_1.

5. (a) What is the number of 2-letter combinations in which the 2 letters occur in alphabetical order? For example: "kx" is such a combination, whereas "xk" is not.

(b) What is the number of 3-letter combinations in which the 3 letters occur in alphabetical order?

(c) What is the number of n-letter combinations in which the n letters occur in alphabetical order, for every natural $n : n \leq 26$?

6. We consider (finite) sequences g, of length n, consisting of natural numbers, with the additional property that $g_i \leq i$, for all $i : 0 \leq i < n$. (Here g_i denotes the element at position i in the sequence, where positions are numbered from 0, as usual.)

   (a) What is the number of this type of sequences, as a function of $n \in \mathbb{N}^+$?

   (b) Define a bijection between the set of these sequences and the set of all *permutations* of $[0..n)$.

7. This exercise is about strings of beads. The answers to the following questions depend on which strings of beads one considers “the same”: therefore, give this some thought to start with.

   (a) What is the number of ways to thread n different beads onto a string?

   (b) We have $2*n$ beads in n different colors; per color we have exactly 2 beads, which are indistinguishable. What is the number of ways to thread these beads onto a string?

   (c) The same question, but now for $3*n$ beads, with 3 indistinguishable beads per color.

   (d) What is the number of ways to thread m red and n blue beads onto a string, if, again, beads of the same color are indistinguishable?

8. The sequence of, so-called, *Fibonacci numbers* is the function F defined recursively by: $F_0 = 0$, $F_1 = 1$, and $F_{i+2} = F_{i+1} + F_i$, for $i \in \mathbb{N}$. The sequence S of, so-called, *partial sums* of F is defined by: $S_n = (\Sigma i : 0 \leq i < n : F_i)$, for all $n \in \mathbb{N}$. Prove that $S_n = F_{n+1} - 1$, for all $n \in \mathbb{N}$.

9. What is the number of anagrams of the word “STRUCTURES”?

10. Prove that $(\Sigma j : 0 \leq j < i : 2^j) = 2^i - 1$, for all $i \in \mathbb{N}$.

11. A given function a on $\mathbb{N}$ satisfies: $a_0 = 0$ and $a_{i+1} = a_i + i$, for all $i \in \mathbb{N}$. Derive an explicit definition for a.

12. A given function a on $\mathbb{N}$ satisfies: $a_0 = 0$ and $a_{i+1} = 2 * a_i + 2^i$, for all $i \in \mathbb{N}$. Derive an explicit definition for a.

13. A given function a on $\mathbb{N}$ satisfies: $a_0 = 0$ and $a_{i+1} = 2 * a_i + 2^{i+1}$, for all $i \in \mathbb{N}$. Derive an explicit definition for a.

14. A given function a on $\mathbb{N}^+$ satisfies: $a_1 = 1$ and $a_{i+1} = (1 + 1/i) * a_i$, for all $i \in \mathbb{N}^+$. Derive an explicit definition for a.

15. At the beginning of some year John deposits 1000 Euro in a savings account, on which he receives 8% interest at the end of every year. At the beginning of each next year he withdraws 100 Euro. How many years can John maintain this behavior, that is, after how many years the balance of his account is insufficient to withdraw yet another 100 Euro?

16. Solve the following recurrence relations for a function a; in each of the cases we have $a_0 = 0$ and $a_1 = 1$, and for all $i \in \mathbb{N}$:

    (a) $a_{i+2} = 6 * a_{i+1} - 8 * a_i$;

    (b) $a_{i+2} = 6 * a_{i+1} - 9 * a_i$;

    (c) $a_{i+2} = 6 * a_{i+1} - 10 * a_i$.

17. Solve the recurrence relation $a_{i+2} = 6 * a_{i+1} + 9 * a_i$, for all $i \in \mathbb{N}$, with $a_0 = 6$ and $a_1 = 9$.

18. The, so-called, Lucas sequence is the function L defined recursively by: $L_0 = 2$, $L_1 = 1$, and $L_{i+2} = L_{i+1} + L_i$, for all $i \in \mathbb{N}$. Determine the first 8 elements of this sequence, and derive an explicit definition for L.

19. Let V be a finite set with m elements. Let n satisfy: $0 \leq n \leq m$. What is the number of functions in $V \to \{0, 1\}$, with the additional property that $\#\{v \in V \mid f(v) = 1\} = n$?

20. A chess club with 20 members must elect a board consisting of a chairman, a secretary, and a treasurer.

    (a) What is the number of ways to form a board (from members of the club) if the three positions must be occupied by different persons?

    (b) What is the number of ways if it is permitted that a person occupies several positions?

    (c) What is the number of ways if the rule is that every person occupies at most 2 positions?

21. What is the number of sequences, of length 27, consisting of exactly 9 symbols 0, 9 symbols 1, and 9 symbols 2?

22. In a two-dimensional plane, a robot walks from grid point $(0, 0)$ to grid point $(12, 5)$, by successively taking a unit step, either in the positive x-direction or in the positive y-direction; it never takes a step backwards. What is the number of possibles routes the robot can walk?

23. What is the number of 8-digit decimal numbers in which the digits occur in *descending* order only? For example, "77763331" is such a number, whereas "98764511" is not.

7 Number Theory

7.1 Introduction

The basic arithmetic operations we have learned in primary school are addition, subtraction, multiplication, and division on natural numbers. These operations are meaningful, not only for numbers, but also for more general objects, like functions and, in particular, polynomials. Some properties of the arithmetic operations remain valid in these more general structures, whereas other properties lose their validity.

In this chapter we study some of the properties of integer numbers, which are the numbers $\cdots, -2, -1, 0, 1, 2, 3, \cdots$. The set of these numbers is called $\mathbb{Z}$; it has the set $\mathbb{N}$ of the natural numbers $0, 1, 2, 3, \cdots$ as a subset. So, $\mathbb{N}$ includes 0. In the earlier days of mathematics 0 was not considered a natural number, but if we "define" the natural numbers as the numbers used for *counting* then 0 is a very natural number: at the moment I write this, for instance, I have 0 coins in my pocket. (As a child I have learned that "zero is nothing", but this is not true, of course: although I have 0 coins in my pocket, it is not empty: it contains 0 coins but 1 handkerchief and 1 keyring holding 5 keys.) Also, at any given moment my wallet may contain 3 Euros and 0 U.S. dollars. Moreover, 0 has the, very important, algebraic property that it is the identity element of addition: $x+0 = x$, for all $x{\in}\mathbb{N}$ (and also for x in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, of course). In addition, the natural numbers have the property that every natural number is equal to the number of its *predecessors*, where the predecessors of x are all natural numbers less than x: for every $x{\in}\mathbb{N}$, we have that x is equal to the number of elements of the set $\{y{\in}\mathbb{N} \mid y{<}x\}$, and this is also true if $x = 0$.

The set of *positive naturals* is denoted by $\mathbb{N}^+$; it equals $\mathbb{N}$ but without 0, so we have $\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$. When we discuss the *prime numbers* we will have need of the set of all natural numbers that are at least 2, so this is $\mathbb{N}$ without 0 and 1. We will call such numbers "multiples" and denote its set as $\mathbb{N}^{+2}$. So, $\mathbb{N}^{+2} = \mathbb{N}\backslash\{0, 1\}$.

7.2 Divisibility

We start our subject with an exploration of *divisibility* and its, hopefully well-known, properties.

7.1 Definition. For $a, d \in \mathbb{Z}$ we say that "a is *divisible by* d" or, equivalently, that "a is a *multiple of* d" or, equivalently, "d is a *divisor of* a" if and only if:

$$(\exists q : q{\in}\mathbb{Z} : a = q * d) \quad .$$

□

By this definition, every integer is a divisor of 0, even 0 itself, although $0/0$ is not defined! If, however, $d \neq 0$, then for every $a{\in}\mathbb{Z}$ the value q, if it exists, for which $a = q * d$ is *unique*, and we write it as a/d, called the "quotient of" a and d. So, note that a/d is well-defined *if and only if* both a is divisible by d and $d \neq 0$.

Other simple properties are that every integer is divisible by 1 and by itself, and, as a consequence, 1 is a divisor of every integer.

The relation "is a divisor of" is often denoted by the (infix) symbol $|$. That is, we write $d|a$ for the proposition "d is a *divisor of* a". Then, as we have seen earlier, $(\mathbb{N}^+, |)$ is a poset: the relation $|$ is reflexive, anti-symmetric, and transitive.

7.2 Lemma. $(\forall a, d : a, d \in \mathbb{N}^+ : d|a \Rightarrow d \leq a)$.

Proof. If $d|a$ for $d, a \in \mathbb{N}^+$, then $a = q * d$ for some integer q. Since $d, a \in \mathbb{N}^+$ this is only possible for $q \geq 1$, so $a - d = q * d - d = (q-1) * d \geq 0$. □

A direct consequence of Lemma 7.2 is that the set of all (positive) divisors of a positive natural number is *finite*: the set of divisors of $a \in \mathbb{N}^+$ is a subset of the (finite) interval $[1, a]$. Because $1|a$ the set of divisors of a is non-empty, for every $a \in \mathbb{N}^+$.

