CHAPTER 15

ANSWERS TO EXERCISES

Chapter 1

1.1. We have $A\cap\overline{B} = (A\cap\overline{A})\cup(A\cap\overline{B}) = A\cap(\overline{A}\cup\overline{B}) = A\cap\overline{A\cap B}$. Similarly, $A\cap\overline{C} = A\cap\overline{A\cap C}$, and we deduce $A\cap B = A\cap C \Longrightarrow A\cap\overline{B} = A\cap\overline{C}$.

Since $\overline{\overline{X}} = X$ for any subset X of E, this also proves the converse :

$$A\cap\overline{B} = A\cap\overline{C} \Longrightarrow A\cap\overline{\overline{B}} = A\cap\overline{\overline{C}} \Longrightarrow A\cap B = A\cap C\ .$$

1.2. Assume $A\cup B\subseteq A\cup C$ and $A\cap B\subseteq A\cap C$. We have $B\subseteq A\cup B\subseteq A\cup C$. Thus

$$B\subseteq B\cap(A\cup C) = (B\cap A)\cup(B\cap C)\subseteq(A\cap C)\cup(B\cap C) = (A\cup B)\cap C\subseteq C\ .$$

Let us show that $B=C \iff \big(\ A\cup B = A\cup C\ \text{ and }\ A\cap B = A\cap C\ \big)$. The implication $\Longrightarrow$ is straightforward. Conversely, applying the preceding result twice we have $B\subseteq C$ and $C\subseteq B$, and hence $B=C$.

1.3. By the definition of the symmetric difference we have $A\Delta B = (A\cap\overline{B})\cup(\overline{A}\cap B)$. Thus

$$\begin{aligned}
(A\triangle B)\cap(A\triangle C) &= \big((A\cap\overline{B})\cup(\overline{A}\cap B)\big)\cap\big((A\cap\overline{C})\cup(\overline{A}\cap C)\big)\\
&= \Big((A\cap\overline{B})\cap\big((A\cap\overline{C})\cup(\overline{A}\cap C)\big)\Big)\\
&\qquad\cup\Big((\overline{A}\cap B)\cap\big((A\cap\overline{C})\cup(\overline{A}\cap C)\big)\Big)\\
&= (A\cap\overline{B}\cap\overline{C})\cup(\overline{A}\cap B\cap C)\\
&= (A\cap\overline{B\cup C})\cup\big(\overline{A}\cap(B\cap C)\big).
\end{aligned}$$

Because $\overline{B\cup C}\subseteq\overline{B\cap C}$, we have

$$(A\triangle B)\cap(A\triangle C)\subseteq(A\cap\overline{B\cap C})\cup\big(\overline{A}\cap(B\cap C)\big) = A\triangle(B\cap C).$$

Because A and $\overline{A}$ are disjoint, equality holds if and only if $A\cap\overline{B\cup C} = A\cap\overline{B\cap C}$. We have

$$\begin{aligned}
A\cap\overline{B\cup C} = A\cap\overline{B\cap C} &\iff A\cap\overline{B}\cap\overline{C} = A\cap(\overline{B}\cup\overline{C})\\
&\iff A\cap\overline{B}\cap\overline{C} = (A\cap\overline{B})\cup(A\cap\overline{C})\\
&\iff A\cap\overline{B} = A\cap\overline{C}\,.
\end{aligned}$$

Hence, using Exercise 1.1, equality holds if and only if $A\cap B = A\cap C$. Similarly, we prove that $A\triangle(B\cup C)\subseteq(A\triangle B)\cup(A\triangle C)$ and that equality holds if and only if $A\cap(B\cup C) = A\cap B\cap C$.

1.4. 1. Let $x \in A \bigcup \Big(\bigcap_{i \in I} B_i \Big)$. If $x \in A$ then $\forall i \in I, x \in A \cup B_i$, and thus $x \in \bigcap_{i \in I} (A \cup B_i)$. Otherwise, $\forall i \in I, x \in B_i$, and hence $x \in A \cup B_i$ and we again have $x \in \bigcap_{i \in I} (A \cup B_i)$. We have thus shown that $A \bigcup \Big(\bigcap_{i \in I} B_i \Big) \subseteq \bigcap_{i \in E} (A \cup B_i)$. Conversely, if $x \in \bigcap_{i \in I} (A \cup B_i)$, we have $\forall i \in I, x \in A \cup B_i$. Hence, either $x \in A$ or $\forall i \in I$, $x \in B_i$. We thus have $x \in A \bigcup \Big(\bigcap_{i \in I} B_i \Big)$, and this proves the reverse inclusion.

2.
$$\begin{aligned} x \in A \cap \Big(\bigcup_{i \in I} B_i \Big) &\iff \exists i \in I \colon x \in A \cup B_i \\ &\iff x \in \bigcup_{i \in I} (A \cup B_i) \,. \end{aligned}$$

1.5. $\forall x \in E, f(x) \in F = \bigcup_{i \in I} A_i$. Thus $\exists i \in I, f(x) \in A_i$. We then have $x \in f^{-1}(A_i)$ and, consequently, $E = \bigcup_{i \in I} f^{-1}(A_i)$.

Let $i, j \in I$ be such that $i \neq j, f^{-1}(A_i) \cap f^{-1}(A_j) = f^{-1}(A_i \cap A_j) = f^{-1}(\emptyset) = \emptyset$. The family $\big(f^{-1}(A_i)\big)_{i \in I}$ is hence *almost* a partition of E.

A necessary and sufficient condition for all the sets $f^{-1}(A_i)$ to be non-empty is that $\forall i$, $A_i \cap Im(f) \neq \emptyset$. This condition is verified if f is surjective. Thus, a sufficient condition for all the sets $f^{-1}(A_i)$ to be non-empty is that f is surjective.

1.6. Assume that the image by f of any partition of E is a partition of F.

Let (E) be the rough partition of E into a single set. $f(E)$ is a partition of F. Hence, $F = f(E)$, which means that f is surjective.

Let $(\{x\})_{x \in E}$ be the discrete partition of E into singleton sets. $(\{f(x)\})_{x \in E}$ is a partition of F, and hence $\forall x, y \in E, x \neq y \Longrightarrow \{f(x)\} \cap \{f(y)\} = \emptyset$. That is, $f(x) \neq f(y)$. Hence, f is injective.

Conversely, assume that f is bijective. Let $(A_i)_{i \in I}$ be any partition of E. We have

- $\bigcup_{i \in I} f(A_i) = f(\bigcup_{i \in I} A_i) = f(E) = F$ because f is surjective.
- Let $i, j \in I$ be such that $i \neq j$. Since $(A_i)_{i \in I}$ is a partition, $A_i \cap A_j = \emptyset$, and since f is injective, $f(A_i) \bigcap f(A_j) = f(A_i \bigcap A_j) = f(\emptyset) = \emptyset$.
- $\forall i \in I, f(A_i) \neq \emptyset$, because $A_i \neq \emptyset$ and f is a mapping. Hence, $\big(f(A_i)\big)_{i \in I}$ is a partition of F.

1.7. 1. It is clear that the inclusion $X \subseteq f^{-1}(f(X))$ always holds. Assume f is injective and let $X \subseteq A$. If $x \in f^{-1}(f(X))$ then $f(x) \in f(X)$, and hence $\exists y \in X$ such that $f(x) = f(y)$. Because f is injective, we have that $x = y$, and hence $x \in X$. Finally, $f^{-1}(f(x)) \subseteq X$, and thus $X = f^{-1}(f(X))$.

Conversely, let $x, y \in A$ be such that $f(x) = f(y)$. Letting $X = \{x\}$, we have

$$f(y) \in f(X) = \{f(x)\} \,.$$

Hence, $y \in f^{-1}(f(X)) = X = \{x\}$. Hence, $y = x$, and f is injective.

2. Here, too, the inclusion $f(f^{-1}(Y)) \subseteq Y$ always holds. Assume f is surjective and let $Y \subseteq B$. $\forall y \in Y, \exists x \in A$ such that $f(x) = y$. Hence, $x \in f^{-1}(Y)$ and $y = f(x) \in f(f^{-1}(Y))$. We thus have $Y \subseteq f(f^{-1}(Y))$, and therefore $Y = f(f^{-1}(Y))$.

Conversely, let $y \in B$ and $Y = \{y\}$. We have $y \in Y = f(f^{-1}(Y))$, and hence $\exists x \in f^{-1}(Y) \subseteq A$ such that $f(x) = y$. Hence, f is surjective.

1.8. Note, first, that the inclusion $f(X \cap Y) \subseteq f(X) \cap f(Y)$ always holds.

Assume f is injective. Let $X, Y \subseteq A$ and let $z \in f(X) \cap f(Y)$. $\exists x \in X\colon f(x) = z$ and $\exists y \in Y\colon f(y) = z$. Because f is injective, $f(x) = z = f(y)$ implies $x = y$. Hence, $x = y \in X \cap Y$ and $z = f(x) \in f(X \cap Y)$. Thus, $f(X) \cap f(Y) \subseteq f(X \cap Y)$, and therefore $f(X) \cap f(Y) = f(X \cap Y)$.

Conversely, let $x, y \in A$ be such that $f(x) = f(y)$. Let $X = \{x\}$ and $Y = \{y\}$. We have $f(x) = f(y) \in f(X) \cap f(Y) = f(X \cap Y)$. Hence, $f(X \cap Y) \neq \emptyset$, and thus $X \cap Y \neq \emptyset$. This implies $x = y$.

1.9. 1. Let us show, first, that f is injective if and only if $A \cup B = E$.

Note, first, that because intersection distributes over union we have

$$X \cap (A \cup B) = (X \cap A) \cup (X \cap B)\,.$$

Assume that $A \cup B = E$. Let $X, Y \subseteq E$ be such that $f(X) = f(Y)$. We have

$$X = X \cap E = X \cap (A \cup B) = (X \cap A) \cup (X \cap B) = (Y \cap A) \cup (Y \cap B) = Y.$$

f is thus injective.

To prove the converse, consider its contrapositive. Assume $A \cup B \subsetneq E$. Let $x \in E \setminus (A \cup B)$. We have $f(\{x\}) = (\emptyset, \emptyset) = f(\emptyset)$ and $\{x\} \neq \emptyset$. Hence, f is not injective.

2. Let us now show that f is surjective if and only if $A \cap B = \emptyset$.

Assume $A \cap B = \emptyset$. Let $(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(B)$. Because $X \subseteq A$, $X \cap A = X$; because $Y \subseteq B$, $(Y \cap A) \subseteq (B \cap A) = \emptyset$. We thus have $(X \cup Y) \cap A = (X \cap A) \cup (Y \cap A) = X \cup \emptyset = X$. For the same reasons $(X \cup Y) \cap B = Y$. Hence, $f(X \cup Y) = (X, Y)$, and f is surjective.

We prove the converse by contradiction. Assume f is surjective and $A \cap B \neq \emptyset$. Let $x \in A \cap B$ and let X be a preimage by f of $(\{x\}, \emptyset)$; i.e. $X \cap A = \{x\}$ and $X \cap B = \emptyset$. We have $x \in X \cap A \subseteq X$ and $x \in B$, and hence $x \in X \cap B$, which contradicts $X \cap B = \emptyset$.

3. We deduce from the two preceding points that f is bijective if and only if $A \cup B = E$ and $A \cap B = \emptyset$. If, moreover, we assume that A and B are non-empty, this can be stated by saying that (A, B) is a partition of E.

1.10. (i) Let $x, y \in E$ be such that $(g \circ f)(x) = (g \circ f)(y)$. Because g and f are injective we deduce that $f(x) = f(y)$ and this implies that $x = y$. Hence, $g \circ f$ is injective.

(ii) Let $z \in G$. Because g is surjective, there exists $y \in F$ such that $g(y) = z$. Because f is surjective, there exists $x \in E$ such that $f(x) = y$. We deduce that $(g \circ f)(x) = z$, which proves that $g \circ f$ is surjective.

1.11. 1. (i) Assume that $g \circ f$ is injective. $\forall x, y \in A$, we have

$$f(x) = f(y) \Longrightarrow g(f(x)) = g(f(y)) \Longrightarrow x = y.$$

Hence, f is injective.

(ii) Assume that $g \circ f$ is surjective. $\forall z \in C, \exists x \in A$ such that $(g \circ f)(x) = z$. Hence, $\exists y \in B$ $(y = f(x))$ such that $g(y) = z$, and so g is surjective.

2. Let $f\colon \{1\} \longrightarrow \{1, 2\}$ be defined by $f(1) = 1$ and $g\colon \{1, 2\} \longrightarrow \{1\}$ be defined by $g(1) = g(2)$ $= 1$. The mapping $g \circ f$ is a bijection (it is the identity), f is not surjective and g is not injective.

3. (i) Let $x, y \in B$. Since f is surjective, $\exists x', y' \in A$ such that $f(x') = x$ and $f(y') = y$. We have

$$\begin{aligned} g(x) = g(y) &\Longrightarrow g \circ f(x') = g \circ f(y') \\ &\Longrightarrow x' = y' \\ &\Longrightarrow x = y\,. \end{aligned}$$

Hence, g is injective.

(ii) Let $y \in B$. Since $g \circ f$ is surjective, $\exists x \in A$ such that $(g \circ f)(x) = g(y)$. Because g is injective, we deduce that $f(x) = y$. Hence, f is surjective.

1.12. 1. Using Exercise 1.11, we deduce from the hypotheses that f, $g \circ f$, h, and $f \circ h$ are injective and that f and $f \circ h$ are surjective. Hence, f is bijective. From $f \circ h$ surjective and f injective we deduce that h is surjective. Consequently, h is bijective.

Lastly, from $g \circ f$ injective and f surjective we deduce that g is injective, and from $f \circ h \circ g$ surjective and $f \circ h$ injective we deduce that g is surjective. Hence, g is also bijective.

2. idem.

1.13. (i) ($\Longrightarrow$) Assume f is injective. Choose any element $x_\circ$ of E. (This is possible because $E \neq \emptyset$.) Let $y \in F$. If y has a preimage x by f then this preimage is unique since f is injective ; then let $r(y) = x$. Otherwise, let $r(y) = x_\circ$. For any x of E, x is the unique preimage of $f(x)$. We thus have that $\forall x \in E, \quad r \circ f(x) = r(f(x)) = x$.

(ii) ($\Longrightarrow$) Let $y \in F$. Because f is surjective, there exist elements x in E such that $y = f(x)$. Choose an arbitrary element x among those and let $s(y) = x$. $\forall y \in F$ we have $f(s(y)) = y$, and thus $f \circ s = id_F$.

(iii) ($\Longrightarrow$) Assume f is bijective. It suffices to show that the mapping s defined above also verifies $s \circ f = id_E$. Let $x \in E$ and $y = f(x)$. Because f is injective, x is the unique preimage of y by f. We thus have $s(y) = x$ and, consequently, $s(f(x)) = x$.

The converses are deduced from Exercise 1.11, together with the fact that r is surjective, s is injective and f^{-1} is bijective.

1.14. Let us prove by induction on n that if there exists an injection from $[m]$ to $[n]$ then $m \leq n$.

If $n = 0$ then $[n] = \emptyset$, and if there exists a mapping from $[m]$ to $\emptyset$ then it must be true that $[m] = \emptyset$, and so $m = 0$.

Let n be a fixed integer. Assume that the existence of an injection from $[m]$ to $[n]$ implies $m \leq n$. Let $f\colon [m] \longrightarrow [n+1]$ be an injection. If $f^{-1}(n+1) = \emptyset$ then $f\colon [m] \longrightarrow [n]$ is an injection, and by the hypothesis we have that $m \leq n$, and hence $m \leq n+1$. Otherwise, let p be the unique preimage of $n+1$ by f. If $p = m$ then the mapping $g\colon [m-1] \longrightarrow [n]$ defined by $g(x) = f(x)$ is an injection. (g is the restriction of f to $[m-1]$.) Hence, $m-1 \leq n$, and thus $m \leq n+1$. Lastly, if $p \neq m$ then the mapping $g\colon [m-1] \longrightarrow [n]$ defined by

$$g(x) = \begin{cases} f(x) & \text{if } x \neq p, \\ f(m) & \text{if } x = p, \end{cases}$$

is an injection. Here, too, we have $m-1 \leq n$, and so $m \leq n+1$.

1.15. (i) Let $f\colon E \longrightarrow [n]$ and $g\colon F \longrightarrow [p]$ be two bijections. We can easily verify that the mapping $h\colon E \cup F \longrightarrow [n+p]$ defined by $\forall x \in E, h(x) = f(x)$ and $\forall x \in F, h(x) = g(x) + n$ is a bijection. We deduce that $|E \cup F| = n + p = |E| + |F|$.

(ii) Consequence of (i).

(iii) With the same notations as for (i), we define the mapping $h\colon E \times F \longrightarrow [n \times p]$ by letting $\forall (x,y) \in E \times F$, $h(x,y) = p \times (f(x) - 1) + g(y)$. We check that h is a bijection and hence $|E \times F| = |E| \times |F|$. We can also use (ii) to prove this result because the family $(E \times \{y\})_{y \in F}$ is a partition of $E \times F$.

(iv) If $E = \{a_1, \ldots, a_n\}$, then a mapping $f\colon E \longrightarrow F$ is fully specified by the images $b_1, \ldots, b_n$ of $a_1, \ldots, a_n$. Each b_i, where $i \in [n]$, can be chosen in $|F|$ possible ways. We thus have $|F|^n = |F|^{|E|}$ possible choices for f. So, there is a bijection from the set of mappings of E to F to the Cartesian product F^n, and this is the reason why the set of mappings from E to F is denoted by F^E.

(v) The mapping associating with each subset A of E its characteristic function χ_A is a bijection. Thus $|\mathcal{P}(E)| = |\{0,1\}^E| = 2^{|E|}$.

1.16. Let $A = [m]$ be the set of pigeons to be placed and let A_i be the set of pigeons nesting in the pigeonhole i, for $i \in [n]$. $A_1, \ldots, A_n$ form a partition of A, and thus

$$|A| = \sum_{i=1}^{n} |A_i| \, .$$

If we had that $\forall i \in [n]$, $|A_i| < m/n$, we would deduce $|A| = \sum_{i=1}^{n} |A_i| < n \times m/n = m$, a contradiction ; we thus have that $|A_i| \geq m/n$ for at least one i.

1.17. Note, first, that the existence of a surjection from E to F is equivalent to the existence of an injection from F to E. So let $f: E \longrightarrow F$ and $g: F \longrightarrow E$ be two injections. We define the following sets by induction :

- $E_0 = E$ and $F_0 = F$.
- $F_{n+1} = f(E_n), F'_{n+1} = F_n \setminus F_{n+1}, E'_{n+1} = g(F'_{n+1})$, and $E_{n+1} = E_n \setminus E'_{n+1}$.

We then verify that $X = \bigcap_{n\geq 0} E_n$ and $X' = \bigcup_{n\geq 1} E'_n$ almost form a partition of E, i.e. $X \cap X' = \emptyset$ and $E = X \cup X'$ with X or X' possibly empty. Indeed, let $x \in X'$. $\exists n \geq 1$ such that $x \in E'_n$. By the definition of $E_n, x \notin E_n$ and hence $x \notin X$. The sets X and X' are hence disjoint. Let $x \in E \setminus X$ and let $n \geq 0$ be such that $x \in E_n$ and $x \notin E_{n+1}$. We necessarily have $x \in E'_{n+1} \subseteq X'$. Thus $E = X \cup X'$.

Similarly, $Y = \bigcap_{n\geq 0} F_n$ and $Y' = \bigcup_{n\geq 1} F'_n$ almost form a partition of E.

Note that $X' \subseteq Im(g)$ because $\forall n \geq 1, E'_n = g(F'_n)$. Because g is injective, any element x of $Im(g)$, and hence of X', has a unique preimage by g denoted by $g^{-1}(x)$. The mapping $h: E \longrightarrow F$ is hence fully defined by

$$h(x) = \begin{cases} f(x) & \text{if } x \in X, \\ g^{-1}(x) & \text{if } x \in X'. \end{cases}$$

It remains to check that it is a bijection.

Let $x, y \in E$ and assume $h(x) = h(y)$. If $x, y \in X$ then $x = y$ because f is injective. If $x, y \in X'$ then $x = g(g^{-1}(x)) = g(h(x)) = g(h(y)) = y$. Finally, note that $f(X) = \bigcap_{n\geq 0} f(E_n) = Y$ and that $g(Y') = \bigcup_{n\geq 1} g(F'_n) = \bigcup_{n\geq 1} E'_n = X'$. Because g is injective, we deduce that $g^{-1}(X') = Y'$. Hence, $x \in X$ and $y \in X'$ cannot hold because in this case $h(x) = f(x) \in f(X) = Y$ and $h(y) = g^{-1}(y) \in g^{-1}(X') = Y'$. We would then have $h(x) = h(y) \in Y \bigcap Y' = \emptyset$. Hence, h is injective. We finally show that h is surjective. Let $y \in F$. If $y \in Y'$ then $g(y) \in g(Y') = X'$, and hence $h\big(g(y)\big) = g^{-1}\big(g(y)\big) = y$. If $y \in Y$ then $y \in F_1 = Im(f)$. Hence, y has a unique preimage x by f. We then show that $\forall n \geq 0, x \in E_n$. Indeed, we have $y \in Y \subseteq F_{n+1} = f(E_n)$, and because f is injective this implies that $x \in E_n$. Hence, $x \in X = \bigcap_{n\geq 0} E_n$, and $h(x) = f(x) = y$.

1.18. Consider the mapping $f: \mathbb{N}^2 \longrightarrow \mathbb{N}$ defined by

$$f(x, y) = y + \big(0 + 1 + 2 + \cdots + (x + y)\big).$$

This mapping gives a diagonal enumeration of the elements of $\mathbb{N}^2$ as indicated in figure 15.1.

Figure 15.1

We show that f is bijective. Let $n \in \mathbb{N}$. There exists a unique $a \in \mathbb{N}$ such that

$$(0 + 1 + \cdots + a) \leq n < \big(0 + 1 + \cdots + (a + 1)\big)\,.$$

The unique preimage of n by f is given by $y = n - (0 + 1 + \cdots + a)$ and $x = a - y$.

A different bijection from $\mathbb{N}^2$ to $\mathbb{N}$ is given by the function $g: \mathbb{N}^2 \longrightarrow \mathbb{N}$ defined by $g(x, y) = 2^x(2y + 1) - 1$. The fact that it is a bijection follows from the remark that any strictly positive integer is the product of a power of two and an odd number.

1.19. By contradiction. Assume that U is countable and let $(x_n)_{n\in\mathbb{N}}$ be an enumeration of U. We can represent the values $(x_n)_{n\in\mathbb{N}}$ by the following table :

x	0	1	2	$\ldots$	n	$\ldots$
x_0	x_0^0	x_0^1	x_0^2	$\ldots$	x_0^n	$\ldots$
x_1	x_1^0	x_1^1	x_1^2	$\ldots$	x_1^n	$\ldots$
x_2	x_2^0	x_2^1	x_2^2	$\ldots$	x_2^n	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$
x_n	x_n^0	x_n^1	x_n^2	$\ldots$	x_n^n	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$

We then apply a so-called *diagonalization* argument : let u be the sequence defined by

$$\forall n \in \mathbb{N}, \quad u_n = \begin{cases} 0 & \text{if } x_n^n = 1, \\ 1 & \text{if } x_n^n = 0. \end{cases}$$

Then u cannot be equal to any x_n because $u_n \neq x_n^n$ for any n.

This also proves that $\mathcal{P}(\mathbb{N})$ is uncountable because $\mathcal{P}(\mathbb{N})$ is in bijection with U. To this end we associate with each subset A of $\mathbb{N}$ the sequence u defined by the characteristic function χ_A of A (i.e. $u_n = \chi_A(n)$ for any n in $\mathbb{N}$).

1.20. Let $\mathbb{1}$ and $\mathbb{1}'$ be two units. We have $\mathbb{1}' = \mathbb{1}' * \mathbb{1} = \mathbb{1}$.

1.21. 1. $(e, e') \in (\mathcal{R}_1 \cup \mathcal{R}_2)^{-1}$ if and only if $(e', e) \in \mathcal{R}_1 \cup \mathcal{R}_2$ if and only if $\big((e', e) \in \mathcal{R}_1$ or $(e', e) \in \mathcal{R}_2\big)$ if and only if $\big((e, e') \in (\mathcal{R}_1)^{-1}$ or $(e, e') \in (\mathcal{R}_2)^{-1}\big)$ if and only if $(e, e') \in (\mathcal{R}_1)^{-1} \cup (\mathcal{R}_2)^{-1}$.

2. $(e, e') \in (\mathcal{R}_1 \cap \mathcal{R}_2)^{-1}$ if and only if $(e', e) \in \mathcal{R}_1 \cap \mathcal{R}_2$ if and only if $\big((e', e) \in \mathcal{R}_1$ and $(e', e) \in \mathcal{R}_2\big)$ if and only if $\big((e, e') \in (\mathcal{R}_1)^{-1}$ and $(e, e') \in (\mathcal{R}_2)^{-1}\big)$ if and only if $(e, e') \in (\mathcal{R}_1)^{-1} \cap (\mathcal{R}_2)^{-1}$.

3. $(e, e') \in (\overline{\mathcal{R}})^{-1}$ if and only if $(e', e) \in \overline{\mathcal{R}}$ if and only if $(e', e) \notin \mathcal{R}$ if and only if $(e, e') \notin \mathcal{R}^{-1}$ if and only if $(e, e') \in \overline{\mathcal{R}^{-1}}$.

4. Assume $\mathcal{R}_1 \subseteq \mathcal{R}_2$. If $(e, e') \in \mathcal{R}_1^{-1}$, then $(e', e) \in \mathcal{R}_1$, and hence $(e', e) \in \mathcal{R}_2$ and $(e, e') \in \mathcal{R}_2^{-1}$. Conversely, assume $\mathcal{R}_1^{-1} \subseteq \mathcal{R}_2^{-1}$. If $(e, e') \in \mathcal{R}_1$, then $(e', e) \in \mathcal{R}_1^{-1}$, and hence $(e', e) \in \mathcal{R}_2^{-1}$ and $(e, e') \in \mathcal{R}_2$.

5. $(e, e') \in (\mathcal{R}^{-1})^{-1}$ if and only if $(e', e) \in \mathcal{R}^{-1}$ if and only if $(e, e') \in \mathcal{R}$.

6. We know that $\mathcal{R}^* = Id_E \cup \mathcal{R}^+$. But $\mathcal{R}^+ = \bigcup_{i>0} \mathcal{R}^i$, and as $Id_E \subseteq \mathcal{R}$, we have $Id_E \subseteq \mathcal{R}^+$, and hence $\mathcal{R}^* = \mathcal{R}^+$.

The converse is false. Let $\mathcal{R}$ be the relation defined by : $x \mathrel{\mathcal{R}} y \iff x \neq y$ on a set E with at least two distinct elements. Then $Id_E \not\subseteq \mathcal{R}$, but $Id_E \subseteq \mathcal{R}^2 \subseteq \mathcal{R}^+$.

1.22. 1.(a) $(e, e') \in (\mathcal{R}_1.\mathcal{R}_2)^{-1}$ if and only if $(e', e) \in \mathcal{R}_1.\mathcal{R}_2$ if and only if $\big(\exists e'' : (e', e'') \in \mathcal{R}_1$ and $(e'', e) \in \mathcal{R}_2\big)$ if and only if $\big(\exists e'' : (e'', e') \in \mathcal{R}_1^{-1}$ and $(e, e'') \in \mathcal{R}_2^{-1}\big)$ if and only if $(e, e') \in (\mathcal{R}_2)^{-1}.(\mathcal{R}_1)^{-1}$.

1.(b) $(e, e') \in (\mathcal{R}_1 \cup \mathcal{R}_2).\mathcal{R}$ if and only if $\big(\exists e'' : (e, e'') \in \mathcal{R}_1 \cup \mathcal{R}_2$ and $(e'', e') \in \mathcal{R}\big)$ if and only if $\big(\exists e'' : ((e, e'') \in \mathcal{R}_1$ or $(e, e'') \in \mathcal{R}_2)$ and $(e'', e') \in \mathcal{R}\big)$ if and only if $\big(\exists e'' : ((e, e'') \in \mathcal{R}_1$ and $(e'', e') \in \mathcal{R})$ or $((e, e'') \in \mathcal{R}_2$ and $(e'', e') \in \mathcal{R})\big)$ if and only if $\big(\exists e_1 : ((e, e_1) \in \mathcal{R}_1$ and $(e_1, e') \in \mathcal{R})$ or $\exists e_2 : ((e, e_2) \in \mathcal{R}_2$ and $(e_2, e') \in \mathcal{R})\big)$ if and only if $(e, e') \in \mathcal{R}_1.\mathcal{R} \cup \mathcal{R}_2.\mathcal{R}$.

1.(c) is proved in the same way as 1.(b).

2. The inclusion is straightforward ; the difference with case 1.(b) is that

$$\exists e'' : ((e, e'') \in \mathcal{R}_1 \text{ and } (e'', e') \in \mathcal{R}) \text{ and } ((e, e'') \in \mathcal{R}_2) \text{ and } (e'', e') \in \mathcal{R})$$

is not equivalent to

$$\exists e_1 : ((e, e_1) \in \mathcal{R}_1 \text{ and } (e_1, e') \in \mathcal{R}) \text{ and } \exists e_2 : ((e, e_2) \in \mathcal{R}_2 \text{ and } (e_2, e') \in \mathcal{R}).$$

Indeed, let $\mathcal{R}_1 = \{(a, b)\}$, $\mathcal{R}_2 = \{(a, c)\}$, and $\mathcal{R} = \{(b, d), (c, d)\}$. We have $\mathcal{R}_1 \cap \mathcal{R}_2 = \emptyset$, and hence $(\mathcal{R}_1 \cap \mathcal{R}_2).\mathcal{R} = \emptyset$ whilst $\mathcal{R}_1.\mathcal{R} = \mathcal{R}_2.\mathcal{R} = \{(a, d)\}$, and hence $\mathcal{R}_1.\mathcal{R} \cap \mathcal{R}_2.\mathcal{R} = \{(a, d)\}$.

1.23. 1. If $\mathcal{R}$ is left complete, then $\forall e, e' \in E, e \mathrel{\mathcal{R}} e'$. Hence, $\forall e, e' \in E$, $e' \mathcal{R}^{-1} e$, and so $\mathcal{R}^{-1}$ is right complete. The proof of the other case is symmetric.

2.(i) If $Id_E \subseteq \mathcal{R}.\mathcal{R}^{-1}$ we have $\forall e \in E, (e, e) \in \mathcal{R}.\mathcal{R}^{-1}$. As $(e, e) \in \mathcal{R}.\mathcal{R}^{-1} \Longrightarrow \exists e' : (e, e') \in \mathcal{R}$, this shows that $\mathcal{R}$ is left complete. Conversely, if $\mathcal{R}$ is left complete, then for any e there exists an e' such that $(e, e') \in \mathcal{R}$. We thus have that $(e', e) \in \mathcal{R}^{-1}$, and hence $(e, e) \in \mathcal{R}.\mathcal{R}^{-1}$.

2.(ii) If $Id_E \subseteq \mathcal{R}^{-1}.\mathcal{R} = \mathcal{R}^{-1}.(\mathcal{R}^{-1})^{-1}$ then $\mathcal{R}^{-1}$ is left complete, and hence $\mathcal{R}$ is right complete (see point 1).

3. If $(e,e') \in \mathcal{R} \cap \mathcal{R}^{-1}$ then $(e,e') \in \mathcal{R}$ and $(e,e') \in \mathcal{R}^{-1}$. So $(e',e) \in \mathcal{R}^{-1}$ and $(e',e) \in \mathcal{R}$, and hence $(e',e) \in \mathcal{R} \cap \mathcal{R}^{-1}$. If $(e,e') \in \mathcal{R} \cup \mathcal{R}^{-1}$ then $(e,e') \in \mathcal{R}$ or $(e,e') \in \mathcal{R}^{-1}$, and hence $(e',e) \in \mathcal{R}^{-1}$ or $(e',e) \in \mathcal{R}$. Thus $(e',e) \in \mathcal{R} \cup \mathcal{R}^{-1}$.

4. If $(e,e') \in \mathcal{R}_1 \cap \mathcal{R}_2$ and if $(e',e'') \in \mathcal{R}_1 \cap \mathcal{R}_2$ then $(e,e') \in \mathcal{R}_1$, $(e,e') \in \mathcal{R}_2$, $(e',e'') \in \mathcal{R}_1$, and $(e',e'') \in \mathcal{R}_2$. Because $\mathcal{R}_1$ and $\mathcal{R}_2$ are transitive, $(e,e'') \in \mathcal{R}_1$ and $(e,e'') \in \mathcal{R}_2$. Hence, $(e,e'') \in \mathcal{R}_1 \cap \mathcal{R}_2$, which is thus indeed transitive.

The relation $\mathcal{R}_1 = \{(a,b)\}$ is transitive because $\mathcal{R}_1^2 = \emptyset \subseteq \mathcal{R}_1$. Similarly, $\mathcal{R}_2 = \{(b,a)\}$ is also transitive. Their union, $\mathcal{R} = \{(a,b),(b,a)\}$, is not transitive because $\mathcal{R}^2 = \{(a,a),(b,b)\}$ is not in $\mathcal{R}$.

5. Assume that $e\ \mathcal{R}^+\ e'$ and $e'\ \mathcal{R}^+\ e''$. Therefore, there exist two integers i and j such that $e\ \mathcal{R}^i\ e'$ and $e'\ \mathcal{R}^j\ e''$. We thus have $(e,e'') \in \mathcal{R}^{i+j} \subseteq \mathcal{R}^+$.

6. Because $\mathcal{R} \subseteq \mathcal{R}^+$, we have that if $\mathcal{R} \neq \mathcal{R}^+$ then $\mathcal{R}^+ \not\subseteq \mathcal{R}$. Therefore, there exists at least one integer i such that $\mathcal{R}^i \not\subseteq \mathcal{R}$. Let i_0 be the least such integer. This integer i_0 is strictly larger than 1 because $\mathcal{R}^0 = Id_E \subseteq \mathcal{R}^+$ and $\mathcal{R}^1 = \mathcal{R} \subseteq \mathcal{R}^+$. Moreover, $\mathcal{R}^{i_0-1} \subseteq \mathcal{R}$. Because $\mathcal{R}^{i_0} \not\subseteq \mathcal{R}$, there exist e_0 and e_{i_0} such that $e_0\mathcal{R}^{i_0}e_{i_0}$ and $e_0\ \overline{\mathcal{R}}\ e_{i_0}$. Therefore, there exist $e_1, \ldots, e_{i_0-1}$ such that $e_j\ \mathcal{R}\ e_{j+1}$ for $0 \leq j < i_0$. We thus have $e_1\ \mathcal{R}^{i_0-1}\ e_{i_0}$, and hence $e_1\ \mathcal{R}\ e_{i_0}$. Because $\mathcal{R}$ is transitive we have that $e_0\ \mathcal{R}\ e_{i_0}$, a contradiction.

1.24. If $\mathcal{R}$ were symmetric, we would have $m = n+1 \iff n = m+1$, and that is impossible. If it were reflexive, we would have $n = n+1$. If it were transitive, we would have

$$m = n+1 \text{ and } p = m+1 \Longrightarrow p = n+1\,.$$

We see that $n\ \mathcal{R}^i\ m$ if and only if $m = n+i$, and hence $\mathcal{R}^+$ is the strict ordering $<$ on the integers and $\mathcal{R}^*$ is the large ordering $\leq$ (see Chapter 2).

1.25. This relation is not transitive. For instance, 2 and 6 have a common divisor (2), 6 and 3 have a common divisor (3), but the only divisor common to 2 and 3 is 1.

1.26. 1. The relation $\mathcal{R}$ is symmetric if the matrix M is symmetric (i.e. if $\forall i,j,\ m_{i,j} = m_{j,i}$). It is reflexive if there are only 1s on the diagonal, and it is irreflexive if there are only 0s. It is antisymmetric if $\forall i,j, m_{i,j} \neq m_{j,i}$.