Another important property of divisibility (by d) is that it is invariant under addition of multiples (of d). We call this a *translation property*.

7.3 Lemma. $(\forall a, d, x : a, d \in \mathbb{N}^+ \wedge x \in \mathbb{Z} : d|a \Leftrightarrow d|(a + x * d))$.

Proof. If $d|a$ then $a = q*d$ for some integer q. Hence $a+x*d = q*d+x*d = (q+x)*d$. Since both q and x are integer, so is $q + x$, hence $d|(a + x * d)$.

Conversely, assume $d|(a+x*d)$. Then $a+x*d = q*d$ for some integer q. Hence $a = q * d - x * d = (q - x) * d$. Since both q and x are integer, so is $q - x$, hence $d|a$. □

* * *

We have seen that not every number is divisible by every other number: a/d is not defined for all a, d, even if $d \neq 0$. Division can, however, be defined more generally, if only we allow the possibility of a, so-called, *remainder*. For the sake of this discussion we restrict ourselves to *positive* d, so $d \in \mathbb{N}^+$.

The equation, with $q \in \mathbb{Z}$ as the unknown, $a = q * d$ may not have a solution, but we can weaken the equation in such a way that it has a solution, and then the solution still happens to be unique.

7.4 Theorem. For all $a \in \mathbb{Z}$ and $d \in \mathbb{N}^+$ unique integers q, r exist satisfying:

$$a = q * d + r \ \wedge \ 0 \leq r < d \ .$$

Proof. We prove existence of the solution and its uniqueness separately.

Existence. We distinguish the cases $0 \leq a$ and $a < 0$. For the first case we prove, for all $a \in \mathbb{N}$, existence of a solution by Mathematical Induction on a. Firstly, if $a < d$, then $q = 0$ and $r = a$ are a solution. Secondly, if $d \leq a$ then $a - d \in \mathbb{N}$ and, because $1 \leq d$, we have $a - d < a$. Now, we assume, by Induction Hypothesis, that q and r satisfy:

$$a-d \;=\; q*d+r \;\;\wedge\;\; 0\le r<d \quad .$$

Then we also have:

$$a \;=\; (q+1)*d+r \;\;\wedge\;\; 0\le r<d \quad ,$$

hence, $q+1$ and r are a solution for a and d.

The proof for the case $a<0$ is very similar, but now by Mathematical Induction on $-a$. Firstly, if $-d\le a$ then $q=-1$ and $r=a+d$ are a solution. Secondly, if $a\le -d$ then we have $a+d<0$ and $-(a+d)<-a$. So let, again by Induction Hypothesis, q and r satisfy:

$$a+d \;=\; q*d+r \;\;\wedge\;\; 0\le r<d \quad .$$

Then we also have:

$$a \;=\; (q-1)*d+r \;\;\wedge\;\; 0\le r<d \quad ,$$

hence, now $q-1$ and r are a solution for a and d.

Uniqueness. Assume that q_0 and r_0 satisfy: $a \;=\; q_0*d+r_0 \;\wedge\; 0\le r_0<d$, and, similarly, assume that q_1 and r_1 satisfy: $a \;=\; q_1*d+r_1 \;\wedge\; 0\le r_1<d$. To prove uniqueness of the solution, then, we must prove $q_0=q_1$ and $r_0=r_1$. We now derive:

$$\begin{array}{ll} & a \;=\; q_0*d+r_0 \;\;\wedge\;\; a \;=\; q_1*d+r_1 \\ \Rightarrow & \qquad \{\text{ transitivity of } = \} \\ & q_0*d+r_0 \;=\; q_1*d+r_1 \\ \Leftrightarrow & \qquad \{\text{ algebra }\} \\ & r_0-r_1 \;=\; (q_1-q_0)*d \quad , \end{array}$$

from which we conclude that r_0-r_1 is a multiple of d. From the restrictions on r_0 and r_1, in the above equations, however, it follows that $-d<r_0-r_1<+d$, and the only multiple of d in this range is 0. So, we conclude that $r_0-r_1=0$, which is equivalent to $r_0=r_1$. But now we also have $(q_1-q_0)*d=0$, which, because $d\neq 0$, is equivalent to $q_0=q_1$, as required.

□

7.5 Definition. The unique value q mentioned in the theorem is called the "quotient of" a and d, and is denoted as $a \,\mathsf{div}\, d$. The unique value r mentioned in the theorem is called the "remainder of" a and d, and is denoted as $a \,\mathsf{mod}\, d$. As a result we obtain the following relation for div and mod, which we consider their definition, albeit an implicit one:

$$a \;=\; (a \,\mathsf{div}\, d)*d + a \,\mathsf{mod}\, d \;\;\wedge\;\; 0\le a \,\mathsf{mod}\, d<d \quad .$$

□

warning: Most programming languages have operators for quotient and remainder, even for negative values of d. The definitions of these operators not always are consistent with the definition given here. They do, however, always yield values q and r that satisfy $a \;=\; q*d+r$, but differences may arise in the additional restrictions imposed upon r. If both a and d are natural, however, so $0 \leq a$ and $1 \leq d$, then the operators for quotient and remainder yield the same values as $a \operatorname{div} d$ and $a \operatorname{mod} d$ as defined here. Be careful, though, in cases where either a or d may be negative. In particular, for negative a or d, the operations in several programming languages do *not* have the translation properties in Lemma 7.7

□

Operators div and mod are a true generalization of division, as they have the following properties that are immediate from the definitions.

7.6 Lemma. For all $a \in \mathbb{Z}$ and $d \in \mathbb{N}^+$ we have:

$$a \operatorname{mod} d = 0 \ \Leftrightarrow \ d \mid a \quad \text{, and:}$$

$$a \operatorname{mod} d = 0 \ \Rightarrow \ a \operatorname{div} d \ = \ a/d \quad .$$

□

Operators div and mod have many other useful properties, such as the following, so-called, *translation properties*. For more properties we refer the reader to the exercises.

7.7 Lemma. For all $a \in \mathbb{Z}$ and $d \in \mathbb{N}^+$, and for all $x \in \mathbb{Z}$ we have:

$$(a + x * d) \operatorname{div} d \ = \ a \operatorname{div} d + x \quad \text{, and:}$$

$$(a + x * d) \operatorname{mod} d \ = \ a \operatorname{mod} d$$

Proof. $a + x * d = (a \operatorname{div} d) * d + a \operatorname{mod} d + x * d = ((a \operatorname{div} d) + x) * d + a \operatorname{mod} d$, due to $0 \leq a \operatorname{mod} d < d$ and unicity as stated in Theorem 7.4 we conclude the lemma. □

7.3 Greatest common divisors

In this section we consider positive natural numbers only. Throughout this chapter we use names a, b, c, d for variables of type $\mathbb{N}^+$ and variables x, y, z to denote variables of type $\mathbb{Z}$.

As we have seen already in Lemma 7.2 the set of (positive) divisors of $a \in \mathbb{N}^+$ is non-empty, as it contains 1 and a, and it is finite. We denote this set as $\mathcal{D}(a)$.

7.8 Definition. For $a \in \mathbb{N}^+$ the set $\mathcal{D}(a)$ of (positive) divisors of a is defined by:

$$\mathcal{D}(a) \ = \ \{ d \in \mathbb{N}^+ \mid d \mid a \} \quad .$$

□

For all $a, b \in \mathbb{N}^+$ their respective sets $\mathcal{D}(a)$ and $\mathcal{D}(b)$ have a non-empty intersection, because both contain 1, and this intersection is finite as well. The elements of the set $\mathcal{D}(a) \cap \mathcal{D}(b)$ are called *common divisors* of a and b. As an abbreviation we also denote this intersection as $\mathcal{D}(a, b)$. So, by definition $\mathcal{D}(a, b)$ satisfies:

$$\mathcal{D}(a,b) \;=\; \{\, d{\in}\mathbb{N}^+ \mid d|a \wedge d|b \,\} \quad .$$

Because $\mathcal{D}(a,b)$ is non-empty and finite it has a maximum. This maximum is called the *greatest common divisor* of a and b. This depends on a and b, of course, so it is a function, which we call gcd.

7.9 Definition. Function gcd, of type $\mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$, is defined by, for all $a,b \in \mathbb{N}^+$:

$$gcd(a,b) \;=\; \mathsf{max}\,\mathcal{D}(a,b) \quad ,$$

or, stated in words, $gcd(a,b)$ is the greatest number of which both a and b is a divisor.
□

The common divisors of a and a itself just are the divisors of a, that is, we have $\mathcal{D}(a,a) = \mathcal{D}(a)$; hence the greatest common divisor of a and a itself just is the greatest divisor of a, which is a. If $b<a$ then $a-b \in \mathbb{N}^+$, and on account of translation Lemma 7.3, we conclude that $\mathcal{D}(a,b) = \mathcal{D}(a{-}b\,,b)$. In words: if $b<a$ then a and b have the same common divisors as $a-b$ and b; hence, their greatest common divisors are equal as well. Similarly, if $a<b$ then $\mathcal{D}(a,b) = \mathcal{D}(a\,,b{-}a)$ and the greatest common divisor of a and b is equal to the greatest common divisor of b and $b-a$. Thus we obtain the following lemma.

7.10 Lemma. For all $a,b \in \mathbb{N}^+$:

$$\begin{array}{lcll} gcd(a,a) & = & a & \\ gcd(a,b) & = & gcd(a{-}b\,,b) & \text{, if } b<a \\ gcd(a,b) & = & gcd(a\,,b{-}a) & \text{, if } a<b \end{array}$$

□

Greatest common divisors also have the following, quite surprising, property that the common divisors of a and b are the divisors of $gcd(a,b)$.

7.11 Lemma. For all $a,b,c \in \mathbb{N}^+$ with $c = gcd(a,b)$:

$$\mathcal{D}(a,b) \;=\; \mathcal{D}(c) \quad .$$

Proof. By Mathematical Induction on the value $a{+}b$. Firstly, if $a=b$ then, as we have seen, $\mathcal{D}(a,b) = \mathcal{D}(a)$ and, by Lemma 7.10, we have $c=a$, so also $\mathcal{D}(c) = \mathcal{D}(a)$; hence, $\mathcal{D}(a,b) = \mathcal{D}(c)$. Secondly, if $b<a$ then, as we have seen, $\mathcal{D}(a,b) = \mathcal{D}(a{-}b\,,b)$, and, by Lemma 7.10, we have $c = gcd(a{-}b\,,b)$; now we assume, by Induction Hypothesis $-$because $(a-b)+b < a+b$ $-$ that $\mathcal{D}(a{-}b\,,b) = \mathcal{D}(c)$; then it also follows that $\mathcal{D}(a,b) = \mathcal{D}(c)$. Thirdly, the case $a<b$ is similar to the previous case, because the situation is symmetric in a and b.
□

As was stated in Section 4.4, gcd coincides with the infimum in the lattice of natural numbers with the divisibility relation.
A direct consequence of translation Lemma 7.3 is that every common divisor of a and b also is divisor of any linear combination of a and b.

7.12 Lemma. For all $a, b, d \in \mathbb{N}^+$ and for all $x, y \in \mathbb{Z}$:

$$d \mid a \wedge d \mid b \;\Rightarrow\; d \mid (x{*}a + y{*}b) \quad .$$

□

In particular, $gcd(a,b)$ is a common divisor of a and b; hence, $gcd(a,b)$ also is a divisor of every linear combination of a and b. There is more to this, however, as the following theorem shows.

7.13 Theorem. For all $a, b \in \mathbb{N}^+$, integers $x, y \in \mathbb{Z}$ exist satisfying:

$$gcd(a,b) \;=\; x * a \,+\, y * b$$

Proof. A constructive proof is given in the next section, in the form of Euclid's extended algorithm, which shows how suitable numbers x and y can be calculated.
□

A consequence of this theorem is that $gcd(a,b)$ is the *smallest* of all positive linear combinations of a and b.

7.14 Theorem. For all $a, b \in \mathbb{N}^+$ we have:

$$gcd(a,b) \;=\; \mathsf{min}\,\{\, x{*}a + y{*}b \mid x, y {\in} \mathbb{Z} \wedge 1 \leq x{*}a + y{*}b \,\} \quad .$$

Proof. Let xm and ym be integers for which $xm * a + ym * b$ is positive and minimal. Let $c = gcd(a,b)$ and let xc and yc be integers for which $c = xc * a + yc * b$; on account of Theorem 7.13 such numbers exist. Now we must prove: $c = xm * a + ym * b$, which we do by proving $c \leq xm * a + ym * b$ and $xm * a + ym * b \leq c$ separately:

$$\begin{array}{cl}
 & c \leq xm * a + ym * b \\
\Leftarrow & \quad \{ \text{ Lemma 7.2, using that both } c \text{ and } xm{*}a + ym{*}b \text{ are positive } \} \\
 & c \mid (xm * a + ym * b) \\
\Leftarrow & \quad \{ \text{ Lemma 7.12 } \} \\
 & c \mid a \;\wedge\; c \mid b \\
\Leftrightarrow & \quad \{ \; c = gcd(a,b) \; \} \\
 & \mathsf{true} \quad ,
\end{array}$$

and:

$$\begin{array}{cl}
 & xm * a + ym * b \leq c \\
\Leftrightarrow & \quad \{ \text{ definition of } xc \text{ and } yc \;\} \\
 & xm * a + ym * b \;\leq\; xc * a + yc * b \\
\Leftrightarrow & \quad \{ \text{ both sides of the inequality are positive, and the LHS is minimal } \} \\
 & \mathsf{true}
\end{array}$$

□

* * *

Numbers of which the greatest common divisor equals 1 are called *relatively prime* or also *co-prime*. As we have seen −Theorem 7.13−, for all $a, b \in \mathbb{N}^+$ integers x, y exist such that

$$gcd(a,b) \;=\; x*a \,+\, y*b \;\; .$$

If $gcd(a,b) = 1$ this amounts to the existence of integers x and y satisfying:

$$x*a \,+\, y*b \;=\; 1 \;\; .$$

The following two lemmas are useful consequences of this property.

7.15 Lemma. For all $a, b, c \in \mathbb{N}^+$: $\;gcd(a,b) = 1 \,\wedge\, a \mid (b*c) \;\Rightarrow\; a \mid c$.

Proof. Let $gcd(a,b) = 1$ and let $a \mid (b*c)$; that is, assume that $x, y, z \in \mathbb{Z}$ satisfy:

(15) $\quad x*a + y*b \,=\, 1$

(16) $\quad b*c \,=\, z*a$

Now we derive:

$$
\begin{array}{ll}
 & \mathsf{true} \\
\Leftrightarrow & \quad \{\ (15)\ \} \\
 & x*a + y*b \,=\, 1 \\
\Rightarrow & \quad \{\ \text{Leibniz}\ \} \\
 & x*a*c + y*b*c \,=\, c \\
\Leftrightarrow & \quad \{\ (16)\ \} \\
 & x*a*c + y*z*a \,=\, c \\
\Leftrightarrow & \quad \{\ \text{algebra}\ \} \\
 & (\,x*c + y*z\,)*a \,=\, c \\
\Rightarrow & \quad \{\ \exists\text{-introduction, with } q := x*c+y*z\ \} \\
 & (\exists q : q \in \mathbb{Z} : c = q*a\,) \\
\Leftrightarrow & \quad \{\ \text{Definition of } \mid\ \} \\
 & a \mid c
\end{array}
$$

□

7.16 Lemma. For all $a, b, c \in \mathbb{N}^+$: $\;gcd(a,b) = c \;\Rightarrow\; gcd(a/c\,,\, b/c) = 1$.

□

7.4 Euclid's algorithm and its extension

The relations in Lemma 7.10 can be considered as a recursive definition of function gcd; that, thus, function gcd is well-defined is, again, proved by Mathematical Induction on the value $a+b$. So, the following recursive definition actually constitutes an algorithm for the computation of the greatest common divisor of two positive naturals. This is known as "Euclid's algorithm". For all $a,b\in\mathbb{N}^+$:

$$
\begin{array}{rcll}
gcd(a,b) & = & \mathsf{if} & a=b \;\rightarrow\; a \\
 & & [\,] & a>b \;\rightarrow\; gcd(a-b\,,b) \\
 & & [\,] & a<b \;\rightarrow\; gcd(a\,,b-a) \\
 & & \mathsf{fi} &
\end{array}
$$

This version of the algorithm is not particularly *efficient*, but it is the simplest possible. If, for instance, a is very much larger than b the calculation of $gcd(a,b)$ gives rise to the repeated subtraction $a-b$, until a does not exceed b anymore. Therefore, a more efficient algorithm can be constructed by means of div and mod operations.

* * *

According to Theorem 7.13 we have that $gcd(a,b)$ is a *linear combination* of a and b; this means that, for every $a,b\in\mathbb{N}^+$, integers x,y exist satisfying:

(17) $\qquad gcd(a,b) \;=\; x*a \,+\, y*b \;\;.$

In what follows we call such integers "matching numbers" for $gcd(a,b)$. Matching numbers are not *unique*: if, for instance, x and y are matching numbers for $gcd(a,b)$ then so are $x+b$ and $y-a$.

Because Theorem 7.13 is about *existence* of integers, we can try to prove it constructively by showing how these numbers can be computed. It so happens that Euclid's algorithm can be *extended* in such a way that, in addition to $gcd(a,b)$, integers x and y are calculated that satisfy (17) as well. As a result, provided we have proved the correctness of the extended algorithm, we not only have a proof of the theorem but we also obtain an algorithm to compute these numbers. (And, from the point of view of proving the theorem, efficiency is of no concern and the simplest possible algorithm yields the simplest possible proof.)