2. $M' = M_{\mathcal{R}^{-1}}$ is the transpose of matrix $M : m'_{i,j} = m_{j,i}$. $M' = M_{\overline{\mathcal{R}}}$ is the matrix defined by $m'_{i,j} = 1 - m_{i,j}$. If $M = M_{\mathcal{R}}$ and $M' = M_{\mathcal{R}'}$, $M'' = M_{\mathcal{R}.\mathcal{R}'}$ is the matrix defined by $m''_{i,j} = 1$ if and only if $\exists k : m_{i,k}m'_{k,j} = 1$.

1.27. By Proposition 1.23, the least equivalence relation containing $\mathcal{R}$ and $\mathcal{R}'$ is $((\mathcal{R} \cup \mathcal{R}') \cup (\mathcal{R} \cup \mathcal{R}')^{-1})^*$. Because $\mathcal{R}$ and $\mathcal{R}'$ are symmetric, $\mathcal{R} \cup \mathcal{R}'$ is symmetric and equal to $(\mathcal{R} \cup \mathcal{R}')^{-1}$.

Because $\mathcal{R}$ and $\mathcal{R}'$ are reflexive, $\mathcal{R} \cup \mathcal{R}'$ contains the identity, and $(\mathcal{R} \cup \mathcal{R}')^* = (\mathcal{R} \cup \mathcal{R}')^+$ (see Exercise 1.21).

1.28. We first show that if $\mathcal{R} \subseteq \mathcal{R}'$ then $\forall e \in E$, $[e]_{\mathcal{R}} \subseteq [e]_{\mathcal{R}'}$. Indeed, $e' \in [e]_{\mathcal{R}} \Longrightarrow e'\ \mathcal{R}\ e \Longrightarrow e'\ \mathcal{R}'\ e \Longrightarrow e' \in [e]_{\mathcal{R}'}$. Hence, $E/\mathcal{R}$ is a refinement of $E/\mathcal{R}'$.

Conversely, we let $e, e' \in E$ be such that $e\ \mathcal{R}\ e'$ and show that $e\ \mathcal{R}'\ e'$. As $e\ \mathcal{R}\ e'$, $e' \in [e]_{\mathcal{R}}$; since $E/\mathcal{R}$ is a refinement of $E/\mathcal{R}'$, there exists $e'' \in E$ such that $[e]_{\mathcal{R}} \subseteq [e'']_{\mathcal{R}'}$. We thus have $e' \in [e'']_{\mathcal{R}'}$ and $e \in [e'']_{\mathcal{R}'}$ (because $e, e' \in [e]_{\mathcal{R}}$), and hence $e\ \mathcal{R}'\ e''\ \mathcal{R}'\ e'$.

1.29. 1. Straightforward.

2. Assume $\mathcal{R}$ is antisymmetric, and let $x, y \in E$ be such that $x \neq y$. Because $x\ \mathcal{R}\ y$ and $y\ \mathcal{R}\ x$ cannot hold simultaneously, we can assume without loss of generality that $x\ \overline{\mathcal{R}}\ y$. There thus exists $X \in \mathcal{F}_x \setminus \mathcal{F}_y$ (i.e. $\exists X \in \mathcal{F}$ such that $x \in X$ and $y \notin X$), and hence $|X \cap \{x,y\}| = 1$.

Conversely, let x and y be two distinct elements of E and let $X \in \mathcal{F}$ be such that $|X \cap \{x,y\}| = 1$. For instance, $x \in X$ and $y \notin X$ (i.e. $X \in \mathcal{F}_x \setminus \mathcal{F}_y$). Hence, $x\ \overline{\mathcal{R}}\ y$.

3. Let $x, y \in E$ be such that $x \mathcal{R} y$ (i.e. $\mathcal{F}_x \subseteq \mathcal{F}_y$). Let $X \in \mathcal{F}_y$ and $\overline{X} \in (\mathcal{F} \setminus \mathcal{F}_y) \subseteq (\mathcal{F} \setminus \mathcal{F}_x)$. Then $X \in \mathcal{F}_x$ and we have that $\mathcal{F}_y \subseteq \mathcal{F}_x$, and hence $y \mathcal{R} x$.

4. If $\mathcal{R}$ is symmetric, it is an equivalence relation. We show that for all $x \in E$, we have $[x] = \bigcap_{X \in \mathcal{F}_x} X$. Let $y \in [x]$. We have $x \mathcal{R} y$, and hence $\forall X \in \mathcal{F}_x, y \in X$ (i.e. $y \in \bigcap_{X \in \mathcal{F}_x} X$). Conversely, let $y \in \bigcap_{X \in \mathcal{F}_x} X$. We have $\mathcal{F}_x \subseteq \mathcal{F}_y$, and hence $x \mathcal{R} y$ (i.e. $y \in [x]$).

Because $\mathcal{F}$ is closed by intersection, we deduce that $\forall x \in E, [x] \in \mathcal{F}$.

Letting $X \in \mathcal{F}$, we show that X is a union of equivalence classes. Let $x \in X$. We have that $X \in \mathcal{F}_x$ and thus $[x] = \bigcap_{Y \in \mathcal{F}_x} Y \subseteq X$. We thus have $X = \bigcup_{x \in X} [x]$.

We deduce $\overline{X} = \bigcup_{x \notin X} [x]$. Since $\mathcal{F}$ is closed by union, we have $\overline{X} \in \mathcal{F}$.

1.30. 1. Commutativity of + and × is clear and associativity is easily checked. The units of + and × are $(0, 1)$ and $(1, 1)$.

2. Reflexivity and symmetry are straightforward. Transitivity follows immediately from the property : $(a, b) \sim (c, d)$ if and only if $\dfrac{a}{b} = \dfrac{c}{d}$ in $\mathbb{Q}$. But the goal of the exercise is the definition of $\mathbb{Q}$, and so a direct proof of this result follows.

Assume that $(a, b) \sim (c, d) \sim (e, f)$. We have $ad = bc$ and $cf = de$. Thus $adf = bcf = bde$, and because $d \neq 0, af = be$ (i.e. $(a, b) \sim (e, f)$). Let us show now that $\sim$ is a congruence. Assume that $(a, b) \sim (c, d)$ and let $(e, f) \in E$. We have $(a, b) + (e, f) = (af + be, bf)$ and $(c, d) + (e, f) = (cf + de, df)$. Therefore,

$$(af + be) \times df = adf^2 + bdef = bcf^2 + bdef = bf(cf + de).$$

Hence, $(a, b) + (e, f) \sim (c, d) + (e, f)$, which shows that $\sim$ is a congruence for + because this operation is commutative. We show similarly that $\sim$ is a congruence for ×.

3. Let $(a, b) \in E$. We have that $(a, b) + (-a, b) = (ab - ab, bb) = (0, bb)$ and $(0, bb) \sim (0, 1)$. Hence, in $E/\sim$ the inverse of $[(a, b)]$ for $[+]$ is $[(-a, b)]$. The distributivity of $[\times]$ over $[+]$ is easily verified.

Let $[(a, b)]$ be an element of $E/\sim$ with $[(c, d)]$ as its inverse for $[\times]$. We have that $(a, b) \times (c, d) = (ac, bd) \sim (1, 1)$, and hence $ac = bd \neq 0$ and $[(a, b)] \neq [(0, 1)]$. Conversely, if $[(a, b)] \neq [(0, 1)]$ then $a \neq 0$ and $(b, a) \in E$. We then have that $(a, b) \times (b, a) = (ab, ab) \sim (1, 1)$, and hence $[(b, a)]$ is the inverse of $[(a, b)]$ for $[\times]$.

Chapter 2

2.1. Because $\mathcal{E} = Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1})$ is included in $Id_E \cup \mathcal{R}$ and because $\mathcal{R}$ is transitive, we indeed have $\mathcal{E}.\mathcal{R}.\mathcal{E} \subseteq \mathcal{R}$.

2.2. The relation $\mathcal{R}^\dagger$ is reflexive by definition.

If $x \mathcal{R}^\dagger y$ and $y \mathcal{R}^\dagger x$, and if $x \neq y$, then

$$x \,\mathcal{R}\, y \ , \ y \,\overline{\mathcal{R}}\, x \ , \ y \,\mathcal{R}\, x \ , \ x \,\overline{\mathcal{R}}\, y,$$

a contradiction. We must thus have that $x = y$, and the relation is antisymmetric.

To show the transitivity of $\mathcal{R}^\dagger$, it suffices to show that if $x \mathcal{R}^\dagger y$ and $y \mathcal{R}^\dagger z$, with $x \neq y$, $y \neq z$ and $x \neq z$, then $x \mathcal{R}^\dagger z$. By the definition of $\mathcal{R}^\dagger$, we have

$$x \,\mathcal{R}\, y \ , \ y \,\overline{\mathcal{R}}\, x \ , \ y \,\mathcal{R}\, z \ , \ z \,\overline{\mathcal{R}}\, y.$$

Since $\mathcal{R}$ is a transitive relation, $x \mathcal{R} z$. Assume that $z \mathcal{R} x$; we thus also have, by the transitivity of $\mathcal{R}$, $z \mathcal{R} y$, which is excluded. Hence, $z \overline{\mathcal{R}} x$ and thus $x \mathcal{R}^\dagger z$.

2.3. First, we show a slightly stronger result than the mere existence of a linear extension, namely :

> if we are given two incomparable elements e and e' in E, then there is a linear extension $\leq_t$ of $\leq$ such that $e \leq_t e'$.

Note that if E does not contain two incomparable elements, then it is totally ordered and the existence of a linear extension is clear.

We prove this result by induction on the number n of elements of E. If $n = 0$ or $n = 1$, the property holds vacuously because E does not contain two elements.

We assume $|E| = n + 1$, with $n > 0$. With each element x of E, we associate an integer $r(x)$ defined as the cardinality of the set $\{y \in E \,/\, y < x\}$. It is clear that $x < x' \Longrightarrow r(x) < r(x')$. Moreover, if $r(x) > 0$, there exists a y such that $y < x$. We easily deduce

$$\forall x \in E, r(x) > 0 \Longrightarrow \exists x' < x : r(x') = 0.$$

We then let

$$x_0 = \begin{cases} e & \text{if } r(e) = 0, \\ x & \text{otherwise.} \end{cases}$$

where x is an arbitrary element of E such that $x < e$ and $r(x) = 0$.

By the induction hypothesis, there is a linear extension $\leq'_t$ of the restriction of $\leq$ to $E \setminus \{x_0\}$, and it can be chosen such that $e \leq'_t e'$ if $e \neq x_0$. We then obtain the required result by defining $\leq_t = \leq'_t \cup \{(x_0, x) \,/\, x \in E\}$.

Let $\leq'$ be the intersection of the linear extensions of $\leq$. We have that $\leq \, \subseteq \, \leq'$. If the equality does not hold, then there must exist x and y (where $x \neq y$) such that $x \leq' y$ and $x \not\leq y$. We have that $y \not\leq x$, because if $y \leq x$ we would also have that $y \leq' x$ and thus $x = y$. We have just seen that it is possible to find a linear extension $\leq_t$ of $\leq$ such that $y \leq_t x$. As $\leq' \, \subseteq \, \leq_t$, we also have $x \leq_t y$ and thus $x = y$, a contradiction.

2.4. 1. We have $(x_1, x_2) \leq (y_1, y_2) \Longrightarrow \pi_i(x_1, x_2) = x_i \leq y_i = \pi_i(y_1, y_2)$.

2. Let $E = \{a, b\}$ with $a < b$. In $E \times E$, (a, b) and (b, a) are incomparable.

3. Let b be the bijection from $(E_1 \times E_2) \times E_3$ to $E_1 \times (E_2 \times E_3)$ associating $(x_1, (x_2, x_3))$ with $((x_1, x_2), x_3)$. It is an isomorphism because

$$\begin{aligned} ((x_1, x_2), x_3) \leq ((y_1, y_2), y_3) &\Longleftrightarrow (x_1, x_2) \leq (y_1, y_2) \text{ and } x_3 \leq_3 y_3 \\ &\Longleftrightarrow x_1 \leq_1 y_1, x_2 \leq_2 y_2 \text{ and } x_3 \leq_3 y_3 \\ &\Longleftrightarrow x_1 \leq_1 y_1 \text{ and } (x_2, x_3) \leq (y_2, y_3) \\ &\Longleftrightarrow (x_1, (x_2, x_3)) \leq (y_1, (y_2, y_3)). \end{aligned}$$

Similarly,

$$(x_1, x_2) \leq (y_1, y_2) \Longleftrightarrow x_1 \leq_1 y_1 \text{ and } x_2 \leq_2 y_2 \Longleftrightarrow (x_2, x_1) \leq (y_2, y_1).$$

2.5. 1. Obvious.

2. Let $E_1 = \{a, b\}$ with $a < b$ and $E_2 = \{c, d\}$, where c and d are incomparable. The lexicographic ordering on $E_2 \times E_1$ is $\{(ca, cb), (da, db)\}$. The lexicographic ordering on $E_1 \times E_2$ is $\{(ac, bc), (ac, bd), (ad, bc), (ad, bd)\}$.

3. Let (x_1, x_2) and (y_1, y_2) be in $E_1 \times E_2$. Because E_1 is totally ordered, three cases are possible :

- $x_1 < y_1$, and in this case $(x_1, x_2) < (y_1, y_2)$,
- $y_1 < x_1$, and in this case $(y_1, y_2) < (x_1, x_2)$,
- $x_1 = y_1$, and, because E_2 is totally ordered,
  - either $x_2 \leq y_2$, and then $(x_1, x_2) \leq (y_1, y_2)$,
  - or $y_2 \leq x_2$ and $(y_1, y_2) \leq (x_1, x_2)$.

2.6. 1. Let E' be an antichain having at least two distinct elements x and y. Because E is totally ordered, assume that e.g. $x < y$. Then the relation $\leq \cap (E' \times E')$ contains the pair (x, y) and cannot be equal to the identity.

2. It follows that an antichain of an ordered set, or the intersection of a chain and an antichain, cannot contain two or more elements, because then we could find an antichain containing two distinct elements x and y with $x < y$.

2.7. If $x \leq y$, then $[x, y]$ contains x and y. If $[x, y]$ is non-empty, then there exists z such that $x \leq z$ and $z \leq y$, and hence $x \leq y$.

2.8. Assume that no element of $[x, y]$ covers x. We thus have

$$\forall z \in [x, y], \exists z' \in [x, z] : x \neq z' \text{ and } z \neq z'.$$

In other words, $\forall z \in [x, y]$, $\exists z' : x < z' < z$.

We can thus construct a sequence $(z_i)_{i \geq 0}$ of elements of $[x, y]$ such that $z_0 = y$ and $\forall i \geq 0$, $x < z_{i+1} < z_i \leq y$, contradicting the fact that $[x, y]$ is finite.

2.9. By definition of the covering relation, $\prec \subseteq \leq$; because $\leq$ is a reflexive and transitive relation and $\prec^*$ is the least reflexive and transitive relation containing $\prec$, we have $\prec^* \subseteq \leq$.

Conversely, let us show by complete induction the property

$$\forall n, \forall x, y \in E, \qquad x < y \text{ and } |[x, y]| \leq n \qquad \Longrightarrow \qquad x \prec^* y.$$

Assume that $x < y$ and $|[x, y]| = n$. By Exercise 2.8, there exists z such that $x \prec z$ and $z \leq y$. If $z = y$, we have $x \prec^* y$. Otherwise, $[z, y] \subseteq [x, y] \setminus \{x\}$ and $|[z, y]| < n$. By the induction hypothesis, $z \prec^* y$ and thus $x \prec^* y$.

2.10. 1. Consider the ordered set E obtained by adding to $\mathbb{N}$, equipped with the usual ordering on the integers, an element a, incomparable to any other element. Let $E' = E$. Element a is indeed the unique maximal element of E', but it is not the greatest element.

2. If E is totally ordered, then any finite subset has a unique maximal element which is also the greatest element. The converse is false : the set E of Example 2.25, 2, is such that for any subset having a unique maximal element, this maximal element is also the greatest element, but E is not totally ordered.

2.11. The same proof as in Example 2.30, 3, shows that $\preceq'$ is a well-founded ordering. This proof shows that in general the lexicographic product of two well-founded sets is also a well-founded set.

Moreover, $\preceq'$ is a total ordering because $<_1$ and $<_2$ are total orderings.

2.12. 1. The 'only if' direction is clear. 'If' direction : we prove by induction on n that any n-element subset has a least upper bound and a greatest lower bound.

2. The 'only if' direction is clear. 'If' direction : let F be any subset of E, and let $\text{Min}(F)$ be the set of lower bounds of F, then the least upper bound of $\text{Min}(F)$ is the greatest lower bound of F.

2.13. Let x and y be two elements of e such that $x \leq y$. Clearly, $\sup(\{x, y\}) = y$, and the continuity of f implies that $\sup(\{f(x), f(y)\}) = f(y)$, and hence $f(x) \leq f(y)$.

2.14. 1. $f(\perp) = \perp$ because $\sup(\emptyset) = \perp$ and because f preserves the least upper bound of $\emptyset$.

2. If $f(\perp) = \perp$, the least fixed point of f is $\perp$.

2.15. Let $(X_i)_{i\geq 0}$ be a sequence of subsets of $E \times E$. Let $\mathcal{R}_1 = Id_E \cup \mathcal{R}.(\bigcup_{i\geq 0} X_i)$ and $\mathcal{R}_2 = \bigcup_{i\geq 0}(Id_E \cup \mathcal{R}.X_i)$. Show that $\mathcal{R}_1 = \mathcal{R}_2$, which proves the continuity of f.

$$\begin{aligned}(x,y) \in \mathcal{R}_1 &\iff x = y \text{ or } \exists z : x \; \mathcal{R} \; z \text{ and } (z,y) \in \bigcup_{i\geq 0} X_i \\ &\iff x = y \text{ or } \exists z : x \; \mathcal{R} \; z \text{ and } \exists i : (z,y) \in X_i. \\ (x,y) \in \mathcal{R}_2 &\iff \exists i : x = y \text{ or } \exists z : x \; \mathcal{R} \; z \text{ and } (z,y) \in X_i.\end{aligned}$$

We see that these two conditions are equivalent.