As was the case with function gcd we present Euclid's extended algorithm in the form of a recursively defined function. For this purpose we simply call this function F here; it maps a pair of positive naturals to a *triple* consisting of a positive natural and two integers, namely the GCD of the pair together with matching numbers. We denote such a triple as $\langle\, c\,,x\,,y\,\rangle$, in which c, x, and y are the elements of the triple. This means that function F is required to satisfy the following *specification*.

specification: Function F has type $\mathbb{N}^+\times\mathbb{N}^+\rightarrow\mathbb{N}^+\times\mathbb{Z}\times\mathbb{Z}$, and for all $a,b,c\in\mathbb{N}^+$ and for all $x,y\in\mathbb{Z}$, function F satisfies:

$$F(a,b)=\langle\, c\,,x\,,y\,\rangle \;\Rightarrow\; c=gcd(a,b) \;\wedge\; c=x*a+y*b$$

□

Notice that this specification does not specify F uniquely: because, as we have seen, matching numbers are not unique, several different functions F will satisfy this specification. This specification only states, firstly, that for every pair of positive naturals a and b its value $F(a,b)$ is a triple consisting of a positive natural and two integers, and, secondly, that for every such triple its first element is equal to $gcd(a,b)$ and its second and third elements are matching numbers for $gcd(a,b)$.

A simple recursive definition for F can now be constructed, based on the following considerations, using Mathematical Induction on $a+b$ again. Firstly, if $a=b$ then $gcd(a,b)=a$, and $a = 1*a+0*b$: hence, in this case $x=1$ and $y=0$ is an acceptable solution for x and y. Because $a=b$ we also have $gcd(a,b)=b$; therefore, $x=0$ and $y=1$ is an acceptable solution too: this illustrates once more that the numbers x and y are not unique.

Secondly, if $a>b$ then we have $gcd(a,b) = gcd(a–b\,,b)$. Now suppose, by Induction Hypothesis, that x,y are integers satisfying:

$$gcd(a–b\,,b) \;=\; x*(a–b) + y*b \quad .$$

The right-hand side of this equality can be rewritten to:

$$gcd(a–b\,,b) \;=\; x*a + (y–x)*b \quad ,$$

and because $gcd(a,b) = gcd(a–b\,,b)$ this is equivalent to:

$$gcd(a,b) \;=\; x*a + (y–x)*b \quad .$$

From this we conclude that if x and y are matching numbers for $gcd(a–b\,,b)$ then x and $y–x$ are matching numbers for $gcd(a,b)$.

Finally and similarly, for the case $a<b$ we can show that if x and y are matching numbers for $gcd(a\,,b–a)$ then $x–y$ and y are matching numbers for $gcd(a,b)$.

We now combine these results into the following recursive definition for F; this we call *Euclid's extended algorithm*:

$$
\begin{array}{lll}
F(a,b) \;=\; & \mathsf{if}\;\; a=b \;\rightarrow & \langle\, a\,,1\,,0\,\rangle \\
& [\,]\;\; a>b \;\rightarrow & \langle\, c\,,x\,,y–x\,\rangle \\
& & \quad \mathsf{where}\;\langle\, c\,,x\,,y\,\rangle \;=\; F(a–b\,,b) \\
& [\,]\;\; a<b \;\rightarrow & \langle\, c\,,x–y\,,y\,\rangle \\
& & \quad \mathsf{where}\;\langle\, c\,,x\,,y\,\rangle \;=\; F(a\,,b–a) \\
& \mathsf{fi} &
\end{array}
$$

This recursive definition is an example of a, so-called, *functional program*, but it is not difficult to encode this as a recursive function in languages like PASCAL or JAVA. As was the case with Euclid's algorithm proper, this algorithm is not very efficient, but it can be transformed into a more efficient one by means of division and remainder operations.

When applying this version of Euclid's algorithm or its extension to compute the gcd of, for instance, 1 and one million, the number one will be subtracted from the other number nearly one million times. As this example already shows, the complexity of the algorithm will not be better than linear in the arguments, which is not acceptable for applications in which the argument may be very large, as e.g. in cryptography. Now we present an improvement for which the complexity is improved to be logarithmic in the size of the arguments, by which it is suitable for using it for arguments in the order of magnitude of 10^{1000}. This improved version is one of the building blocks of modern public key cryptography.

The key ingredient of Euclid's algorithm as presented is that $gcd(a,b) = gcd(a,b-a)$, for $b > a > 0$. However, we also have $gcd(a,b) = gcd(a, b - c * a)$ for any choice for c we like, satisfying $c * a \leq b$. In the above version $c = 1$ was chosen, while the improved version takes $c = b \,\mathsf{div}\, a$. A first attempt looks as follows:

$$\begin{array}{lcl} gcd(a,b) & = & \mathsf{if}\ \ a = b \ \rightarrow \ \ a \\ & & [\!]\ \ a > b \ \rightarrow \ \ \cdots \\ & & [\!]\ \ a < b \ \rightarrow \ \ gcd(a\,, b - (b \,\mathsf{div}\, a) * a) \\ & & \mathsf{fi} \end{array}$$

This we will work out further. Note that $b - (b \,\mathsf{div}\, a) * a = b \,\mathsf{mod}\, a$. A further difference with our first version is that in case a is a divisor of b, we obtain $b - (b \,\mathsf{div}\, a) * a = 0$, and the resulting $b - (b \,\mathsf{div}\, a) * a = b \,\mathsf{mod}\, a$ is always $< a$. By keeping the first argument always less than the second argument, we now may further polish our algorithm without case analysis on $a > b$ and $a < b$. The resulting algorithm for $gcd(a,b)$ for $0 \leq a < b$ reads:

$$\begin{array}{lcl} gcd(a,b) & = & \mathsf{if}\ \ a = 0 \ \rightarrow \ \ b \\ & & [\!]\ \ a > 0 \ \rightarrow \ \ gcd(b \,\mathsf{mod}\, a, a) \\ & & \mathsf{fi} \end{array}$$

This version correctly computes $gcd(a,b)$ for $a < b$ by construction, while now the worst case complexity can be shown to be logarithmic in the largest argument b.

Also the extended version can be modified in this way:

$$\begin{array}{lcl} F(a,b) & = & \mathsf{if}\ \ a = 0 \ \rightarrow \ \ \langle\, b\,, 0\,, 1\,\rangle \\ & & [\!]\ \ a > 0 \ \rightarrow \ \ \langle\, c\,, y - x * (b \,\mathsf{div}\, a)\,, x\,\rangle \\ & & \qquad\qquad\qquad \mathsf{where}\ \langle\, c\,, x\,, y\,\rangle \ = \ F(b \,\mathsf{mod}\, a\,, a) \\ & & \mathsf{fi} \end{array}$$

Here for $0 \leq a < b$ the result of $F(a,b)$ is a triple (c,x,y) in which $c = gcd(a,b)$ and $x * a + y * b = c$. Also this algorithm can be shown to be logarithmic in the largest argument b since the number of steps is the same as for the basic gcd algorithm. Correctness follows since from $c = x * (b \,\mathsf{mod}\, a) + y * a$ one concludes $c = (y - x * (b \,\mathsf{div}\, a)) * a + x * b$. This is the version of the algorithm that is extensively used in practice.

To get a feeling how the algorithm works we apply it by hand to compute values x, y satisfying $73x + 87y = 1 = gcd(73, 87)$. In order to compute $F(73, 87)$ by the algorithm we have to compute $F(14, 73)$ since $87 \,\mathsf{mod}\, 73 = 14$, for which we have to compute $F(3, 14)$, and so on, until we arrive at $F(0, 1) = (1, 0, 1)$. In fact executing the algorithm corresponds to filling the following table:

a	b	x	y	$c = x * a + y * b$
73	87	31	-26	1
14	73	-26	5	1
3	14	5	-1	1
2	3	-1	1	1
1	2	1	0	1
0	1	0	1	1

Here first the columns for a and b are filled from top to bottom. Then in the last line $x = 0$ and $y = 1$ is filled, yielding $c = x * a + y * b = 1$. Next the values for x and y are filled from bottom to top in such a way that for every line $x * a + y * b = 1$ holds: according to the algorithm this is done by giving y the value of x from the line below, and giving x the value $y - x * (b \,\mathsf{div}\, a)$. At the end we fill the first line by $x = 31$ and $y = -26$, indeed satisfying the required property $73*31+87*(-26) = 1 = gcd(73, 87)$.

7.5 The prime numbers

In this section we study the set $\mathbb{N}^{+2}$ of *multiples*, which are the natural numbers from 2 onwards. As we have seen, every integer, and, hence, also every multiple is divisible by 1 and by itself. A multiple with the property that it is *not* divisible by any other number is called a *prime (number)*.

7.17 Definition. A *prime* is a multiple that is divisible by 1 and itself only.

□

If we would not restrict ourselves to multiples but to positive naturals instead, 1 would be a prime too, according to this definition. There are sound, technical reasons, however, not to consider 1 as a prime, which is why we define the primes as a subset of the multiples. So, the smallest prime is 2.

7.18 Example. The primes less than 100 are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Notice that 2 is even and that it is the *only* even prime.

□

The following lemma expresses that every multiple is divisible by at least one prime. If we would have allowed 1 as a prime number this lemma would have been void.

7.19 Lemma. For every $a \in \mathbb{N}^{+2}$ a prime p exists such that $p \mid a$.

Proof. By Mathematical Induction on a. Firstly, if a is a prime then a is a prime and $a\,|\,a$. Secondly, if a is not prime then a multiple $b\in\mathbb{N}^{+2}$ exists satisfying $b\neq a$, and $b\,|\,a$. From Lemma 7.2, using $b\,|\,a$, we conclude that $b\leq a$, but because $b\neq a$ this amounts to $b<a$. So, by Induction Hypothesis, we may assume that p is a prime such that $p\,|\,b$. Because $b\,|\,a$, by the transitivity of divisibility, we then conclude $p\,|\,a$, as required.

□

The following theorem is important; it has been proved already by Euclides.

7.20 Theorem. The set of all primes is infinite.

Proof. One way to prove that a set is infinite is to prove that every *finite subset* of it differs from the whole set; that is, for every finite subset the whole set contains an element not in that subset. So, let V be a finite subset of the primes. Now we define multiple a by:

$$a \;=\; (\Pi p : p\in V : p) + 1 \quad .$$

Because the product $(\Pi p : p\in V : p)$ is divisible by every $p\in V$, the number a is *not* divisible by p , for every $p\in V$. On account of Lemma 7.19, however, a is divisible by at least one prime, which therefore, is not an element of V .

□

* * *

A very old algorithm to compute "all" primes is known as *Eratosthenes's sieve*. This involves infinite enumerations of infinite subsets of the multiples, which is unfeasible, of course, but for the purpose of computing any finite number of primes, finite prefixes of these infinite enumerations will do. To compute all, infinitely many, primes would, of course, take an infinite amount of time. Yet, we call it an algorithm to compute "all" primes because it can be used to compute as many primes as desired in a finite amount of time.

Informally, the algorithm is presented as follows. One starts with writing down all – that is: sufficiently many – multiples in increasing order:

$$2\,,\,3\,,\,4\,,\,5\,,\,6\,,\,7\,,\,8\,,\,9\,,\,10\,,\,11\,,\,12\,,\,13\,,\,14\,,\,15\,,\,16\,,\,17\,,\,18\,,\,19\,,\,20\,,\,21\,,\,22\,,\,23\,,\,\cdots \quad .$$

The first number of this sequence, 2 , is the first prime number, and we now construct a new sequence from the first one by eliminating all multiples of 2 from it:

$$3\,,\,5\,,\,7\,,\,9\,,\,11\,,\,13\,,\,15\,,\,17\,,\,19\,,\,21\,,\,23\,,\,\cdots \quad .$$

This second sequence is an enumeration, again in increasing order, of all multiples that are not divisible by the first prime, 2 . The first number, 3 , of this second sequence is the second prime, and, again, we construct a third sequence from this second one, this time by eliminating all multiples of 3 :

$5, 7, 11, 13, 17, 19, 23, \cdots$.

This sequence contains all multiples that are not divisible by either 2 or 3; its first element, 5, is the *next* prime number, which is the smallest prime that is larger than 2 and 3. And so on...

The general properties on account of which this algorithm is correct are easily formulated. After n steps, for some $n \in \mathbb{N}$, a sequence is obtained that contains, in increasing order, all multiples that are *not* divisible by the smallest n prime numbers. The first number of this sequence then, because the sequence is increasing, is its minimum, and it can be proved that this minimum is the *next* prime, that is, the smallest prime number exceeding the smallest n prime numbers. By eliminating all multiples of this next prime the next sequence is obtained, containing all multiples not divisible by the first $n+1$ primes.

* * *

We have seen that the set of primes is infinite, but we may still ask for the *density* of the primes; that is, for any given multiple n we may ask *how many* primes are less than n. Because the number of potential divisors of n increases with n, the likelihood – not in the mathematical meaning of the word – that an arbitrary number is prime may be expected to decrease with increasing numbers.

The, so-called, *Prime Number Theorem* states that the number of primes less than n is approximately $n / \ln(n)$. This formula really gives an approximation only; for example, the number of primes less than 10^9 equals $50\,847\,534$, whereas $10^9 / \ln(10^9)$ is $48\,254\,942$ (rounded). An elementary proof of the Prime Number Theorem has been constructed by the famous Hungarian mathematician Pál Erdös.

The greatest common divisor of a prime p and a positive natural a can have only one out of two possible values: either $p \mid a$ and then $gcd(p, a) = p$, or $\neg(p \mid a)$ and then $gcd(p, a) = 1$. An important consequence of this is the following lemma.

7.21 Lemma. For every prime p and for all $a, b \in \mathbb{N}^+$: $p \mid (a*b) \;\Rightarrow\; p \mid a \vee p \mid b$.

Proof. By distinguishing the cases $p \mid a$ and $\neg(p \mid a)$ and, for the latter case, using Lemma 7.15 and $gcd(a, p) = 1$ if $\neg(p \mid a)$.

□

7.22 Lemma. If p, q are distinct prime numbers and $k \geq 0$, then q is not a divisor of p^k.

Proof. Induction on k. For $k = 0$ clearly q is not a divisor of $p^k = p^0 = 1$. For $k > 0$ we write $p^k = p * p^{k-1}$. If $q \mid p * p^{k-1}$ then by Lemma 7.15 and $gcd(p, q) = 1$ we conclude $q \mid p^{k-1}$, contradicting the induction hypothesis. □

The following theorem is known as the Unique Prime Factorization Theorem. Just like we write Σ for summation, we write Π for product. We even take infinite products over all prime numbers as long as all but finitely many are equal to 1: then the meaning of the product is the product of the remaining finitely many arguments.

7.23 Theorem. Every positive natural $a \in \mathbb{N}^+$ satisfies

$$a = \prod_{p \text{ prime}} p^{k(p,a)}$$

in which $k(p,a)$ is the largest number k such that $p^k \,|\, a$, for every prime number p.

Proof. We apply induction on a. For $a = 1$ we have $k(p,a) = 0$ for all prime numbers, indeed yielding $1 = \Pi_{p \text{ prime}} p^{k(p,1)}$.

For $a > 1$ by Lemma 7.19 a prime q exists such that $q \,|\, a$. We will apply the induction hypothesis on a/q, yielding $a/q = \Pi_{p \text{ prime}} p^{k(p,a/q)}$, and we will compare $k(p,a/q)$ with $k(p,a)$ for all primes p. Since $q^{k(q,a/q)} \,|\, a/q$ but not $q^{k(q,a/q)+1} \,|\, a/q$, we obtain $q^{k(q,a/q)+1} \,|\, a$ but not $q^{k(q,a/q)+2} \,|\, a$, so $k(q,a) = k(q,a/q) + 1$.

Next let p be any prime number unequal to q and k any number > 0. We will prove $p^k \,|\, a$ if and only if $p^k \,|\, a/q$. If $p^k \,|\, a/q$ then $a/q = b * p^k$ for some b, yielding $a = p^k * (b * q)$, so $p^k \,|\, a$. Conversely let $p^k \,|\, a$. Then $a = b * p^k$ for some b. Since $q \,|\, a$ but not $q \,|\, p^k$ (by Lemma 7.22), by Lemma 7.21 we conclude $q \,|\, b$, so $b = q * c$ for some c. From $a = b * p^k = q * c * p^k$ we conclude $a/q = c * p^k$, so $p^k \,|\, a/q$. So we have proved $p^k \,|\, a$ if and only if $p^k \,|\, a/q$, so $k(p,a) = k(p,a/q)$.

Combining these results yields

$$\begin{array}{rcll} a & = & q * (a/q) & \\ & = & q * \prod_{p \text{ prime}} p^{k(p,a/q)} & \text{(induction hypothesis)} \\ & = & q * q^{k(q,a/q)} * \prod_{p \text{ prime}, p \neq q} p^{k(p,a/q)} & \text{(splitting product)} \\ & = & q^{k(q,a)} * \prod_{p \text{ prime}, p \neq q} p^{k(p,a)} & \text{(above observations)} \\ & = & \prod_{p \text{ prime}} p^{k(p,a)} & \text{(combine product),} \end{array}$$

concluding the proof. □

If $a = \prod_{p \text{ prime}} p^{k(p,a)}$ and $b = \prod_{p \text{ prime}} p^{k(p,b)}$, then it is easily checked that $a \,|\, b$ if and only if $k(p,a) \leq k(p,b$ for all prime numbers p. As a consequence we obtain

$$gcd(a,b) \;=\; \prod_{p \text{ prime}} p^{\min(k(p,a),k(p,b))}.$$

For instance, $6! = 2 * 3 * 4 * 5 * 6 = 2^4 * 3^2 * 5^1 * 7^0$ and $\binom{8}{3} = 6 * 7 * 8/(3!) = 2^3 * 3^0 * 5^0 * 7^1$, so $gcd(6!, \binom{8}{3}) = 2^3 * 3^0 * 5^0 * 7^0 = 8$.