The least element of $\mathcal{P}(E \times E)$ is the empty relation $\emptyset_E$. By Theorem 2.40, the least fixed point of f is $\bigcup_{k\geq 0} f^k(\emptyset_E)$. The result is then immediately deduced from the identity

$$f^{k+1}(\emptyset_E) = Id_E \cup \mathcal{R} \cup \mathcal{R}^2 \cup \cdots \cup \mathcal{R}^k.$$

This identity is easily proved by induction. Indeed,

$$\begin{aligned} f^0(\emptyset_E) &= \emptyset_E, \\ f^1(\emptyset_E) &= Id_E \cup \mathcal{R}.\emptyset_E = Id_E, \\ f^2(\emptyset_E) &= f(Id_E) = Id_E \cup \mathcal{R}.Id_E = Id_E \cup \mathcal{R}, \\ &\vdots \\ f^{k+2}(\emptyset_E) &= f(Id_E \cup \mathcal{R} \cup \mathcal{R}^2 \cup \cdots \cup \mathcal{R}^k) \\ &= Id_E \cup \mathcal{R}.(Id_E \cup \mathcal{R} \cup \mathcal{R}^2 \cup \cdots \cup \mathcal{R}^k) \\ &= Id_E \cup \mathcal{R} \cup \mathcal{R}^2 \cup \cdots \cup \mathcal{R}^k \cup \mathcal{R}^{k+1}, \\ &\vdots \end{aligned}$$

2.16. Because $x \sqcap y \leq x$ and $x \sqcap y \leq y$, we also have that $x \sqcap y \leq x'$ and $x \sqcap y \leq y'$ and thus $x \sqcap y$ is less than or equal to the greatest lower bound $x' \sqcap y'$ of x' and y'.

Similarly, $x' \leq x' \sqcup y'$ and $y' \leq x' \sqcup y'$, and hence $x \leq x' \sqcup y'$ and $y \leq x' \sqcup y'$. Thus $x \sqcup y \leq x' \sqcup y'$.

2.17. 1. We must show the identity

$$\gcd(x, \operatorname{lcm}(y,z)) = \operatorname{lcm}(\gcd(x,y), \gcd(y,z))\,.$$

We decompose x, y and z into products of primes. We can thus write

$$\begin{aligned} x &= p_0^{n_0} p_1^{n_1} \cdots p_k^{n_k}, \\ y &= p_0^{m_0} p_1^{m_1} \cdots p_k^{m_k}, \\ x &= p_0^{r_0} p_1^{r_1} \cdots p_k^{r_k}, \end{aligned}$$

where $p_0, p_1, \ldots, p_k$ are the $k+1$ first primes, and where their exponents are positive or null integers. The fact that $p_0^{a_0} p_1^{a_1} \cdots p_k^{a_k}$ divides $p_0^{b_0} p_1^{b_1} \cdots p_k^{b_k}$ can hence be written as : $\forall i, a_i \leq b_i$. We can thus also represent the number 0 in this form (even though it is not a product of primes) by assuming that all exponents are infinite.

Moreover, the lcm of the two numbers $p_0^{a_0} p_1^{a_1} \cdots p_k^{a_k}$ and $p_0^{b_0} p_1^{b_1} \cdots p_k^{b_k}$ is equal to

$$p_0^{\sup(a_0,b_0)} p_1^{\sup(a_1,b_1)} \cdots p_k^{\sup(a_k,b_k)}$$

and their gcd is equal to

$$p_0^{\inf(a_0,b_0)} p_1^{\inf(a_1,b_1)} \cdots p_k^{\inf(a_k,b_k)} .$$

We thus have to show that for any three integers, possibly equal to ∞, we have

$$\inf(n, \sup(m,r)) = \sup(\inf(n,m), \inf(n,r)) .$$

Without loss of generality we can assume $m \leq r$. In this case $\inf(n,m) \leq \inf(n,r)$ and

$$\inf(n, \sup(m,r)) = \inf(n,r) = \sup(\inf(n,m), \inf(n,r)) .$$

2. If the lattice is complemented, then for any integer n there exists an integer m such that $\gcd(n,m) = 1$ and $\mathrm{lcm}(n,m) = 0$. Let $n > 1$; then we must have that $m \neq 0$, because otherwise n would be a common divisor of n and 0. On the other hand, the lcm of two numbers must necessarily divide their product ; thus nm divides 0, and this implies $m = 0$, a contradiction.

2.18. 1. If $\mathcal{R}_1$ and $\mathcal{R}_2$ are two equivalence relations, then $\mathcal{R}_1 \sqcap \mathcal{R}_2 = \mathcal{R}_1 \cap \mathcal{R}_2$ and $\mathcal{R}_1 \sqcup \mathcal{R}_2$ is the least equivalence relation containing $\mathcal{R}_1$ and $\mathcal{R}_2$ (see Exercise 1.27).

2. Consider the three equivalence relations $\equiv_1$, $\equiv_2$ and $\equiv_3$ on $E = \{a,b,c\}$ whose equivalence classes are, respectively :

$$\{a,c\}, \{b\}$$
$$\{a,b\}, \{c\}$$
$$\{b,c\}, \{a\}$$

It is easy to see that $(\equiv_1 \cap \equiv_2) = (\equiv_1 \cap \equiv_3) = Id_E$. The least upper bound of the two equivalence relations $\equiv_1 \cap \equiv_2$ and $\equiv_1 \cap \equiv_3$ is thus Id_E. Since $a \equiv_2 b \equiv_3 c$, the least upper bound of the relations $\equiv_2$ and $\equiv_3$ is the full relation, whose intersection with $\equiv_1$ is $\equiv_1$. Thus :

$$\equiv_1 \cap (\equiv_2 \cup \equiv_3) \neq (\equiv_1 \cap \equiv_2) \cup (\equiv_1 \cap \equiv_3)$$

and the lattice of equivalence relations is not distributive.

3. Although it is not distributive, the lattice of equivalence relations is nevertheless complemented (but the complement is not unique). Let $\equiv$ be an equivalence relation on E. With each equivalence class C we associate an arbitrary element x_C of that class. Let X be the set of these elements. We thus have $\forall e \in E, |X \cap [e]_\equiv| = 1$.

Let $\equiv'$ be the equivalence relation whose classes are X and $\{y\}$ for any $y \in E \setminus X$. Then $\equiv \cap \equiv' = Id_E$. Indeed, let e and e' be such that $e \equiv e'$ and $e \equiv' e'$. Because $e \equiv' e'$, if $e \notin X$ then $e = e'$, and if $e \in X$ then $e' \in X$ and $\{e,e'\} \subseteq X \cap [e]_\equiv$, and hence $e = e'$. On the other hand, the least upper bound of the relations $\equiv$ and $\equiv'$ is the full relation. Indeed, let y_1 and y_2 be any two elements of E. Let, for $i = 1,2$,

$$y'_i = \begin{cases} y_i & \text{if } y_i \in X, \\ x_{[y_i]_\equiv} & \text{otherwise.} \end{cases}$$

We then have : $y_1 \equiv y'_1 \equiv' y'_2 \equiv y_2$.

2.19. $\nu(\bot) = \nu(\bot) \sqcup \bot = \top$, $\nu(\top) = \nu(\top) \sqcap \top = \bot$.

2.20. We assume that there exists an element x such that $x = \nu(x)$. We then have :

$$x = x \sqcap x = x \sqcap \nu(x) = \bot \ ,$$
$$x = x \sqcup x = x \sqcup \nu(x) = \top \ .$$

Hence $\bot = \top$, a contradiction.

Chapter 3

3.1. The case $r = 1$ is clear for S_n and was studied in Example 3.3 for T_n. Let $r \neq 1$. We consider the property $P(n)$: ‘ $S_n = \dfrac{r^{n+1}-1}{r-1}$ ’. We verify

$$P(0)\colon \quad S_0 = r^0 = 1 = \frac{r-1}{r-1}\,.$$

Let $n \geq 0$. We assume that $P(n)$ is true and we verify

$$P(n+1)\colon \quad S_{n+1} = S_n + r^{n+1} = \frac{r^{n+1}-1}{r-1} + r^{n+1} = \frac{r^{n+2}-1}{r-1}\,.$$

We thus deduce that $\forall n \geq 0$, $S_n = \dfrac{r^{n+1}-1}{r-1}$. The proof is similar for T_n.

3.2. 1. Let $P(n)$ be the property ‘$S_n = 2n^4 - n^2$’. $P(1)$ is true because $S_1 = 1 = 2 - 1$. Let $n \geq 1$. We assume $P(n)$. We have $S_{n+1} = S_n + (2n+1)^3 = 2n^4 - n^2 + (2n+1)^3 = 2n^4 + 8n^3 + 11n^2 + 6n + 1 = 2(n+1)^4 - (n+1)^2$. Thus $P(n+1)$ is true. We deduce $\forall n \geq 1$, $P(n)$.

2. We note that $T_1 = \frac{1}{3}, T_2 = \frac{1}{3} + \frac{1}{15} = \frac{2}{5}$ and $T_3 = \frac{1}{3} + \frac{1}{15} + \frac{1}{35} = \frac{3}{7}$. We guess the property $Q(n)$: ‘$T_n = \dfrac{n}{2n+1}$’ that we prove by induction.

We have already verified $Q(1)$, $Q(2)$ and $Q(3)$. Let $n \geq 1$ be such that $Q(n)$ is true. We have

$$\begin{aligned} T_{n+1} = T_n + \frac{1}{4(n+1)^2-1} &= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \\ &= \frac{2n^2+3n+1}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}\,. \end{aligned}$$

Hence $Q(n+1)$ is true. We deduce that $\forall n \geq 1$, $Q(n)$.

3.3. 1. We have $P(x+1) - P(x) = x^2 + (2a+1)x + (a+b+1/3)$. The property is thus verified if and only if $2a+1 = 0$ and $a+b+1/3 = 0$, i.e. $a = -1/2$ and $b = 1/6$.

2. We prove this by induction on n. Let $Q(n)$ be the property ‘$P(n)$ is an integer’. $P(0) = 0$, and hence $Q(0)$ is true. Let $n \geq 0$ and assume $Q(n)$ is true. $P(n+1) = P(n) + n^2$, and hence $Q(n+1)$ is true. We deduce $\forall n \geq 0, Q(n)$.

3. We prove by induction the property $R(n)\colon S_n = P(n+1)$. $S_0 = 0 = P(1)$, and thus $R(0)$ is true. Let $n \geq 0$, and assume $R(n)$. We have $S_{n+1} = S_n + (n+1)^2 = P(n+1) + (n+1)^2 = P(n+2)$, and hence $R(n+1)$ is true. We deduce $\forall n \geq 0$, $R(n)$.

Finally, $\dfrac{n(n+1)(2n+1)}{6} = \dfrac{1}{3}n^3 + \dfrac{1}{2}n^2 + \dfrac{1}{6}n = P(n) + n^2 = P(n+1)$.

3.4. By induction on n. Let $P(n)$ be the property ‘$\forall A \subseteq \{1, 2, \ldots, 2n\}$ such that $|A| \geq n+1$, $\exists a, b \in A$ such that $a < b$ and $a \mid b$’, where the relation $\mid$ means ‘divides’, i.e. $a \mid b \iff (\exists c \in \mathbb{N}, b = ac)$.

We verify $P(1)$: if $A \subseteq \{1, 2\}$ and $|A| \geq 2$ then $A = \{1, 2\}$ and the pair $(a, b) = (1, 2)$ is suitable.

For $n \geq 1$ we assume $P(n)$ and show $P(n+1)$. Let $A \subseteq \{1, 2, \ldots, 2n+2\}$ be such that $|A| \geq n+2$. Let $B = A \cap \{1, 2, \ldots, 2n\}$. If $|B| \geq n+1$ then by hypothesis $\exists a, b \in B \subseteq A$ such that $a < b$ and $a|b$. Otherwise, $\{2n+1, 2n+2\} \subseteq A$ must hold. If $n+1 \in A$ then the pair $(n+1, 2n+2)$ is suitable. Otherwise, $|B \cup \{n+1\}| \geq n+1$ and $\exists a, b \in B \cup \{n+1\}$ such that $a < b$ and $a|b$. Necessarily, $a \neq n+1$. If $b \neq n+1$ then $a, b \in A$ are suitable. Otherwise, $a, 2n+2 \in A$ are suitable because $a|b$ and $b|(2n+2)$. Finally, $P(n+1)$ is true and we deduce $\forall n \geq 1$, $P(n)$.

3.5. We show this result by induction on i. If $i = 0$ then, since $\mathcal{R}^0 = Id_E$ is the unit of the product of relations, $\mathcal{R}^j = \mathcal{R}^0.\mathcal{R}^j$. We assume that $\mathcal{R}^{i+j} = \mathcal{R}^i.\mathcal{R}^j$. Since the product of relations is associative, $\mathcal{R}^{i+1} = \mathcal{R}.\mathcal{R}^i$, we have

$$\mathcal{R}^{i+1}.\mathcal{R}^j = \mathcal{R}.\mathcal{R}^i.\mathcal{R}^j = \mathcal{R}.\mathcal{R}^{i+j} = \mathcal{R}^{i+1+j}.$$

3.6. 1. Let $n \in \mathbb{N}$. We assume $P(n) : \exists k \in \mathbb{N},\ 10^n - 1 = 9k$ and we show $P(n+1)$. We have $10^{n+1} - 1 = 10(10^n - 1) + 10 - 1 = 9(10k+1)$ and hence $9 \mid 10^{n+1} - 1$. The proof is similar for Q : we assume $\exists k \in \mathbb{N},\ 10^n + 1 = 9k$ and we deduce $10^{n+1} + 1 = 10(10^n + 1) - 10 + 1 = 9(10k - 1)$.

2. $P(0)$ is true because $10^0 - 1 = 0 = 9 \times 0$, and hence $\forall n \geq 0, P(n)$. $Q(0)$ is false because $10^0 + 1 = 2$. Hence, we can draw no conclusion. In fact we will show that $\forall n \geq 0$, $Q(n)$ is false. More precisely, we show that $R(n)$: 'the remainder of the division of $10^n + 1$ by 9 is 2'.

$R(0)$ is true because $10^0+1 = 2$. Let $n \in \mathbb{N}$ be such that $R(n)$ is true : $\exists k \in \mathbb{N}, 10^n+1 = 9k+2$. We show $R(n+1) : 10^{n+1} + 1 = 10(10^n + 1) - 10 + 1 = 90k + 11 = 9(10k+1) + 2$. Thus $\forall n \geq 0$, $R(n)$.

3.7. In fact the inductive step (I) holds only for $n \geq 2$. An individual number n is indeed a member of G_1, but in order for it to also be a member of G_2, it is necessary (and sufficient) that n be greater than or equal to 2. We have thus shown $P(1)$ and $\forall n \geq 2$, $P(n) \Longrightarrow P(n+1)$. We can draw no conclusion.

3.8. Let P be a property depending on n. If P verifies (B) and (I), then P verifies (I′) : indeed, (B) and (I) imply that $\forall n, P(n)$, and hence (I′) is true.

Conversely, if P verifies (I′), then :

- P verifies (B) by Remark 3.5, 1, and hence $P(0)$ is true,
- P verifies (I) : otherwise, $\exists n, \neg\big(P(n) \Longrightarrow P(n+1)\big)$ (see Chapter 5). Let n_0 be the least n such that $\big(P(n_0) \Longrightarrow P(n_0+1)\big)$ is false ; we then have : $\big(\forall k < n_0 + 1, P(k)\big)$ and $\neg P(n_0 + 1)$, which contradicts (I′).

On structures more complex than $\mathbb{N}$, the second induction principle is more powerful than the first one. In fact, the first induction principle may even not hold, as is shown by the next example. Consider the set $2\omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$, consisting of two consecutive copies of $\mathbb{N}$. Let $P(x)$ be the property 'x is finite'. P verifies (B) and (I), but P is false on 2ω, because $P(\omega)$, $P(\omega+1)$, etc., are false. On the other hand, P does not verify (I′), because $\forall k < \omega$, $P(k)$, whilst $P(\omega)$ does not hold.

3.9. 1. Here, induction is not needed ; it suffices to expand and simplify.

2. We prove by induction the property

$$P(m)\text{:}\quad \text{`}\exists n \in \mathbb{N}\,,\ \exists \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{-1, 1\}\,,\ \ m = \varepsilon_1 1^2 + \varepsilon_2 2^2 + \cdots + \varepsilon_n n^2\,\text{'}.$$

$P(0)$: $0 = 1^2 + 2^2 - 3^2 + 4^2 - 5^2 - 6^2 + 7^2$,

$P(1)$: $1 = 1^2$,

$P(2)$: $2 = -1^2 - 2^2 - 3^2 + 4^2$,

$P(3)$: $3 = -1^2 + 2^2$.

Let $m \geq 4$; assume that $\forall k < m$, $P(k)$. $P(m-4)$ is thus true :

$$\exists n \in \mathbb{N}\,,\ \exists \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{-1, 1\}\,,\ \ (m-4) = \varepsilon_1 1^2 + \varepsilon_2 2^2 + \cdots + \varepsilon_n n^2\,.$$

We deduce $m = \varepsilon_1 1^2 + \varepsilon_2 2^2 + \cdots + \varepsilon_n n^2 + (n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4)^2$ and hence $P(m)$ is true.

Using the second induction principle, we can deduce $\forall n \geq 0$, $P(n)$.

3.10. One implication is straightforward. If $p, q \in \mathbb{N}$ exist such that $u = w^p$ et $v = w^q$, we have $u \cdot v = w^{p+q} = v \cdot u$.

The converse implication is proved by induction on $|u| + |v|$. That is, we consider the property $P(n)$: '$\forall u, v \in A^*$ such that $|u| + |v| = n$ we have $u \cdot v = v \cdot u \implies \exists w \in A^*, \exists p, q \in \mathbb{N}$: $u = w^p$ and $v = w^q$'. We use the second induction principle on $\mathbb{N}$. Let $n \in \mathbb{N}$. We assume that $\forall k < n, P(k)$ is true. Let $u, v \in A^*$ be such that $|u| + |v| = n$. By symmetry we can assume $|u| \leq |v|$, and hence figure 15.2.