Apart from the Greatest Common Divisor (gcd) of two numbers $a, b > 0$ one may also consider the Least Common Multiple (lcm): $lcm(a,b)$ is defined to be the least number n such that $a|n$ and $b|n$. Such a number n with $a|n$ and $b|n$ always exists since $a*b$ satisfies the requirements, but $a*b$ does not need to be the smallest one. In fact, from the above observations one easily checks

$$lcm(a,b) \;=\; \prod_{p \text{ prime}} p^{\max(k(p,a),k(p,b))}.$$

Since for any two numbers k, k' we have $\max(k,k') + \min(k,k') = k + k'$, we obtain

$$gcd(a,b) * lcm(a,b) \;=\; \prod_{p \text{ prime}} p^{\min(k(p,a),k(p,b))+\max(k(p,a),k(p,b))}$$

$$= \prod_{p \text{ prime}} p^{k(p,a)+k(p,b)} \;=\; a*b$$

for all $a, b > 0$.

From these characterizations of *gcd* and *lcm* one easily derives that

$$c|a \wedge c|b \;\Leftrightarrow\; c|\,gcd(a,b)$$

and

$$a|c \wedge b|c \;\Leftrightarrow\; gcd(a,b)\,|\,c$$

for all numbers $a, b, c > 0$. As a consequence, we obtain that $(\mathbb{N}^+, |)$ is a *lattice*, in which *gcd* corresponds to the infimum and *lcm* corresponds to the supremum.

7.6 Modular Arithmetic

7.6.1 Congruence relations

Almost everybody probably knows that the product of two *even* integers is even, and that the product of two *odd* integers is odd. Also, the sum of two even integers is even too, and even the sum of two odd numbers is even. The point is that, apparently, whether the result of an operation, like addition or multiplication, is even or odd *only* depends on whether the arguments of the operation are even or odd.

The proposition that integer "x is even" is equivalent to "x is divisible by 2", which in turn is equivalent to $x \,\mathsf{mod}\, 2 = 0$; similarly, the proposition "x is odd" is equivalent to $x \,\mathsf{mod}\, 2 = 1$. That the property "being even" of the sum of two integers only depends on the "being even" of these two numbers know means that $(x+y) \,\mathsf{mod}\, 2$ only depends on $x \,\mathsf{mod}\, 2$ and $y \,\mathsf{mod}\, 2$ (and not on $x \,\mathsf{div}\, 2$ or $y \,\mathsf{div}\, 2$). In formula this is rendered as:

(18) $\qquad (x+y) \,\mathsf{mod}\, 2 \;=\; (x \,\mathsf{mod}\, 2 + y \,\mathsf{mod}\, 2) \,\mathsf{mod}\, 2$, for all $x, y \in \mathbb{Z}$.

Properties like these are not specific for 2 as a divisor: similar properties hold for all positive divisors. From the chapter on relations we recall that, for every function of type $B \to V$, the relation, on its domain B, "having the same function value" is an equivalence relation. For any fixed $d \in \mathbb{N}^+$, the function $(\mathsf{mod}\, d)$ that maps every $x \in \mathbb{Z}$ to $x \,\mathsf{mod}\, d$ has type $\mathbb{Z} \to [\,0\,..\,d\,)$. This function induces an equivalence relation, on $\mathbb{Z}$, of "having the same remainder when divided by d". This relation partitions $\mathbb{Z}$ into d different (and, as always, disjoint) equivalence classes, namely one for every value of the function $(\mathsf{mod}\, d)$: the equivalence class corresponding to $a \in [\,0\,..\,d\,)$ is the set

$$\{\, x{\in}\mathbb{Z} \mid x \,\mathsf{mod}\, d = a \,\} \quad ,$$

which can also be formulated as:

$$\{\, q*d+a \mid q{\in}\mathbb{Z} \,\} \quad .$$

In particular, of course, $a \in \{\, x{\in}\mathbb{Z} \mid x \,\mathsf{mod}\, d = a \,\}$, because $a \,\mathsf{mod}\, d = a$, for every $a \in [\,0\,..\,d\,)$.

Now properties similar to (18) also hold in this case; that is, we now have:

(19) $$(x+y) \,\mathsf{mod}\, d \;=\; (\, x \,\mathsf{mod}\, d + y \,\mathsf{mod}\, d\,) \,\mathsf{mod}\, d \quad \text{, for all } x,y \in \mathbb{Z} \quad .$$

A similar property holds for subtraction and multiplication:

(20) $$(x*y) \,\mathsf{mod}\, d \;=\; (\, x \,\mathsf{mod}\, d * y \,\mathsf{mod}\, d\,) \,\mathsf{mod}\, d \quad \text{, for all } x,y \in \mathbb{Z} \quad .$$

A consequence of propositions like (19) and (20) is that equivalence is *preserved under* arithmetic operations like addition and multiplication. Using (19), for instance, we can now derive, for all $x,y,z \in \mathbb{Z}$:

(21) $$x \,\mathsf{mod}\, d \;=\; y \,\mathsf{mod}\, d \;\Rightarrow\; (x+z) \,\mathsf{mod}\, d \;=\; (y+z) \,\mathsf{mod}\, d \quad .$$

An equivalence relation that is preserved under a given set of operations is called a *congruence relation*. In our case, the relation "having the same remainder when divided by d" is congruent with the operations addition, subtraction, and multiplication. Conversely, we also say that the operations addition, subtraction, and multiplication are *compatible with* the relation.

Notation: According to mathematical tradition, the fact that x and y are congruent modulo d is often denoted as:

$$x \;=\; y \pmod{d} \quad .$$

This notation is somewhat awkward, though, because it is not very clear what the *scope* is of the suffix "$(\mathrm{mod}\, d)$". Apparently, its scope extends over the complete equality textually preceding it; that is, if we would use some sort of brackets to delineate the scope of "$(\mathrm{mod}\, d)$" more explicitly, we should write something like:

$$[\![\; x \;=\; y \pmod{d} \;]\!] \quad .$$

Because the relation is a congruence relation and because it is not the same as sheer equality, although it resembles it, it seems better to denote the relation as an infix symbol resembling but different from "$=$". For example, the symbol "$=_{\text{mod}\,d}$" would be appropriate, as the subscript explicitly indicates the nature of the congruence. In this text we will abbreviate this to "$=_d$"; so, by definition we now have, for all $d \in \mathbb{N}^+$ and $x, y \in \mathbb{Z}$:

$$x =_d y \;\Leftrightarrow\; x \,\mathsf{mod}\, d = y \,\mathsf{mod}\, d \quad .$$

For example, congruence property (21) can now be rendered as, for all $x, y, z \in \mathbb{Z}$:

$$x =_d y \;\Rightarrow\; x+z =_d y+z \quad .$$

□

Other algebraic properties are compatible with congruence modulo d too. The numbers 0 and 1, for instance, are the identity elements of addition and multiplication, respectively, and this remains so under congruence. In addition, the property that 0 is a zero-element of multiplication −that is: $0*x = 0$− is retained. Finally, that multiplication distributes over addition remains true as well.

For any given $d \in \mathbb{N}^+$ we can now define binary operations $\oplus$ and $\otimes$, say, by, for all $x, y \in \mathbb{Z}$:

$$x \oplus y \;=\; (x+y) \,\mathsf{mod}\, d \quad \text{, and:}$$

$$x \otimes y \;=\; (x*y) \,\mathsf{mod}\, d \quad \text{, and:}$$

(If we would be very strict we should make the dependence on d explicit by writing $\oplus_d$ and $\otimes_d$.) Now $\oplus$ and $\otimes$ have type $[\,0\,..\,d\,) \times [\,0\,..\,d\,) \to [\,0\,..\,d\,)$ and with these operators various algebraic structures can be formed, which we mention here without further elaboration or proofs.

7.24 Theorem. For all $d \in \mathbb{N}^+$:

(a) $(\,[\,0\,..\,d\,)\,, \oplus\,, 0\,)$ is a group.

(b) $(\,[\,0\,..\,d\,)\,, \otimes\,, 1\,)$ is a monoid but not a group.

(c) $(\,[\,1\,..\,d\,)\,, \otimes\,, 1\,)$ is a group if and only if d is prime.

Proof. Most monoid and group axioms are checked straightforwardly, where 0 is the identity of $\oplus$ and 1 is the identity of $\otimes$.

In (b) it is not a group since 0 has no inverse: there is no $x \in [\,0\,..\,d\,)$ such that $x \otimes 0 = 1$.

For (c) we also have to check that $\otimes$ is well-defined, that is, if $a, b \in [\,1\,..\,d\,)$ then $a \otimes b$ should be in $[\,1\,..\,d\,)$ too, that is, $a * b \,\mathsf{mod}\, d \in [\,1\,..\,d\,)$. If d is not a prime, this is not the case since we can write $d = a * b$ for $a, b \in [\,1\,..\,d\,)$, by which $a * b \,\mathsf{mod}\, d = 0 \notin [\,1\,..\,d\,)$. If d is prime then well-definedness holds since if $a, b \in [\,1\,..\,d\,)$ then $a * b \,\mathsf{mod}\, d \neq 0$ due to Lemma 7.21. It remains to prove that every $a \in [\,1\,..\,d\,)$ has an inverse. Observe that $gcd(a, d) = 1$. By the extended Euclid's algorithm then there exist x, y such that $x * a + y * d = 1$. Hence $x * a \,\mathsf{mod}\, d = 1$, so x is the inverse of a.

□

7.6.2 An application: the nine and eleven tests

A technique that was commonly applied to verify manual calculations is the, so-called, *nine test*. This is based on the property that, in our decimal number representation, the remainder of a number when divided by 9 can be easily calculated: it equals the remainder of the sum of the number's digits modulo 9. As the sum of the digits of a number usually is much smaller than the number itself, the problem has been reduced. This process is repeated until a number is obtained that is less than 10: this last number, then, is the remainder of the original number modulo 9, except when it is 9 in which case the remainder is 0, of course.

For example, the sum of the digits of the number 123456789 equals 45, and the sum of the digits of 45 is 9. Hence, the remainder of 123456789 modulo 9 is 0.

Now to verify a calculation, for instance the addition or multiplication of two large numbers, one calculates the remainders modulo 9 of both numbers and of the result of the calculation, and one performs the same operation, modulo 9, to these remainders. If the results match we can be pretty confident that our calculation was correct, although we do not have certainty, of course. But, if the results do not match we certainly have made an error!

* * *

The property that the remainder modulo 9 of a number equals the remainder modulo 9 of the sum of the digits of that number's decimal representation is based on the observation that $10 \,\mathsf{mod}\, 9 = 1$. Now we have that a number like, for instance, 1437 is equal to $143*10+7$. Therefore, we have:

$$
\begin{array}{ll}
 & 1437 \;\mathsf{mod}\; 9 \\
= & \quad \{ \text{ above property } \} \\
 & (143*10+7) \;\mathsf{mod}\; 9 \\
= & \quad \{ \; 10 = 9+1 \; \} \\
 & (143*9+143*1+7) \;\mathsf{mod}\; 9 \\
= & \quad \{ \; \mathsf{mod} \text{ over } + \text{; multiples of 9 may be discarded and } 7 \,\mathsf{mod}\, 9 = 7 \; \} \\
 & (143 \,\mathsf{mod}\, 9 + 7) \;\mathsf{mod}\; 9 \quad .
\end{array}
$$

This calculation shows that $1437 \,\mathsf{mod}\, 9$ is equal to $143 \,\mathsf{mod}\, 9$ plus 7, modulo 9; if now, by Induction Hypothesis, $143 \,\mathsf{mod}\, 9$ is equal to the sum, modulo 9, of the digits of 143 then $1437 \,\mathsf{mod}\, 9$ also is equal to the sum of its digits, modulo 9.

* * *

In general, the decimal representation of natural numbers can be defined in a recursive way, as follows. A sequence of n decimal digits "$d_{n-1} \cdots d_2 d_1 d_0$" represents the natural number d_0 if $n=1$: in this case the sequence just is a single digit, "d_0". If $n \geq 2$, the number represented by the sequence is equal to the number represented by the sequence of $n-1$ digits "$d_{n-1} \cdots d_2 d_1$" times 10 plus d_0.

By means of this recursive definition it can be proved, by Mathematical Induction, of course, that the number represented by a sequence of decimal digits and the sum of these digits are congruent modulo 9. By means of the recursive definition it also is possible to prove that the number represented by the sequence of digits "$d_{n-1}\cdots d_2 d_1 d_0$" is equal to:

$$(\Sigma i : 0 \le i < n : d_i * 10^i) \quad ,$$

but in most cases the recursive definition is more manageable than this expression.

* * *

In a very similar, albeit slightly more complicated way we observe that 10 is congruent to -1 modulo 11, and that $100 \,\mathsf{mod}\, 11$ is equal to 1. This is the basis of the *eleven test*: the remainder of a natural number modulo 11 is equal to the remainder modulo 11 of the sum of the digits of that number's decimal representation, but here the digits are added with *alternating signs*, starting at the least-significant digit with a positive sign. The number 123456789, for example, is congruent modulo 11 to: $+9-8+7-6+5-4+3-2+1$, which equals 5.

As was the case with the nine test, the eleven test can be used to "verify" the results of calculations.

7.7 Fermat's little theorem

We prove the following theorem which is known as "Fermat's little theorem".

7.25 Theorem. For every prime number p and for every $a \in \mathbb{N}^+$ we have:

$$\neg(p\,|\,a) \;\Rightarrow\; a^{p-1} \,\mathsf{mod}\, p \,=\, 1 \quad .$$

Proof. Let p be a prime and let $a \in \mathbb{N}^+$. Assume $\neg(p\,|\,a)$; this is equivalent to $a \,\mathsf{mod}\, p \neq 0$, so we have: $1 \le a \,\mathsf{mod}\, p < p$; that is, $a \,\mathsf{mod}\, p \in [1\,..\,p)$. For the sake of brevity, we define $b = a \,\mathsf{mod}\, p$. Now we have that $a^{p-1} \,\mathsf{mod}\, p$ is equal to b^{p-1}, where $b \in [1\,..\,p)$ and b^{p-1} is to be interpreted in terms of $\otimes$-operations, instead of $*$. Hence, we also have $b^{p-1} \in [1\,..\,p)$.

By Theorem 7.24, part (c), we have that $([1\,..\,p), \otimes, 1)$ is a group, because p is prime. The set $\{b^i \mid 0 \le i\}$ together with $\otimes$ and 1 is the subgroup of $([1\,..\,p), \otimes, 1)$ generated by b. Because the whole group is finite, of size $p-1$, so is this subgroup. Therefore, a number $n \in \mathbb{N}^+$ exists such that $b^n = 1$ and $b^i \neq 1$, for all $i : 1 \le i < n$. Then we have: $\{b^i \mid 0 \le i\} = \{b^i \mid 0 \le i < n\}$, and n is the size of this set.

On account of Lagrange's Theorem we conclude $n \mid (p-1)$. So, let $z \in \mathbb{N}$ satisfy $p-1 = z * n$. Now we derive:

$$\begin{array}{ll}
 & a^{p-1} \,\mathsf{mod}\, p \\
= & \quad \{\text{ as observed above }\} \\
 & b^{p-1} \\
= & \quad \{\text{ definition of } z \text{ }\}
\end{array}$$

$$
\begin{array}{ll}
 & b^{z*n} \\
= & \quad \{ \text{ property of exponentiation } \} \\
 & (b^n)^z \\
= & \quad \{ \text{ definition of } n \text{ } \} \\
 & 1^z \\
= & \quad \{ \text{ } 1 \text{ is the identity of } \otimes \text{ } \} \\
 & 1
\end{array}
$$

□

7.8 Cryptography: the RSA algorithm

We conclude this chapter with a practical application of the theory, namely in the area of *cryptography*, which is the art of transmitting messages in a secure way, such that these messages cannot be read by anyone else than the intended receiver. For this purpose the messages are *encrypted* in such a way that they become unintelligible, except for the intended receiver who is the only one able to *decipher* the messages.

The algorithms for encryption and decryption themselves usually are not kept secret, but the parameters used in the process are. In cryptography such parameters usually are called *keys*.

Here we discuss the, so-called, RSA-algorithm, named after its inventors: Rivest, Shamir, and Adleman. This is an example of a so-called *public key* system. This means that the keys needed for encryption and decryption are chosen by the receiver of the messages, and the receiver makes the encryption key publicly known: everybody who wishes to send a message to this particular receiver now can use this public encryption key. The security of this arrangement is based on the assumption that it is (virtually) impossible to infer the (secret) decryption key from the (public) encryption key.

In older encryption schemes the encryption and decryption keys used to be chosen by the sender of the messages, and the sender now was faced with the problem how to communicate the decryption key to the intended receiver(s) in a secure way. In a public key system this difficulty is avoided.

The security of the RSA-algorithm rest on the assumption that it is very hard to factorize very large numbers into their prime factors. Here "very large numbers" means: numbers the decimal representation of which comprises several hundreds of digits.