Figure 15.2

u is thus a prefix of v. If $u = \varepsilon$ or $u = v$, then we obtain the result by letting $w = v$. If u is a proper prefix of v, let $v' \in A^*$ be such that $v = uv'$. We easily verify that $v'u = v = uv'$. As $|v'| < |v|$, we apply the induction hypothesis to the pair (u, v') : $\exists w \in A^*, \exists p, q \in \mathbb{N}$ such that $u = w^p$ and $v' = w^q$. Since $v = u \cdot v'$ we deduce $v = w^{p+q}$, and this concludes the proof.

3.11. We show, first, that $L^* = L \cdot L^* \cup \{\varepsilon\}$. Indeed,

$$L^* = \cup_{n \geq 0} L^n = L^0 \cup \Big(\cup_{n \geq 1} L^n\Big) = \{\varepsilon\} \cup \Big(\cup_{n \geq 0} L \cdot L^n\Big) = \{\varepsilon\} \cup L \cdot L^*$$

We deduce that $L^* \cdot M = \{\varepsilon\} \cdot M \cup L \cdot L^* \cdot M$. Therefore, the language $L^* \cdot M$ is a solution of the equation $X = L \cdot X \cup M$.

We now show that this solution is unique. Let $X \subseteq A^*$ be such that $X = L \cdot X \cup M$. In order to show that $L^* \cdot M \subseteq X$ it suffices to prove that $\forall n \in \mathbb{N}$, $L^n \cdot M \subseteq X$ because $L^* \cdot M = \bigcup_{n \geq 0} L^n \cdot M$. Hence, we show by induction the property $P(n)$: '$L^n \cdot M \subseteq X$'. We have $L^0 \cdot M = \{\varepsilon\} \cdot M = M \subseteq M \cup L \cdot X = X$. Thus $P(0)$ is true. Let $n \in \mathbb{N}$ and assume that $P(n)$ holds. We have $L^{n+1} \cdot M = L \cdot L^n \cdot M \subseteq L \cdot X \subseteq L \cdot X \cup M = X$. Thus $P(n+1)$ is true.

Conversely, we prove by induction the property

$$Q(n): \quad \text{'}\big(w \in X \text{ and } |w| = n\big) \implies w \in L^* \cdot M\text{'},$$

which will prove the reverse inclusion. We use the second induction principle. Let $n \in \mathbb{N}$. We assume that $\forall k < n, Q(k)$ is true. Let $w \in X$ be such that $|w| = n$. Since $X = L \cdot X \cup M$, two cases may occur. Either $w \in M$ and we have directly $w \in L^* \cdot M$ since $M \subseteq L^* \cdot M$. Moreover, $w \in L \cdot X$ and $\exists (u, v) \in L \times X$ such that $w = u \cdot v$. Since $\varepsilon \notin L$, we obtain $|u| > 0$ and hence $|v| = |w| - |u| < |w|$. By the induction hypothesis, we have $v \in L^* \cdot M$. Therefore, $w = u \cdot v \in L \cdot L^* \cdot M \subseteq L^* \cdot M$. This proves that $Q(n)$ is true and concludes the proof.

3.12. In order to prove that $X \subseteq BT$, we show by induction the property $P(n)$: '$BT_n \subseteq X$'.

BT_0 is reduced to the unique element of the basis of the inductive definition of BT, and hence $BT_0 \subseteq BT$ and $P(0)$ is verified. Let $n \in \mathbb{N}$, and assume $P(n)$ is true. Let $a \in A$ and let $l, r \in BT_n$. By the induction hypothesis, $BT_n \subseteq BT$. Thus applying the inductive step of the definition of BT we obtain $(a, l, r) \in BT$. Hence,

$$\{(a, l, r) \,/\, a \in A, l, r \in BT_n\} \subseteq BT\,.$$

We deduce $BT_{n+1} \subseteq BT$ by again using the inductive hypothesis : $BT_n \subseteq BT$. Therefore, $\forall n \in \mathbb{N}, BT_n \subseteq BT$ and thus $X = \bigcup_{n \in \mathbb{N}} BT_n \subseteq BT$.

Conversely, in order to show that $BT \subseteq X$, it suffices to prove that X verifies the conditions (B) and (I) of the inductive definition of BT.

(B) $\emptyset \in BT_0 \subseteq X$.

(I) Let $l, r \in X$, $n, m \in \mathbb{N}$ exist such that $g \in BT_n$ and $d \in BT_m$. By symmetry, we can assume that $m \leq n$. Since $BT_m \subseteq BT_n$ we deduce $l, r \in BT_n$, and thus $\forall a \in A$, $(a, l, r) \in BT_{n+1} \subseteq X$.

Finally, we have proved $X = BT$.

3.13. We denote by $\leq$ the prefix ordering on A^*. We saw in Example 3.13 that $\forall x \in D$, $l(x) = r(x)$. We consider the property $P(x)$: '$\forall y \in A^*$, $y \leq x \Longrightarrow l(y) \geq r(y)$'. We show by induction that the elements of D verify P. Clearly, $P(\varepsilon)$ is true. Let $x \in D$ be such that $P(x)$ holds, and let y be a prefix of (x). We distinguish three cases :

- $y = \varepsilon$ or $y =$ (. We then have $l(y) \geq r(y)$.
- $y = (y'$ with y' prefix of x. We then have $l(y) = 1 + l(y') \geq 1 + r(y') > r(y') = r(y)$.
- $y = (x)$. We then have $l(y) = 1 + l(x) = 1 + r(x) = r(y)$.

We show similarly that if $x, y \in D$ verify P then $x \cdot y$ verifies P. We deduce that $D \subseteq L$.

Conversely, we show by induction on $|x|$ that $x \in L \Longrightarrow x \in D$. We thus consider the property $Q(n)$: '$\forall x \in A^*$ such that $|x| = n$, we have $x \in L \Longrightarrow x \in D$'. We use the second induction principle. Let $n \in \mathbb{N}$. We assume that $\forall k < n$, $Q(k)$ is true. Let $x \in L$ be such that $|x| = n$. If $n = 0$ then $x = \varepsilon \in D$. We thus assume $n > 0$. We denote by y the least non-empty prefix of x such that $l(y) = r(y)$; we thus have $y \in L$. We distinguish two cases :

- $|y| < |x|$. Let $z \in A^*$ be such that $x = y \cdot z$. We easily verify that $z \in L$. Moreover, because y is non-empty we also have that $|z| < |x| = n$. By the induction hypothesis we deduce $y, z \in D$. Using the inductive definition of D we obtain $x = y \cdot z \in D$.
- $|y| = |x|$. In this case, we show that $x = (z)$ with $z \in L$. Let x_1 and x_n be the first and last letters of x. We have $x_1 \leq x$ and thus $l(x_1) \geq r(x_1)$, which imply $x_1 =$ (. As $l(x) = r(x)$, we necessarily have that $n \geq 2$. Let $z \in A^*$ be such that $x = x_1 z x_n$. We have $x_1 z \leq x$ and thus $l(x_1 z) \geq r(x_1 z)$. As $l(x) = r(x)$, we deduce $x_n =$) and $l(x_1 z) = r(x_1 z) + 1$. Because $x_1 =$ (we also have that $l(z) = r(z)$. Finally, let z' be a prefix of z. $x_1 z'$ is a prefix of x, and hence $l(x_1 z) \geq r(x_1 z')$. Since $y = x$ we must have that $l(x_1 z') > r(x_1 z')$, and thus $l(z') = l(x_1 z') - 1 \geq r(x_1 z') = r(z')$. We have thus shown that $z' \in L$. Since $|z'| < n$, we deduce that $z' \in D$ and, consequently, $x = (z') \in D$.

Finally, we have shown $\forall n \in \mathbb{N}$, $P(n)$, which means that $L \subseteq D$.

3.14. 1. We proceed of course by induction. The desired property is

$$P(x)\text{: '}n(x) \leq 2^{h(x)} - 1\text{'}.$$

The unique element of the basis is the empty tree and we have $2^{n(\emptyset)} - 1 = 2^0 - 1 = 0 \geq 0 = n(\emptyset)$. Let $x = (a, l, r)$ and assume $P(l)$ and $P(r)$. We have

$$n(x) = 1 + n(l) + n(r) \leq 2^{h(l)} + 2^{h(r)} - 1 \leq 2 \times 2^{max(h(l),h(r))} - 1 = 2^{h(x)} - 1\,.$$

2. We proceed in the same way as for the property $Q(x)$: '$f(x) \leq 2^{h(x)-1}$'. Because of the definition of the function f, we must directly verify Q for the empty tree and for the tree reduced to a single element.

- $f(\emptyset) = 0 \leq 2^{-1} = 2^{h(\emptyset)-1}$,
- $f((a, \emptyset, \emptyset)) = 1 = 2^0 = 2^{h((a,\emptyset,\emptyset))-1}$.

We then verify the inductive step. Let $x = (a, l, r) \in BT$ with $g \neq \emptyset$ or $d \neq \emptyset$ and assume $Q(l)$ and $Q(r)$. $f(x) = f(l) + f(r) \leq 2^{h(l)-1} + 2^{h(r)-1} \leq 2 \times 2^{max(h(l),h(r))-1} = 2^{h(x)} - 1$.

3.15. 1. The inductive definition of the set SBT is

(B) $\forall a \in A, (a, \emptyset, \emptyset) \in SBT$,

(I) $l, r \in SBT \Longrightarrow \forall a \in A,\ (a, l, r) \in SBT$.

2. Let $P(x)$ be the property '$n(x) = 2f(x) - 1$'.

- $\forall a \in A$, if $x = (a, \emptyset, \emptyset)$ then $n(x) = 1 = 2 \times 1 - 1 = 2f(x) - 1$.
- Let $l, r \in SBT$ be such that $P(l)$ and $P(r)$ hold. Let $a \in A$ and $x = (a, l, r)$. We have $n(x) = 1 + n(l) + n(r) = 1 + 2f(l) - 1 + 2f(r) - 1 = 2(f(l) + f(r)) - 1 = 2f(x) - 1$. Hence $\forall x \in SBT$, $P(x)$ is true.

3.16. 1. The inductive definition of the set BBT is

(B) $\emptyset \in BBT$,

(I) if $l, r \in BBT$ verify $|h(l) - h(r)| \leq 1$ then $\forall a \in A, (a, l, r) \in BBT$.

2. We show by induction the property $P(x)$: '$n(x) \geq u_{h(x)}$'.

(B) $n(\emptyset) = 0 = u_0 = u_{h(\emptyset)}$.

(I) Let $l, r \in BBT$ be such that $|h(l) - h(r)| \leq 1$ and $P(l)$ and $P(r)$ hold. Let $a \in A$ and $x = (a, l, r) \in BBT$. We thus have $n(x) = 1 + n(l) + n(r) \geq 1 + u_{h(l)} + u_{h(r)}$.

- If $h(l) < h(r)$ then we have $h(x) = h(r) + 1$ and $h(l) = h(r) - 1 = h(x) - 2$. Thus $n(x) \geq 1 + u_{h(x)-2} + u_{h(x)-1} = u_{h(x)}$.
- Similar proof if $h(l) > h(r)$.
- If $h(l) = h(r)$ then $h(x) = h(l) + 1 = h(r) + 1$. Thus

$$n(x) \geq 1 + 2u_{h(x)-1} \geq 1 + u_{h(x)-1} + u_{h(x)-2} = u_{h(x)}$$

because the sequence $(u_n)_{n\in\mathbb{N}}$ is monotone increasing.

In all three cases we have thus verified $P(x)$. We deduce that $\forall x \in BBT$, $P(x)$.

3.17. 1. The proof is by induction. Denote by $P(L)$ the property '$\widetilde{L} \in Rat$'. We show that $\forall L \in Rat, P(L)$ is true.

(B) $\widetilde{\emptyset} = \emptyset \in Rat$ and $\forall a \in A, \widetilde{\{a\}} = \{a\} \in Rat$. Thus $P(L)$ is verified for any language L of the basis of the inductive definition of Rat.

(I$_1$) Let $L, M \in Rat$ be such that $P(L)$ and $P(M)$ hold. We have $\widetilde{L \cup M} = \widetilde{L} \cup \widetilde{M}$. By the hypothesis, $\widetilde{L}, \widetilde{M} \in Rat$, and applying (I_1) we obtain $\widetilde{L \cup M} \in Rat$.

(I$_2$) Let $L, M \in Rat$ be such that $P(L)$ and $P(M)$ hold. We easily verify that $\widetilde{L \cdot M} = \widetilde{M} \cdot \widetilde{L}$. Applying the hypothesis and (I$_2$) we obtain $\widetilde{L \cdot M} \in Rat$.

(I$_3$) Let $L \in Rat$ be such that $P(L)$ is true. We have $\widetilde{L^*} = \widetilde{L}^* \in Rat$ (hypothesis and (I$_3$)).

We thus have proved : $\forall L \in Rat, \widetilde{L} \in Rat$.

2. The proof is similar. Let $Q(L)$ be the property '$LF(L) \in Rat$'. We show that $\forall L \in Rat$, $Q(L)$ is true.

(B) $LF(\emptyset) = \emptyset \in Rat$ and $\forall a \in A$, $LF(\{a\}) = \{\varepsilon, a\} \in Rat$ since $\{\varepsilon\} = \emptyset^* \in Rat$ (I$_3$) and $\{\varepsilon, a\} = \{\varepsilon\} \cup \{a\} \in Rat$ (B and I$_1$).

(I) Let $L, M \in Rat$ be such that $Q(L)$ and $Q(M)$ hold. We have

- $LF(L \cup M) = LF(L) \cup LF(M) \in Rat$ (induction hypothesis and I$_1$),
- $LF(L \cdot M) = LF(L) \cup (L \cdot LF(M)) \in Rat$ (induction hypothesis, I$_1$ and I$_2$),
- $LF(L^*) = L^* \cdot LF(L) \in Rat$ (induction hypothesis, I$_2$ and I$_3$).

We have thus proved : $\forall L \in Rat$, $LF(L) \in Rat$.

3.18. The mirror image is a mapping from A^* to A^*. In order to define it inductively, we use the inductive definition of A^* given in Example 3.9. We obtain

$$\widetilde{u} = \begin{cases} \varepsilon & \text{if } u = \varepsilon, \\ a \cdot \widetilde{v} & \text{if } u = v \cdot a. \end{cases}$$

3.19. 1. $Q(\varepsilon)$ holds and $Q(x)$ holds implies that $Q(ax)$ holds.

2. $g((a_1), y) = (a_1 y)$.

3. We check by induction that

$$g\big((a_n(a_{n-1}(\ldots(a_1)\ldots))), y\big) = g\big(\varepsilon, (a_1(\ldots(a_{n-1}(a_n y))\ldots))\big).$$

This is clear for $n = 0$. Moreover, assuming it holds for n,

$$\begin{aligned} g\big((a_{n+1}(a_n(\ldots(a_2(a_1))\ldots))), y\big) &= g\big((a_n(\ldots(a_2(a_1))\ldots)), (a_{n+1}y)\big) \\ &= g\big(\varepsilon, (a_1(a_2(\ldots(a_n(a_{n+1}y))\ldots)))\big). \end{aligned}$$

4. Let $rev(x) = g(x, \varepsilon)$ with

$$\begin{aligned} g(\varepsilon, y) &= y \\ g((al), y) &= g(l, (ay)). \end{aligned}$$

Hence,

$$\begin{aligned} rev\big((a_1(a_2(\ldots(a_n)\ldots)))\big) &= g\big((a_1(a_2(\ldots(a_n)\ldots))), \varepsilon\big) \\ &= g\big(\varepsilon, (a_n(\ldots(a_2(a_1\varepsilon))\ldots))\big) = (a_n(\ldots(a_2(a_1))\ldots)). \end{aligned}$$

In Exercise 3.18, even though the strings of X were generated in the form $((\ldots(a_1(a_2))\ldots a_{n-1})a_n)$, where the parentheses are added for outlining the structure implicit in Example 3.9 part 2, A^* is endowed with an associative concatenation and the mirror is defined as a mapping from X into A^*. Here, the lists of L are generated in the form $(a_1(a_2(\ldots(a_n(a_{n+1}))\ldots)))$ by prefixing with letters of A, and, since rev is a mapping $L \longrightarrow L$, the only operations available in L are the prefixings by a letter of A. Thus rev must be defined in terms of these prefixings only, and hence the more complex definition.

3.20. $\mathbb{N} \times \mathbb{N}^*$ coincides with the subset X of $\mathbb{N} \times \mathbb{N}$ inductively defined by

(B) $\forall (n, m) \in \mathbb{N}^2, n < m \Longrightarrow (n, m) \in X$,
(I) $(n, m) \in X \Longrightarrow (n + m, m) \in X$.

This definition is induced by the inductive definition given for the modulo function. It is obviously not the most natural definition of $\mathbb{N} \times \mathbb{N}^*$.

3.21. The function gcd is defined by

$$\gcd(n, m) = \begin{cases} n & \text{if } m = 0, \\ m & \text{if } n = 0, \\ \gcd(n - m, m) & \text{if } 0 < m \le n, \\ \gcd(n, m - n) & \text{if } 0 < n < m. \end{cases}$$

The corresponding definition of X is
(B) $\forall n \in \mathbb{N} \setminus \{0\}$, $(0, n) \in X$ and $(n, 0) \in X$,
(I) $(n, m) \in X$ and $m \neq 0 \implies (n + m, m) \in X$,
$(n, m) \in X$ and $n \neq 0 \implies (n, m + n) \in X$.