*   *   *

The RSA-algorithm is based in two very large prime numbers p and q. Let $n = p*q$. Let a be any positive natural number not divisible by p or q. Then, by Fermat's little theorem, we have:

$$a^{p-1} \,\mathsf{mod}\, p \;=\; 1 \;\;\wedge\;\; a^{q-1} \,\mathsf{mod}\, q \;=\; 1 \quad .$$

From this it follows that we also have, because 1^{p-1} and 1^{q-1} are equal to 1:

$$a^{(p-1)*(q-1)} \,\mathsf{mod}\, p = 1 \;\wedge\; a^{(p-1)*(q-1)} \,\mathsf{mod}\, q = 1 \quad .$$

So $a^{(p-1)*(q-1)} - 1$ is divisible by both p and q, so also by $p * q$ since p and q are prime. So

(22) $$a^{(p-1)*(q-1)} \,\mathsf{mod}\, n = 1 \quad .$$

For every $k \geq 0$ we have $1^k = 1$, so

$$a^{k*(p-1)*(q-1)+1} \,\mathsf{mod}\, n = a.$$

Now encryption of a secret message works as follows. Choose an encryption number e with $gcd(e, (p-1)*(q-1)) = 1$. Represent the message by a number M, with $0 < M < n$, not divisible by p or q, for instance, the number of which the binary representation is the sequence of bits of the message. Now the encrypted message is $M^e \,\mathsf{mod}\, n$. By the extended Euclid's algorithm find numbers d, k such that $d * e - k * (p-1) * (q-1) = 1$. Now we obtain

$$(M^e)^d \,\mathsf{mod}\, n = M^{d*e} \,\mathsf{mod}\, n = M^{k*(p-1)*(q-1)+1} \,\mathsf{mod}\, n = M.$$

If some person A wants to receive a secret message from B then A chooses two large prime numbers p, q, computes $n = p * q$, chooses a corresponding value e and sends n, e to B in a non-safe way, by which also intruders may know n, e. Next B takes its secret message M, and computes $M' = M^e \,\mathsf{mod}\, n$ (encryption), and sends M' to A in a non-safe way, by which also intruders may know M'. Now A can decrypt M' to M by computing d as presented above, and computing $M'^d \,\mathsf{mod}\, n = M$. The crucial point is that knowledge of both p and q are required to do this computation, so intruders that may know n, e, M' have no clue how to construct the secret message M. Safety and feasibility of this approach depend on the following assumptions:

- if you know $n = p * q$, there is no feasible way to establish p and q,
- the extended Euclid's algorithm is feasible, even for n having thousands of digits,
- for numbers a, b, n of thousands of digits each, computation of $a^b \,\mathsf{mod}\, n$ is feasible.

For computing $a^b \,\mathsf{mod}\, n$ clearly a^b should not be computed since this number can never be stored: probably the number of digits of this number exceeds the number of atoms in the universe. Also not b times a multiplication with a should be executed, since b is far too large. But by carefully combining squaring and multiplying by a, and reducing all intermediate result modulo n, computing $a^b \,\mathsf{mod}\, n$ is feasible.

Although there is no formal proof that when knowing n, e, M' it is not feasible to compute M, it has turned out to be safe in practice. The RSA algorithm was proposed by Rivest, Shamir and Adleman in 1977. In that time taking prime numbers of 100 digits was safe. However, both to increasing computational power and improved algorithms the approach is currently not safe any more for 100 digits, but for 1000 digits it is.

7.9 Exercises

1. Let $a, d \in \mathbb{Z}$ and $d \neq 0$. Assuming that a is divisible by d, prove that the value q satisfying $a = q * d$ is unique.

2. (a) What are the divisors of 1? Prove the correctness of your answer.
   (b) Prove $(\forall a, d : a \in \mathbb{Z} \wedge d \in \mathbb{N}^{+2} : d \mid a \Rightarrow \neg(d \mid (a+1)))$.
   (c) Prove $(\forall a, b, d : a, b \in \mathbb{Z} \wedge d \neq 0 : d \mid a \vee d \mid b \Rightarrow d \mid (a * b))$.
   (d) Give a simple counter-example illustrating that Lemma 7.21 does *not* hold if p is *not* prime, for every $p \in \mathbb{N}^{+2}$.

3. Prove the following properties of div and mod, using Definition 7.5; it is given that $d \in \mathbb{N}^{+}$ and that $a, b, x \in \mathbb{Z}$:

   (a) $0 \leq a < d \;\Leftrightarrow\; (a \,\mathsf{mod}\, d) = a$
   (b) $0 \leq a < d \;\Leftrightarrow\; (a \,\mathsf{div}\, d) = 0$
   (c) $0 \leq a \;\Leftrightarrow\; 0 \leq a \,\mathsf{div}\, d$
   (d) $(a+d) \,\mathsf{mod}\, d \;=\; a \,\mathsf{mod}\, d$
   (e) $(a+d) \,\mathsf{div}\, d \;=\; (a \,\mathsf{div}\, d) + 1$
   (f) $(a + x * d) \,\mathsf{mod}\, d \;=\; a \,\mathsf{mod}\, d$
   (g) $(a + x * d) \,\mathsf{div}\, d \;=\; (a \,\mathsf{div}\, d) + x$
   (h) $(a \,\mathsf{mod}\, d) \,\mathsf{mod}\, d \;=\; a \,\mathsf{mod}\, d$
   (i) $(a \,\mathsf{mod}\, d) \,\mathsf{div}\, d \;=\; 0$
   (j) $(a + b) \,\mathsf{mod}\, d \;=\; (a \,\mathsf{mod}\, d + b \,\mathsf{mod}\, d) \,\mathsf{mod}\, d$
   (k) $(a + b) \,\mathsf{div}\, d \;=\; (a \,\mathsf{div}\, d) \;+\; (b \,\mathsf{div}\, d) \;+\; (a \,\mathsf{mod}\, d + b \,\mathsf{mod}\, d) \,\mathsf{div}\, d$
   (l) Give (simple) counter examples illustrating that $(a+b) \,\mathsf{mod}\, d$ is not necessarily equal to $a \,\mathsf{mod}\, d + b \,\mathsf{mod}\, d$, and that $(a+b) \,\mathsf{div}\, d$ is not necessarily equal to $a \,\mathsf{div}\, d + b \,\mathsf{div}\, d$.
   (m) $(a * b) \,\mathsf{mod}\, d \;=\; ((a \,\mathsf{mod}\, d) * (b \,\mathsf{mod}\, d)) \,\mathsf{mod}\, d$
   (n) $a \,\mathsf{mod}\, d = 0 \;\Leftrightarrow\; d \mid a$
   (o) $a \,\mathsf{mod}\, d = 0 \;\Leftrightarrow\; a \,\mathsf{div}\, d \;=\; a / d$
   (p) $1 \leq a \;\Leftrightarrow\; a \,\mathsf{div}\, d < a$, provided that $2 \leq d$
   (q) $a \,\mathsf{mod}\, d \;=\; b \,\mathsf{mod}\, d \;\Leftrightarrow\; (a - b) \,\mathsf{mod}\, d \;=\; 0$
   (r) Determine $(-1) \,\mathsf{div}\, d$ en $(-1) \,\mathsf{mod}\, d$

4. Given are $c, d \in \mathbb{N}^{+}$. Prove that for all $a \in \mathbb{Z}$:
   $$(a * d) \,\mathsf{mod}\, (c * d) \;=\; (a \,\mathsf{mod}\, c) * d \quad \text{and:}$$
   $$(a * d) \,\mathsf{div}\, (c * d) \;=\; a \,\mathsf{div}\, c \quad .$$

5. (a) Determine the *gcd* of the numbers 112 and 280.

(b) Determine numbers x and y satisfying: $x*112 + y*280 = gcd(112, 280)$.

6. Determine, by hand, all prime numbers between 100 and 200.
7. Prove that $x*(x+1)*(x+2)$ is divisible by 6, for all $x \in \mathbb{Z}$.
8. Prove that $(x^2-1) \,\mathsf{mod}\, 8 \in \{0, 3, 7\}$, for all $x \in \mathbb{Z}$.
9. Resolve $8! - 3*7!$ into prime factors.
10. Determine the lcm of the numbers 1500000021 and 3000000045.
11. Find integers x, y such that $100*x + 17*y = 1$.
12. Find an integer x such that $0 < x < 144$ and $83*x \,\mathsf{mod}\, 144 = 1$.
13. Are there integers x, y such that $111*x + 27*y = 5$? If so, find them, if not, prove this.
14. We consider the number whose decimal representation consists of 38 digits 1. We call this number X.
    (a) Give a, formally correct, mathematical expression for X.
    (b) What is the remainder of the division of x by 9?
    (c) What is the remainder of the division of x by 11?
    (d) What is the remainder of the division of x by 99?
15. Determine all values $x \in \mathbb{Z}$ satisfying both: $x = 2 \pmod{11}$ and: $x = 3 \pmod{23}$.
16. Resolve $\binom{17}{5}$ into prime factors.
17. Determine the gcd and lcm of $\binom{17}{5}$ and $\binom{18}{4}$.
18. Prove that $(n+1)*(n+2)*\cdots*(n+k)$ is divisible by $k!$, for all $n, k \in \mathbb{N}$.
19. Prove that a natural number is divisible by 4 if and only if, in the representation of that number in base 17, the sum of the digits is divisible by 4.
20. We know that $37*43 = 1591$. Determine $e \in \mathbb{N}$ in such a way that, for all $m \in \mathbb{Z}$, we have: $m^{127*e} =_{1591} m$.
21. Represent the number 1000 in base m, for every $m \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
22. What is the period of the recurring decimal fraction that represents $1/1001001$?
23. For a natural number $n > 10$ it is given that $2^n \,\mathsf{mod}\, n = 5$. Prove that n is not a prime number.
24. Determine all prime numbers p with the property that $33*p+1$ is a square.

25. A given number requires 10 (ternary) digits for its ternary representation. How many digits are needed to represent this number in the decimal system?

26. For natural numbers a, b prove that $a \mid b$ if and only if $D(a) \subseteq D(b)$.