3.22. We have

$$n(x) = \begin{cases} 0 & \text{if } x = \emptyset, \\ 1 + n(l) + n(r) & \text{if } x = (a, l, r). \end{cases}$$

$$l(x) = \begin{cases} 0 & \text{if } x = \emptyset, \\ 1 & \text{if } x = (a, \emptyset, \emptyset), \\ l(g) + l(d) & \text{if } x = (a, g, d) \text{ with } g \neq \emptyset \text{ or } d \neq \emptyset. \end{cases}$$

3.23. The inductive definition of the preorder traversal of a binary tree is

$$\mathrm{Pref}(x) = \begin{cases} \varepsilon & \text{if } x = \emptyset, \\ a \cdot \mathrm{Pref}(l) \cdot \mathrm{Pref}(r) & \text{if } x = (a, l, r). \end{cases}$$

3.24. By Proposition 3.27, it suffices to show that $C(k\mathbb{N}) \subseteq k\mathbb{N}$. If $n \in C(k\mathbb{N})$, p and q exist in $k\mathbb{N}$ such that $n = p + q$. But $p = kp'$ and $q = kq'$, and hence $n = k(p' + q') \in k\mathbb{N}$.

3.25. $\hat{C}(X)$ is the convex hull of X.

1. C is clearly monotone increasing ; it is finitary by definition, because $x \in C(X)$ implies that there exist $a, b \in X$ such that $x \in [a, b] = C(\{a, b\})$.

2. $\hat{C}(A \cup B)$ is C-closed and contains A, and hence $\hat{C}(A \cup B)$ contains $\hat{C}(A)$; symmetrically, $\hat{C}(A \cup B)$ contains $\hat{C}(B)$; and thus, again because of the closure property, $\hat{C}(A \cup B)$ contains $C(\hat{C}(A) \cup \hat{C}(B))$.

3. By 2, $\forall[a, b] \subseteq C(\bigcup_{F\in\text{fin}(X)} \hat{C}(F))$, $\exists F_1 \in \text{fin}(X)$, with

$$[a, b] \subseteq \hat{C}(F_1) \subseteq \bigcup_{F\in\text{fin}(X)} \hat{C}(F)$$

which is thus C-closed.

4. $\hat{C}$ is monotone increasing ; it is also finitary, since by (3) $\hat{C}(X) = \bigcup_{F\in\text{fin}(X)} \hat{C}(F)$ and because

- $\forall F \in \text{fin}(X)$, $\hat{C}(F) \subseteq \hat{C}(X)$ and
- $\bigcup_{F\in\text{fin}(X)} \hat{C}(F)$ is a C-closed set containing X.

5. Yes, because the proofs of 2 – 4 do not depend on the explicit definition of C.

3.26. $C'(\hat{C}(F_0)) = \big(C(\hat{C}(F_0)) \cup F_0\big) \subseteq \hat{C}(F_0)$ because $\hat{C}(F_0)$ is C-closed and contains F_0. Moreover, $\emptyset \subseteq \hat{C}(F_0)$ hence $\hat{C}'(\emptyset) \subseteq \hat{C}(F_0)$ by Proposition 3.27.

We verify that $F_0 \subseteq \hat{C}'(F_0)$ and $C(\hat{C}'(F_0)) \subseteq \hat{C}'(F_0)$ similarly, hence, by the same Proposition, 3.27, $\hat{C}(F_0) \subseteq \hat{C}'(\emptyset)$.

3.27. Since C is finitary, $\hat{E} = \cup_{n\in\mathbb{N}} E_n$, and we verify by induction on n that $E_n \subseteq T$, $\forall n \in \mathbb{N}$. We might also note that $C(T) \subseteq T$ (by the definition of T), and hence T is C-closed ; because T contains F_0, T also contains its closure $\hat{E}$.

Moreover, since T is the least set verifying conditions (B) and (I) of Definition 3.14, and $\hat{E}$ also verifies these conditions, $T \subseteq \hat{E}$.

3.28. Let $\mathcal{R}$ be a subset of $U \times V$. We define

$$\Gamma(R) = \bigcup_{i>0} \{(f(\sigma_1, \ldots, \sigma_i), h_f(v_1, \ldots, v_i)) \,/\, (\sigma_j, v_j) \in \mathcal{R}, f \in F_i\}.$$

Then Γ is finitary.

Let $R_0 = \{(f, h(f)) \,/\, f \in F_0\}$ and let $\hat{R} = \hat{\Gamma}(T_0)$. Let $P = \{\sigma /$ there exists a unique v: $(\sigma, v) \in \hat{R}\}$. Then $\hat{C}(F_0) \subseteq P$. By the universal induction principle it suffices to show that $F_0 \subseteq P$ and $C(P) \subseteq P$.

1. If $F \in F_0$, $(f, v) \in \hat{R} \Longrightarrow (f, v) \in R_0$. Let $R_{i+1} = R_i \bigcup \Gamma(R_i)$ and let i be the least integer such that $(f, v) \in R_i$. If $i = 0$ the proof is complete. Otherwise $(f, v) \in R_i$ and $(f, v) \notin R_{i-1}$, and hence $(f, v) \in \Gamma(R_{i-1})$. But if $(\sigma, v) \in \Gamma(R_{i-1})$, then $\sigma = f_n(\sigma_1, \ldots, \sigma_n)$ with $f_n \in F_n$ and $f \neq \sigma$, a contradiction.

2. If $f \in F_0$ then $(f, h(f)) \in R_0$, and if $(f, v) \in \hat{R}$ then $(f, v) \in R_0$; hence $v = h(f)$ and $F_0 \subseteq P$.

3. Let $e \in C(P)$. Then $e = f(e_1, \ldots, e_n)$ with $e_j \in P$ and hence there exists a unique v_j such that $(e_j, v_j) \in \hat{R}$; but then $(e, h_f(v_1, \ldots, v_n)) \in \Gamma(\hat{R}) \subseteq \hat{R}$. If $(e, v') \in \hat{R}$, we again consider the least i such that $(e, v') \in R_i$. Because $e \notin F_0, i > 0$ and $(e, v') \notin R_{i-1}$, and hence $(e, v') \in \Gamma(R_{i-1})(e, v') = (f'(e'_1, \ldots, e'_{n'}), h_f(v'_1, \ldots, v'_{n'}))$ with $(e'_j, v'_j) \in R_j$. We deduce that $f = f'$, $n = n'$, and $e_j = e'_j$; hence, since $e_j \in P$, we have that $v_j = v'_j$ and $v' = h_f(v_1, \ldots, v_n)$.

Then let $h^*(e)$ be equal to the unique v such that $(e, v) \in \hat{R}$, and it is easy to check that h^* verifies the required properties.

3.29. 1. We show by induction that $E_i = \{1, \dots, i\}$. $E_0 = \{1\}$, and if $E_i = \{1, \dots, i\}$ then $E_{i+1} = E_i \cup C(E_i) = E_i \cup \{2, \dots, i+1\} = \{1, \dots, i+1\}$.

2. Let E be its limit. We thus have, by Proposition 3.30, $E \subseteq \hat{C}(\{1\})$ and hence $C(E) \subseteq \hat{C}(\{1\})$. As E is infinite, $0 \in C(E)$, and hence $\mathbb{N} = \{0\} \cup E \subseteq \hat{C}(\{1\})$.

3. Since $E \subsetneq \hat{C}(\{1\})$, C is not finitary. Indeed, let X be infinite, then $0 \in C(X)$ and for any finite subset X' of X, $0 \notin C(X')$.

Chapter 4

4.1. Let us recall our hypotheses.

N_0 : $x \sqcup x = x$,
N_1 : $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$,
N_1' : $(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z)$,
N_{2a} :$x \sqcap \top = x$,
N_3 : $x \sqcup \bot = x = \bot \sqcup x$,
N_4 : $x \sqcap \overline{x} = \bot$ and $x \sqcup \overline{x} = \top$.

1. Let us first show that $\sqcap$ is idempotent. Using N_3, N_4, N_1 then again N_4, and N_2, we obtain

$$x \sqcap x = (x \sqcap x) \sqcup \bot = (x \sqcap x) \sqcup (x \sqcap \overline{x}) = x \sqcap (x \sqcup \overline{x}) = x \sqcap \top = x.$$

$\top \sqcap x = x$ also holds since, using N_4, N_1', N_0', N_4 and N_3,

$$\top \sqcap x = (x \sqcup \overline{x}) \sqcap x = (x \sqcap x) \sqcup (x \sqcap \overline{x}) = x \sqcup \bot = x.$$

Using N_{2a}, N_4, N_1, N_1', we obtain

$$\begin{aligned} \top \sqcup x &= (\top \sqcup x) \sqcap \top = (\top \sqcup x) \sqcap (x \sqcup \overline{x}) \\ &= ((\top \sqcup x) \sqcap x) \sqcup ((\top \sqcup x) \sqcap \overline{x}) = ((x \sqcup (x \sqcap x)) \sqcup (\overline{x} \sqcup (x \sqcap \overline{x})). \end{aligned}$$

Using N_0', N_0, N_4 and N_3, we obtain

$$((x \sqcup (x \sqcap x)) \sqcup (\overline{x} \sqcup (x \sqcap \overline{x})) = x \sqcup (\overline{x} \sqcup \bot) = x \sqcup \overline{x} = \top.$$

Similarly,

$$(x \sqcup \top) = (x \sqcup \top) \sqcap (x \sqcup \overline{x}) = x \sqcup \overline{x} = \top.$$

2. Let us assume that $y \sqcap x = \bot$ and $y \sqcup x = \top$. Using N_{2b}, N_4, N_1', N_4 and N_3, we obtain

$$\overline{x} = \top \sqcap \overline{x} = (y \sqcup x) \sqcap \overline{x} = (y \sqcap \overline{x}) \sqcup (x \sqcap \overline{x}) = y \sqcap \overline{x},$$

and, using N_{2a}, N_4, N_1 and N_3,

$$y = y \sqcap \top = y \sqcap (x \sqcup \overline{x}) = (y \sqcap x) \sqcup (y \sqcap \overline{x}) = \bot \sqcup (y \sqcap \overline{x}) = y \sqcap \overline{x}.$$

By N_4, it follows that $x = \overline{\overline{x}}$.
3. Using N_4, N_3, N_1, N_4 and N_3, we have

$$\bot = x \sqcap \overline{x} = x \sqcap (\overline{x} \sqcup \bot) = (x \sqcap \overline{x}) \sqcup (x \sqcap \bot) = \bot \sqcup (x \sqcap \bot) = x \sqcap \bot.$$

As $x = \overline{\overline{x}}$, we also have $\overline{x} \sqcap x = \perp$ and

$$\perp = \overline{x} \sqcap x = (\overline{x} \sqcup \perp) \sqcap x = (\overline{x} \sqcap x) \sqcup (\perp \sqcap x) = \perp \sqcup (\perp \sqcap x) = \perp \sqcap x.$$

4. These four equalities can be proved in similar ways, so we check only one of them :

$$x = x \sqcap \top = x \sqcap (\top \sqcup y) = (x \sqcap \top) \sqcup (x \sqcap y) = x \sqcup (x \sqcap y).$$

The associativity of $\sqcup$ then follows :

$$\begin{aligned}(x \sqcup y) \sqcup z &= ((x \sqcup y) \sqcup z) \sqcap (x \sqcup \overline{x}) = ((x \sqcup y) \sqcup z) \sqcap x) \sqcup ((x \sqcup y) \sqcup z) \sqcap \overline{x})\\ &= (((x \sqcup y) \sqcap x) \sqcup (z \sqcap x)) \sqcup (((x \sqcup y) \sqcap \overline{x}) \sqcup (z \sqcap \overline{x})) = x \sqcup ((y \sqcap \overline{x}) \sqcup (z \sqcap \overline{x})),\\ x \sqcup (y \sqcup z) &= (x \sqcup (y \sqcup z)) \sqcap (x \sqcup \overline{x}) = ((x \sqcup (y \sqcup z)) \sqcap x) \sqcup ((x \sqcup (y \sqcup z)) \sqcap \overline{x})\\ &= x \sqcup ((x \sqcap \overline{x}) \sqcup ((y \sqcup z) \sqcap \overline{x})) = x \sqcup ((y \sqcup z) \sqcap \overline{x}) = x \sqcup ((y \sqcap \overline{x}) \sqcup (z \sqcap \overline{x})).\end{aligned}$$

and also the commutativity :

$$(x \sqcup y) \sqcap (y \sqcup x) = ((x \sqcup y) \sqcap y) \sqcup ((x \sqcup y) \sqcap x) = y \sqcup x,$$

$$(x \sqcup y) \sqcap (y \sqcup x) = (x \sqcap (y \sqcup x)) \sqcup (y \sqcap (y \sqcup x)) = x \sqcup y.$$

Using N_1 and N_1', together with the associativity and commutativity of $\sqcup$, we obtain

$$(x \sqcup y) \sqcap (x \sqcup z) = x \sqcup (x \sqcap y) \sqcup (x \sqcap z) \sqcup (y \sqcap z)$$

and this is equal to $x \sqcup (y \sqcap z)$ by N_5.

5. In order to show that $\overline{x \sqcap y} = \overline{x} \sqcup \overline{y}$, it is enough to show that $(\overline{x} \sqcup \overline{y}) \sqcap (x \sqcap y) = \perp$ and $(\overline{x} \sqcup \overline{y}) \sqcup (x \sqcap y) = \top$. The following holds :

$$(\overline{x} \sqcup \overline{y}) \sqcap (x \sqcap y) = (\overline{x} \sqcap (x \sqcap y)) \sqcup (\overline{y} \sqcap (x \sqcap y)).$$

Since $x = x \sqcup (x \sqcap y)$, and $y = y \sqcup (x \sqcap y)$ we obtain

$$\perp = \overline{x} \sqcap x = \overline{x} \sqcap (x \sqcup (x \sqcap y)) = \overline{x} \sqcap (x \sqcap y),$$

$$\perp = \overline{y} \sqcap y = \overline{y} \sqcap (y \sqcup (x \sqcap y)) = \overline{y} \sqcap (x \sqcap y),$$

and therefore

$$(\overline{x} \sqcup \overline{y}) \sqcap (x \sqcap y) = \perp \sqcup \perp = \perp.$$

The following also holds : $\overline{y} = \top \sqcap \overline{y} = (x \sqcup \overline{x}) \sqcap \overline{y} = (x \sqcap \overline{y}) \sqcup (\overline{x} \sqcap \overline{y})$, and so

$$\overline{y} \sqcup (x \sqcap y) = (x \sqcap \overline{y}) \sqcup (\overline{x} \sqcap \overline{y}) \sqcup (x \sqcap y) = (x \sqcap (\overline{y} \sqcup y)) \sqcup (\overline{x} \sqcap \overline{y}) = x \sqcup (\overline{x} \sqcap \overline{y})$$

and therefore

$$\overline{x} \sqcup \overline{y} \sqcup (x \sqcap y) = \overline{x} \sqcup x \sqcup (\overline{x} \sqcap \overline{y}) = \top \sqcup (\overline{x} \sqcap \overline{y}) = \top.$$

We can easily deduce that $x \sqcup y = \overline{\overline{x}} \sqcup \overline{\overline{y}} = \overline{\overline{x} \sqcap \overline{y}}$ hence $\overline{x \sqcup y} = \overline{x} \sqcap \overline{y}$.

We thus obtain $y \sqcap x = \overline{\overline{y} \sqcup \overline{x}} = \overline{\overline{x} \sqcup \overline{y}} = x \sqcap y$ and

$$(x \sqcap y) \sqcap z = \overline{\overline{(x \sqcap y)} \sqcup \overline{z}} = \overline{\overline{x} \sqcup \overline{y} \sqcup \overline{z}} = \overline{\overline{x} \sqcup \overline{(y \sqcap z)}} = x \sqcap (y \sqcap z).$$

4.2. 1. Multiplying $x = ax + b\overline{x}$ by x, we obtain $xx = axx + b\overline{x}x$, i.e. $x = ax$, whence $x \leq a$. Multiplying by $\overline{x}$, we obtain $0 = b\overline{x}$, and since $b = b(x + \overline{x}) = bx + b\overline{x}$, $b = bx$ holds, therefore $b \leq x$ also holds.

Conversely, If $b \leq x \leq a$, we have $x = ax$ and $b = bx$, whence $b\overline{x} = bx\overline{x} = 0$, and therefore $ax + b\overline{x} = x + 0 = x$.

2. Multiplying $ax + b\overline{x} = 0$ by $\overline{x}$, we obtain $b\overline{x} = 0$ and we have just shown that this implies $b \leq x$. Multiplying by x, we obtain $ax = 0$, and this implies $x \leq \overline{a}$ for the same reasons.

Conversely, $b \leq x$ implies $b\overline{x} = 0$ and $x \leq \overline{a}$ implies $ax = 0$, whence $ax + b\overline{x} = 0$.

3.(i) Multiplying $x = au + b\overline{u}$ by $\overline{a}\overline{b}$, we obtain $\overline{a}\overline{b}x = \overline{a}\overline{b}au + \overline{a}\overline{b}b\overline{u} = 0$. As $x = au + b\overline{u}$, $\overline{x} = (\overline{a} + \overline{u})(\overline{b} + u) = \overline{a}\overline{b} + \overline{a}u + \overline{u}\overline{b}$, and multiplying by ab we obtain $ab\overline{x} = 0$. Therefore, $\overline{a}\overline{b}x + ab\overline{x} = 0$, and, applying the Schröder formula, $ab \leq x \leq \overline{\overline{a}\overline{b}} = a + b$. As $b \leq a$, $ab = b$ and $a + b = a$, the result follows.

3.(ii) Let us assume that $b \leq x \leq a$ and $\overline{b}x \leq u \leq \overline{a} + x$. Since $u = u(\overline{b}x + \overline{\overline{b}x}) = u(\overline{b}x + b + \overline{x})$ and $\overline{b}x \leq u$, we obtain $u = \overline{b}x + ub + u\overline{x}$. Since $u \leq \overline{a} + x$, $u = u(\overline{a} + x) = u\overline{a} + ux$ and $u\overline{x} = u\overline{a}\,\overline{x}$. Letting $y = u$ and $z = u\overline{x}$, $u = \overline{b}x + by + \overline{a}z$ holds. It follows that $\overline{u} = (b + \overline{x})(\overline{b} + \overline{y})(a + \overline{z})$ and therefore

$$\begin{aligned} au + b\overline{u} &= a(\overline{b}x + by + \overline{a}z) + b(b + \overline{x})(\overline{b} + \overline{y})(a + \overline{z}) \\ &= a\overline{b}x + aby + b\overline{y}(a + \overline{z})\,. \end{aligned}$$

Since $b \leq x \leq a$, we have in particular $b(a + \overline{z}) = b$, and we can simplify :

$$\begin{aligned} au + b\overline{u} &= a\overline{b}x + aby + b\overline{y}(a + \overline{z}) \\ &= \overline{b}x + by + b\overline{y} \\ &= \overline{b}x + b\,. \end{aligned}$$

Since $b \leq x$, we conclude $b = bx$ and $\overline{b}x + b = \overline{b}x + bx = x$.

4.3. By definition $x \leq y$ if and only if $x \sqcup y = y$, and $h(x) \leq' h(y)$ if and only if $h(x) \sqcup' h(y) = h(y)$. Now $h(x \sqcup y) = h(x) \sqcup' h(y)$.

Let E be a set. The mapping h from $\mathcal{P}(E)$ to itself defined by

$$h(X) = \begin{cases} \emptyset & \text{if } X = \emptyset, \\ E & \text{otherwise,} \end{cases}$$

is a monotone mapping for the inclusion ordering. It is not a homomorphism of Boolean algebras, because, if X is different from $\emptyset$ and E, then $h(X) = h(\overline{X}) = E$, which contradicts the equality $\emptyset = h(\emptyset) = h(X \cap \overline{X}) = h(X) \cap (\overline{X})$.

4.4. Let us first show that E' is a distributive lattice. To this end, it suffices to show that E' is closed under the sum and product operations, and that e is the maximal element of E'. We have

$$\begin{aligned} x = xe\,,\ y = ye \quad &\Longrightarrow \quad x + y = xe + ye = (x + y)e, \\ x = xe\,,\ y = ye \quad &\Longrightarrow \quad xy = xeye = xye, \\ x = xe \quad &\Longrightarrow \quad x \leq e. \end{aligned}$$

Let us next show that E' is complemented.

- $x\hat{x} = x\overline{x}e = 0e = 0$,
- $x + \hat{x} = xe + \overline{x}e = (x + \overline{x})e = 1e = e$.

Last, it is easy to check that h is a homomorphism by just writing down the definitions.

4.5. We first prove the lemma : if X is a subset of F, then

$$\sum_{Y \subseteq X} \left(\prod_{x \in Y} g(x) \prod_{x \in X \setminus Y} \overline{g(x)} \right) = \prod_{x \in X} (g(x) + \overline{g(x)}) = 1.$$

The proof is by induction on the cardinality of X. If X is empty, the least upper bound

$$\sum_{Y\subseteq X}\left(\prod_{x\in Y} g(x)\prod_{x\in X\setminus Y}\overline{g(x)}\right)$$

coincides with the least upper bound of the empty set which is equal to 1.

Let y be an element of F which is not in X. We have

$$\begin{aligned}\prod_{x\in X\cup\{y\}}(g(x)+\overline{g(x)}) &= (g(y)+\overline{g(y)})\prod_{x\in X}(g(x)+\overline{g(x)})\\ &= (g(y)+\overline{g(y)})\sum_{Y\subseteq X}\left(\prod_{x\in Y} g(x)\prod_{x\in X\setminus Y}\overline{g(x)}\right)\\ &= \sum_{Y\subseteq X}(g(y)\prod_{x\in Y} g(x)\prod_{x\in X\setminus Y}\overline{g(x)})+\sum_{Y\subseteq X}(\overline{g(y)}\prod_{x\in Y} g(x)\prod_{x\in X\setminus Y}\overline{g(x)})\\ &= \sum_{Y\subseteq X}\left(\prod_{x\in Y\cup\{y\}} g(x)\prod_{x\in X\setminus Y}\overline{g(x)}\right)+\sum_{Y\subseteq X}\left(\prod_{x\in Y} g(x)\prod_{x\in(X\cup\{y\})\setminus Y}\overline{g(x)}\right)\\ &= \sum_{Y\subseteq X\cup\{y\}}\left(\prod_{x\in Y} g(x)\prod_{x\in X\setminus Y}\overline{g(x)}\right).\end{aligned}$$

Let us now define the mapping h. Let $h(\emptyset)=0$ and, for $\mathcal{X}\in\mathcal{F}$, $\mathcal{X}\neq\emptyset$, let

$$h(\mathcal{X})=\sum_{X\in\mathcal{X}}\left(\prod_{x\in X} g(x)\prod_{x\notin X}\overline{g(x)}\right)$$

and this is an element of B.

By the lemma, we have $h(\mathcal{P}(F))=\sum_{Y\subseteq F}\left(\prod_{x\in Y} g(x)\prod_{x\in F\setminus Y}\overline{g(x)}\right)=1$.

We also have

$$\begin{aligned}h(i(y)) &= \sum_{X:y\in X}\left(\prod_{x\in X} g(x)\prod_{x\notin X}\overline{g(x)}\right)\\ &= g(y)\sum_{X\subseteq F\setminus\{y\}}\left(\prod_{x\in X} g(x)\prod_{x\in(F\setminus\{y\})\setminus X}\overline{g(x)}\right)\\ &= g(y)1=g(y).\end{aligned}$$

Let us show that h is a homomorphism.

It is clear, by definition, that $h(\emptyset)=0$ and we have just proved that $h(\mathcal{P}(F))=1$. It immediately follows, by the definition of h, that $h(\mathcal{X}\cup\mathcal{Y})=h(\mathcal{X})+h(\mathcal{Y})$

By the De Morgan laws, $h(\mathcal{X}\cap\mathcal{Y})=h(\mathcal{X})h(\mathcal{Y})$ will hold if $h(\overline{\mathcal{X}})=\overline{h(\mathcal{X})}$, and this must be shown anyway. In order to show that $h(\overline{\mathcal{X}})=\overline{h(\mathcal{X})}$, it suffices to show that $h(\overline{\mathcal{X}})+h(\mathcal{X})=1$ and $h(\overline{\mathcal{X}})h(\mathcal{X})=0$.

The first of these two equalities is a consequence of $h(\mathcal{X}\cup\mathcal{Y})=h(\mathcal{X})+h(\mathcal{Y})$.

Let us compute $h(\overline{\mathcal{X}})h(\mathcal{X})$. By definition of h this is equal to

$$\sum_{X_1\notin\mathcal{X}}\left(\prod_{x\in X_1} g(x)\prod_{x\notin X_1}\overline{g(x)}\right)\sum_{X_2\in\mathcal{X}}\left(\prod_{x\in X_2} g(x)\prod_{x\notin X_2}\overline{g(x)}\right)$$

and hence also equal to

$$\sum_{X_1\in\mathcal{X},X_2\notin\mathcal{X}}\left(\prod_{x\in X_1\cup X_2} g(x)\prod_{x\notin X_1\cap X_2}\overline{g(x)}\right).$$

If $X_1 \notin \mathcal{X}$ and if $X_2 \in \mathcal{X}$, then necessarily $X_1 \neq X_2$. Hence it is enough to show that in this case $\prod_{x\in X_1\cup X_2} g(x)\prod_{x\in\overline{X_1}\cup\overline{X_2}}\overline{g(x)} = 0$. Now, if $X_1 \neq X_2$, there exists an element y belonging to X_1 but not to X_2, or belonging to X_2 but not to X_1. In either case, $\prod_{x\in X_1\cup X_2} g(x)\prod_{x\in\overline{X_1}\cup\overline{X_2}}\overline{g(x)}$ can be written $g(y)\overline{g(y)}z$ and is therefore equal to 0.

4.6. The sixteen functions are given by the following table :

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Their polynomial form follows

$$\begin{array}{ccccc}
f_0 & = & \tilde{f}_0 & = & 0 \\
f_1 & = & \tilde{f}_7 & = & xy \\
f_2 & = & \tilde{f}_{11} & = & x\overline{y} \\
f_3 & = & \tilde{f}_3 & = & x \\
f_4 & = & \tilde{f}_{13} & = & \overline{x}y \\
f_5 & = & \tilde{f}_5 & = & y \\
f_6 & = & \tilde{f}_9 & = & \overline{x}y + x\overline{y} \\
f_7 & = & \tilde{f}_2 & = & x + y \\
f_8 & = & \tilde{f}_{14} & = & \overline{x}\,\overline{y} \\
f_9 & = & \tilde{f}_6 & = & xy + \overline{x}\,\overline{y} \\
f_{10} & = & \tilde{f}_{10} & = & \overline{y} \\
f_{11} & = & \tilde{f}_2 & = & x + \overline{y} \\
f_{12} & = & \tilde{f}_{12} & = & \overline{x} \\
f_{13} & = & \tilde{f}_4 & = & \overline{x} + y \\
f_{14} & = & \tilde{f}_8 & = & \overline{x} + \overline{y} \\
f_{15} & = & \tilde{f}_{15} & = & 1
\end{array}$$

Chapter 5

5.1. We note that $p \Longrightarrow q$ is equivalent to $\neg q \Longrightarrow \neg p$. Thus, $[\neg q$ and $(\neg q \Longrightarrow \neg p)] \Longrightarrow \neg p$ is equivalent to the *modus tollens* rule. On the other hand, substituting $\neg q$ for p and $\neg p$ for q in the *modus ponens* rule, we have $[\neg q$ and $(\neg q \Longrightarrow \neg p)] \Longrightarrow \neg p$, which can thus be deduced from the *modus ponens* rule.

The converse can be proved similarly. We notice that $p \Longrightarrow q$ is equivalent to $\neg p$ or q, i.e. $(\neg p \vee q)$; then the *modus ponens* rule that is written $[p \wedge (p \Longrightarrow q)] \Longrightarrow q$ is equivalent to $p \Longrightarrow [(p \Longrightarrow q) \Longrightarrow q]$, and also to $p \Longrightarrow [\neg(p \Longrightarrow q) \vee q]$, whose contrapositive $[(p \Longrightarrow q) \wedge \neg q] \Longrightarrow \neg p$ is the *modus tollens* rule.

5.2. 1. $p \Longrightarrow q$ and its contrapositive implication $\neg q \Longrightarrow \neg p$ are both true. The converse $q \Longrightarrow p$, and its contrapositive $\neg p \Longrightarrow \neg q$, are usually false.

2. $p \Longrightarrow q$ is clearly false ; its converse is, however, true. This example also shows that the quantifiers $\forall$ and $\exists$ may not be permuted (see also Exercise 5.14).

5.3. 1. The identities given above are immediately deduced from the truth table given below :

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \supset q$	$p \supset \neg q$	$\neg p \supset q$	$\neg(p \supset \neg q)$
1	1	0	1	1	1	0	1	1
1	0	0	0	1	0	1	1	0
0	1	1	0	1	1	1	1	0
0	0	1	0	0	1	1	0	0

2. By induction on n.

In order to prove the last identity, first show that

$$\begin{aligned}\overline{I(F_n \wedge (F_{n-1} \wedge (\cdots \wedge (F_2 \wedge F_1))\cdots))} &= \overline{I(F_n)I(F_{n-1})\cdots I(F_2)I(F_1)}\\ &= \overline{I(F_n)} + \overline{I(F_{n-1})} + \cdots + \overline{I(F_1)}\end{aligned}$$

(See Proposition 4.3.)

5.4. If F is unsatisfiable, then $\forall I$, $I(F) = 0$, and thus $\forall I$, $I(\neg F) = \overline{I(F)} = 1$, hence $\neg F$ is valid. The converse can be proved similarly.

5.5. 1. The sequent $(\emptyset, G)$ is true in I if and only if

$$(\forall F \in \emptyset, I(F) = 1) \implies I(G) = 1. \qquad (I)$$

But assertion $\forall F \in \emptyset$, $I(F) = 1$ is trivially true, because it can be rewritten as : $\forall F$, $[F \in \emptyset \Longrightarrow I(F) = 1]$; $F \in \emptyset$ is always false because the set $\emptyset$ is always empty, but then, since 'false implies anything', the implication $F \in \emptyset \Longrightarrow I(F) = 1$, which can be also written as $0 \Longrightarrow I(F) = 1$, is always true, and thus $\big(\forall F \in \emptyset,\ I(F) = 1\big) = 1$. The implication (I) is thus reduced to $1 \Longrightarrow I(G) = 1$, which is true if and only if $I(G) = 1$, i.e. if and only if G is true in I. Validity can be similarly verified.

Z Such arguments about the empty set and the satisfaction of implications $0 \Longrightarrow G$ or $1 \Longrightarrow G$ are tricky, but alas often useful, and should be handled with care in order to avoid errors.

2. Sequent $(\emptyset, (p \supset q))$ is true in I if and only if $p \supset q$ is true in I, i.e. if and only if $I(p) = 0$ or $I(q) = 1$.

Sequent $(\{p, (p \supset q)\}, q)$ is valid because $I(p) = 1$ and $I(p \supset q) = \overline{I(p)} + I(q) = 1$ implies that $I(q) = 1$.

5.6. We assume $S = (\mathcal{F}, G) = (\{F_n, \ldots, F_1\}, F)$; then $\phi(S) = F_n \supset (F_{n-1} \supset (\cdots (F_1 \supset F)\cdots))$ and the result is shown exactly as in Proposition 5.9.

5.7. $\Longleftrightarrow$ is a congruence. It suffices to verify

$$\forall * \in \{\wedge, \vee, \supset\}, \quad \text{if } F_1 \Longleftrightarrow F_1' \text{ and } F_2 \Longleftrightarrow F_2', \text{ then}$$

$$(F_1 * F_2) \Longleftrightarrow (F_1' * F_2') \qquad \text{and}$$

$$\neg F_1 \Longleftrightarrow \neg F_1'.$$

For instance : $F_1 \Longleftrightarrow F_1'$ and $F_2 \Longleftrightarrow F_2'$ imply that : $I(F_1) = I(F_1')$ and $I(F_2) = I(F_2')$, hence, for instance for $* = \vee$, $I\big((F_1 * F_2)\big) = I(F_1) + I(F_2) = I(F_1') + I(F_2') = I\big((F_1' * F_2')\big)$. The other cases can be verified similarly, and follow from the fact that I is a homomorphism from the set of formulas, equipped with the binary operations $\wedge, \vee, \supset$ and the unary operation $\neg$, to the Boolean algebra $\mathbb{B}$, equipped with the operations $\cdot, +, \circ$ and $^{-}$, where $\circ$ is defined by $x \circ y = \overline{x} + y$.

5.8. He mixed $p \supset q$ and $\neg p \supset \neg q$ (that is, the contrapositive of the converse $q \supset p$ of $p \supset q$).

5.9. Let $A =$ 'I love Anne', $M =$ 'I love Mary', and $P = M \supset A =$ 'If I love Mary, then I love Anne'. In 1 we have $(M \vee A) \wedge (M \supset A) = (M \vee A) \wedge (\neg M \vee A) = A$. We can thus conclude with certainty that he loves Anne, but his feelings for Mary no longer fall within the scope of logic. (He may love or may not love Mary ; neither of these two assertions follows from (a) and (b).)

On the other hand, in 2, we know that our logician certainly loves Anne **and** Mary. Indeed, both assertions (a) and (b) hold : (a) : $P \supset M$, and (b) : $M \supset P$. Assume that P is false. Then, because 'false implies anything', it follows from (a) that M is true. But then P is also true by (b), and thus also A ; if P is true, then it also follows from (a) that M is true, and thus also A because P is true. Our logician is thus, with high probability, bigamous (unless his fiancée is called Mary–Anne).

5.10. There are neither free variables nor free occurrences in the first formula ; in the second formula, variable x is free : the first occurrence of x is bound and the second is free.

5.11. (i) $\forall x\,(P(x) \supset Q(x))$.

(ii) $\exists x\,(P(x) \wedge Q(x))$. This is not to be confused with $\exists x\,(P(x) \supset Q(x))$, which *is not* the translation of (ii), but which means 'some individuals either are not Ps or else are Qs'.

(iii) $\forall x\,(P(x) \supset \neg Q(x))$, or also, $\neg\exists x\,(P(x) \wedge Q(x))$.

(iv) $\exists x\,(P(x) \wedge \neg Q(x))$.

5.12. If x is not free in F, then for any valuation v' such that $v' \underset{X-\{x\}}{=} v$, we have, by Proposition 5.32, $\bar{v}(F) = \bar{v}'(F)$. Thus :

$$\begin{aligned} \bar{v}(\forall x F) = 1 \quad &\Longleftrightarrow \quad \text{for all } v' \underset{X-\{x\}}{=} v : \bar{v}'(F) = 1 \quad \Longleftrightarrow \quad \bar{v}(F) = 1 \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \text{there is } v' \underset{X-\{x\}}{=} v \text{ such that } \bar{v}'(F) = 1 \quad \Longleftrightarrow \quad \bar{v}(\exists x F) = 1 \end{aligned}$$

5.13. We have, allowing for some notational flexibility in formulas and writing xRy instead of $R(x,y)$,

$$\begin{aligned} F = \big(\forall x\, xRx\big) \wedge \ &\big(\forall x\, \forall y\ (xRy \wedge yRx \ \supset \ x = y)\big) \\ \wedge \ &\big(\forall x\, \forall y\, \forall z\ (xRy \wedge yRz \ \supset \ xRz)\big). \end{aligned}$$

We add the formula $\forall x\, \forall y\ (xRy \vee yRx)$ in order to obtain a total ordering.

5.14. 1. Clearly, for any r, $\exists y \forall x\, r(x,y) \supset \forall x \exists y\, r(x,y)$ is true, but the converse implication is false ; for instance in $\mathbb{N}$, $\forall x \exists y\ x < y$, but $\neg\exists y \forall x\ x < y$. Similarly, $\exists y(p(y) \wedge q(y)) \supset (\exists y p(y)) \wedge (\exists y q(y))$, but the converse is false ; for instance in $\mathbb{N}^*$, $(\exists y\, \mathrm{even}(y)) \wedge (\exists y\, \mathrm{odd}(y))$ is true, but $\exists y\,(\mathrm{even}(y) \wedge \mathrm{odd}(y))$ is false.

2. By the preceding question, it thus suffices to verify the converse implication when $r(x,y) = p(x) \wedge q(y)$. This implication follows from the fact that, as $q(y)$ does not depend on x, we can choose the same y for all xs verifying $\forall x \exists y\, r(x,y)$. The formal proof is given below.

We assume that $\bar{v}(\forall x \exists y [p(x) \wedge q(y)]) = 1$. Then, $\forall v' \underset{X-\{x\}}{=} v$, there exists v'' such that $v'' \underset{X-\{y\}}{=} v'$: $\bar{v}''(p(x)) = 1$ and $\bar{v}''(q(y)) = 1$. Note that $\bar{v}''(q(y))$ depends only on $y_0 = v''(y)$; we thus have $\bar{v}''(q(y)) = q_S(y_0) = 1$ and $\bar{v}''(p(x)) = \bar{v}'(p(x)) = 1$, and thus $\forall v' \underset{X-\{x\}}{=} v$, $\bar{v}'(p(x)) = 1$. Hence, finally, $\forall v' \underset{X-\{x\}}{=} v$: $\bar{v}'(p(x)) = 1$ and $q_S(y_0) = 1$. Because $\bar{v}'(p(x))$ depends only on $v'(x)$, we can transform this assertion into $\forall v' \underset{X-\{x\}}{=} v''$: $\bar{v}'(p(x)) = 1$ and $\bar{v}''(q(y)) = 1$, which shows that $\exists w = v'' \underset{X-\{y\}}{=} v$, $\forall v' \underset{X-\{x\}}{=} v''$: $\bar{v}'(p(x)) = 1$ and $\bar{v}'(q(y))$= $\bar{v}''(q(y)) = 1$. Hence the required result, $\bar{v}\big(\exists y \forall x\, [p(x) \wedge q(y)]\big) = 1$.

See Proposition 5.43 for a generalization of this result, i.e. if x is not free in G and y is not free in F, then :

$$(\forall x\, F) \wedge (\exists y\, G) \approx \forall x \exists y\, (F \wedge G) \approx \exists y \forall x\, (F \wedge G)$$

5.15. We obtain one of the equivalent prenex forms :

$$\exists x \forall x' \forall y \Big(P(x) \wedge \big(Q(y) \supset R(x')\big)\Big)$$
$$\forall x \forall y \exists x' \Big(P(x') \wedge \big(Q(y) \supset R(x)\big)\Big)$$
$$\forall x \exists x' \forall y \Big(P(x') \wedge \big(Q(y) \supset R(x)\big)\Big)$$

5.16. We prove that there is no programmer. Let us define the following predicates :

$$\begin{cases} p(x) & \text{means `$x$ is a programmer'} \\ e(x,y) & \text{means `x writes programs for y'} \end{cases}$$

Then :

- Rule (a) becomes

$$\forall x \, \big(p(x) \supset \forall y \, (\neg e(y,y) \supset e(x,y))\big)$$

and also

$$\forall x \, \big(\neg p(x) \vee \forall y \, (e(y,y) \vee e(x,y))\big) \ ,$$

and by Proposition 5.43

$$\forall x \, \forall y \, \big(\neg p(x) \vee e(y,y) \vee e(x,y)\big) \ . \qquad (F)$$

- Rule (b) becomes

$$\neg\Big(\exists x \, \exists y \, \big(p(x) \wedge e(y,y) \wedge e(x,y)\big)\Big)$$

and also

$$\forall x \, \forall y \, \big(\neg p(x) \vee \neg e(y,y) \vee \neg e(x,y)\big) \ . \qquad (G)$$

By Proposition 5.42 (i), $F \wedge G$ can be written

$$\forall x \, \forall y \, \Big(\big(\neg p(x) \vee e(y,y) \vee e(x,y)\big) \bigwedge \big(\neg p(x) \vee \neg e(y,y) \vee \neg e(x,y)\big)\Big)$$

and, by distributivity,

$$\forall x \, \forall y \, \Big(\neg p(x) \bigvee \big(e(y,y) \vee e(x,y)\big) \bigwedge \big(\neg e(y,y) \vee \neg e(x,y)\big)\Big) \ .$$

Let S be a $\{p,e\}$-structure in which this formula is valid, i.e. $\emptyset \underset{S}{\models} F \wedge G$. This implies that for any element a of S, the valuation v_a such that $v_a(x) = v_a(y) = a$ verifies

$$\bar{v}_a\Big(\neg p(x) \bigvee \big(e(y,y) \vee e(x,y)\big) \bigwedge \big(\neg e(y,y) \vee \neg e(x,y)\big)\Big) = 1$$

i.e.

$$\overline{p_S(a)} \bigvee \big(e_S(a,a) \vee e_S(a,a)\big) \bigwedge \big(\neg e_S(a,a) \vee \neg e_S(a,a)\big) = 1$$

and thus $p_S(a) = 0$, meaning that there is no programmer.

More formally, we have proved that for any structure S, if $F \wedge G$ is valid in S, then $\forall x \, \neg p(x)$ is also valid in S, i.e. $F \wedge G \models \forall x \, \neg p(x)$.

As there is no programmer, it is then normal to obtain contradictory conclusions if we assume that x is a programmer, because in that case the hypothesis $p(x)$ is false, and we can deduce anything from false (see Exercise 5.5).

5.17. As in Theorem 5.17, it suffices to verify by induction on the length of proofs that each use of a proof rule generates only valid sequents from valid sequents. We verified in Theorem 5.17 that each proof rule of propositional logic given in Definition 5.11 is valid ; it thus suffices to verify that the three rules given in Definition 5.49 are valid.

For instance, validity of the instantiation rule immediately follows from Proposition 5.41, and validity of the generalization rule immediately follows from Proposition 5.38.

5.18. 1. We introduce the predicates

$R(x,y)$, for denoting 'x likes y',

$A(x)$, for 'x is an alpinist',

$S(x)$, for 'x is a skier',

and the constants

s for 'snow', r for 'rain', b for 'Bernard', and c for 'Christopher'.

The hypotheses of the exercise can be written :

$$\begin{aligned} F_1 &= \forall x(A(x) \supset \neg R(x,r)) \\ F_2 &= \forall x(S(x) \supset R(x,s)) \\ F_3 &= \forall x(A(x) \vee S(x)) \\ F_4 &= \forall y(R(b,y) \vee R(c,y)) \\ F_5 &= \exists y(R(b,y) \wedge \neg R(c,y)). \end{aligned}$$

Let $\mathcal{F} = \{F_1, F_2, F_3, F_4, F_5\}$ be the five formulas given above ; $\mathcal{F}$ expresses the requirements of the Alpine Club.

2. We want to determine the models of the five formulas of $\mathcal{F}$.

We first show that it is not possible for Bernard to be an alpinist. Assume that there exists a model H such that

$$\emptyset \underset{H}{\models} A(b).$$

Applying instantiation and *modus ponens* to F_1, we have

$$\emptyset \underset{H}{\models} \neg R(b,r).$$

Applying instantiation and *modus ponens* to F_4, we have

(i) $\emptyset \underset{H}{\models} R(c,r)$, hence $\emptyset \underset{H}{\not\models} R(b,r) \wedge \neg R(c,r)$.

By F_5, we must thus have

(ii) $\emptyset \underset{H}{\models} R(b,s) \wedge \neg R(c,s)$.

If $\emptyset \underset{H}{\models} A(c)$, then, by F_1, $\emptyset \underset{H}{\models} \neg R(c,r)$, which contradicts (i), and if $\emptyset \underset{H}{\models} S(c)$, then, by F_2, $\emptyset \underset{H}{\models} R(c,s)$, which contradicts (ii). We thus necessarily have $\emptyset \underset{H}{\models} \neg A(c) \wedge \neg S(c)$, which contradicts F_3.

We thus cannot have $\emptyset \underset{H}{\models} A(b)$, and because of F_3, we have

$$\emptyset \underset{H}{\models} S(b).$$

By F_2, this implies

(iii) $\emptyset \underset{H}{\models} R(b,s)$.

And hence, because false implies anything, $\emptyset \underset{H}{\models} \neg R(b,s) \supset R(c,s)$. In order for H to be a model of F_4, we must also have

$$\emptyset \underset{H}{\models} \neg R(b,r) \supset R(c,r).$$

On the other hand, in order for F_5 to be satisfied in H, we must have

$$\emptyset \underset{H}{\models} \big(R(b,r) \wedge \neg R(c,r)\big) \vee \big(R(b,s) \wedge \neg R(c,s)\big),$$

which, in view of (iii), can be written

$$\emptyset \underset{H}{\models} \big(R(b,r) \wedge \neg R(c,r)\big) \vee \neg R(c,s).$$

If we then let $\emptyset \underset{H}{\models} R(b,r)$, $\emptyset \underset{H}{\models} \neg R(c,r)$ and $\emptyset \underset{H}{\models} R(c,s)$, we see that all formulas are satisfied, and Christopher may be an alpinist, a skier or even both. Thus let $E = \{b, c\}$.

- Let H be defined by : $S(b)$, $S(c)$, $\neg A(b)$, $\neg A(c)$, $R(b,r)$, $\neg R(c,r)$, $R(b,s)$ and $R(c,s)$ are true in H ; H is a model of $\mathcal{F}$.
- Let H_1 be defined by : $S(b)$, $S(c)$, $\neg A(b)$, $A(c)$, $R(b,r)$, $\neg R(c,r)$, $R(b,s)$ and $R(c,s)$ are true in H_1 ; H_1 is also a model of $\mathcal{F}$.
- Let H_2 be defined by : $S(b)$, $\neg S(c)$, $\neg A(b)$, $A(c)$, $R(b,r)$, $\neg R(c,r)$, $R(b,s)$ and $R(c,s)$ are true in H_2 ; H_2 is also a model of $\mathcal{F}$.
- Let H_3 be defined by : $S(b)$, $\neg S(c)$, $\neg A(b)$, $A(c)$, $R(b,r)$, $\neg R(c,r)$, $R(b,s)$ and $\neg R(c,s)$ are true in H_3 ; H_3 is also a model of $\mathcal{F}$.

In fact H, H_1, H_2, H_3 are Herbrand models of $\mathcal{F}$. (See Section 5.4.2.)

3. Let F be the formula $\exists x\Big(\big(A(x) \wedge \neg S(x)\big) \vee \big(\neg A(x) \wedge S(x)\big)\Big)$. We want to prove that $\mathcal{F} \vdash F$. We reason by contradiction and assume that $\mathcal{F} \cup \{\neg F\}$ is satisfiable ; let H be a model of $\mathcal{F} \cup \{\neg F\}$. Note first that

$$\begin{aligned}\neg F &= \forall x\big((\neg A(x) \vee S(x)) \ \wedge\ (A(x) \vee \neg S(x))\big)\\ &\Longleftrightarrow \forall x\Big(\big(\neg A(x) \wedge (A(x) \vee \neg S(x))\big) \ \vee\ \big(S(x) \wedge (A(x) \vee \neg S(x))\big)\Big)\\ &\Longleftrightarrow \forall x\big((\neg A(x) \wedge \neg S(x)) \ \vee\ (A(x) \wedge S(x))\big)\end{aligned}$$

Let $F' = \forall x\big((\neg A(x) \wedge \neg S(x)) \ \vee\ (A(x) \wedge S(x))\big)$. Because H is a model of $\neg F$, H is a model of F'. Applying instantiation and *modus ponens* to F' and F_3, we have

$\emptyset \underset{H}{\models} A(b) \wedge S(b)$, and $\emptyset \underset{H}{\models} A(c) \wedge S(c)$; and hence,

$\emptyset \underset{H}{\models} A(b)$ and $\emptyset \underset{H}{\models} A(c)$.

Because H is a model of F_1, this implies

$\emptyset \underset{H}{\models} \neg R(b,r)$ and $\emptyset \underset{H}{\models} \neg R(c,r)$.

But H is also a model of F_4, namely, $\forall y(R(b,y) \vee R(c,y))$: a contradiction.

Note that, in fact, we have proved the stronger result that $\{F_1, F_3, F_4\} \vdash F$, because formulas F_2 and F_5 have not been used in the proof.

5.19. $I_0 = \{edge(a,b)\,, edge(b,c)\,, path(a,b)\,, path(b,c)\,, path(a,c)\}$, and also, for any $K \subset \{a,b,c\}^2$,

$$\begin{aligned}I_K &= I_0 \cup \{path(l,l')\,/\,(l,l') \in K\}\\ J_K &= I_0 \cup \{edge(l,l')\,/\,(l,l') \in K\} \cup \{path(l,l')\,/\,(l,l') \in K\}\\ &\quad \cup \{path(l,l')\,/\,(l,l_1) \in K \text{ and } (l_1,l') \in K\}\\ &\quad \cup \{path(l,l')\,/\,(l,l_1) \in K \text{ and } (l_1,l_2) \in K \text{ and } (l_2,l') \in K\}\end{aligned}$$

In other words, on a graph having exactly three vertices a, b and c, Herbrand models of $\mathcal{F}$ yield any relation *path* such that

(i) *path* is a transitive relation (because of formula r_4) ;

(ii) *path* contains the relation *edge* (because of formula r_3) ;

(iii) the relation *edge* contains at least one edge from a to b and one edge from b to c (because of formulas r_1 and r_2).

(i) and (ii) mean that *path* is the transitive closure of *edge*.

5.20. Let $\mathcal{L}' = \mathcal{L} \cup \{f\}$ and let S' be an $\mathcal{L}'$-structure satisfying F' ; the $\mathcal{L}$-structure S that is deduced from S' by omitting the function f_S interpreting f is a model of F, i.e. $\emptyset \underset{S}{\models} F$. Conversely, let S be an $\mathcal{L}$-structure modelling F ; because $\emptyset \underset{S}{\models} F$, for every $a_1, \ldots, a_n$ in the domain E of S, there exists an a in E such that $\emptyset \underset{S}{\models} G[x_1 := a_1] \ldots [x_n := a_n][y := a]$. Defining $f_{S'}(a_1, \ldots, a_n) = a$ yields an expansion S' of S such that $\emptyset \underset{S'}{\models} F'$.

5.21. The possible prenex forms of F are

$$F_1 = \forall u \exists v [R(u) \vee R'(v)] \quad \text{and} \quad F_2 = \exists v \forall u [R(u) \vee R'(v)].$$

Note that F, F_1 and F_2 are equivalent. The corresponding Skolemizations are

$$F_1' = \forall u [R(u) \vee R'(f(u))] \quad \text{and} \quad F_2' = \forall u [R(u) \vee R'(a)].$$

Note that F_1 and F_1' are not equivalent, nor are F_2 and F_2'.

5.22. A possible prenex form of F is $\forall u \exists v \forall w \exists z [R(u,v) \vee \neg R'(w,z)]$, yielding the Skolemization $\forall u \forall w [R(u, f_1(u)) \vee \neg R'(w, f_2(u,w))]$.

Another possible prenex form of F is $\forall u \forall w \exists v \exists z [R(u,v) \vee \neg R'(w,z)]$, yielding the Skolemization $\forall u \forall w [R(u, f_1(u,w)) \vee \neg R'(w, f_2(u,w))]$.

5.23. H defined by $\{S(b),\ S(c),\ R(b,r),\ R(b,s),\ R(c,s)\}$ and H_3 defined by $\{S(b),\ A(c),\ R(b,r),\ R(b,s)\}$ (see Exercise 5.18, 2) are the minimal Herbrand models for the Alpine Club. H and H_3 are incomparable, and their intersection $I = \{S(b),\ R(b,r),\ R(b,s)\}$ is not a model of $\mathcal{F}$.

5.24. The least Herbrand model of P is defined by $I_M = \emptyset$, i.e. the *path* relation is the empty relation.

5.25. Here the Herbrand universe is $U_H = \{s^n(a) \,/\, n \in \mathbb{N}\}$; the least Herbrand model M of the program P is defined by the whole Herbrand basis, i.e. $I_M = B_H = \{i(s^n(a)) \,/\, n \in \mathbb{N}\}$. M can be seen as modelling the set of integers with a successor funtion.

5.26. Let $M = \langle U_H, I_M \rangle$ be the least Herbrand model of P.

1. If $A \in Th(P) \cap B_H$, then $A \in I_M$ because A must be true in any model of P.

2. Conversely, if $A \in I_M$, then A must be true in all Herbrand models of P, and as a result, because A is a universal formula, A must be true in all models of P, thus $A \in Th(P)$.

5.27. Any set $\mathcal{F}$ of Horn clauses which is satisfiable has a least Herbrand model. Let $P \subset \mathcal{F}$ be the set of program clauses in $\mathcal{F}$; P has a least Herbrand model M defined by $I_M = B_H \cap Th(P)$ (see Exercise 5.26). We can prove that M is also the least Herbrand model of $\mathcal{F}$: let $C = \forall x_1 \cdots \forall x_p (\neg A_1 \vee \cdots \vee \neg A_n)$ be a negative clause in $\mathcal{F}$, because $P \cup \{C\}$ is satisfiable, $Th(P \cup \{C\})$ is not contradictory, and hence, by Theorem 5.57, $P \cup \{C\}$ has a model ; by Theorem 5.64 $P \cup \{C\}$ has a Herbrand model $H = \langle U_H, I_H \rangle$. Because $C = \forall x_1 \cdots \forall x_p (\neg A_1 \vee \cdots \vee \neg A_n)$, and $\emptyset \underset{H}{\models} C$, for any valuation $v \colon \{x_1, \ldots, x_p\} \longrightarrow U_H$, $\bar{v}(C) = 1$, hence for any valuation there is an i such that $\bar{v}(\neg A_i) = 1$, which means that the ground instance $A_i[x_1 := v(x_1)] \cdots [x_p := v(x_p)]$ of A_i is not in I_H. Because $I_M = \cap \; \{I_H \;\; / \;\; \emptyset \underset{H}{\models} P\}$, and $\emptyset \underset{H}{\models} P$, $A_i[x_1 := v(x_1)] \cdots [x_p := v(x_p)]$ is not in I_M either ; whence : for any valuation $v \colon \{x_1, \ldots, x_p\} \longrightarrow U_H$, there is an i such that $A_i[x_1 := v(x_1)] \cdots [x_p := v(x_p)] \notin I_M$, and thus $\emptyset \underset{M}{\models} C$. C is true in the least Herbrand model M of P.

5.28. 1. Straightforward.

2. I is a model of P if and only if for any valuation s, and any rule r of P, $\emptyset \underset{I}{\models} s^*(r)$, where $s^*(r)$ is obtained by substituting $s(x)$ for x in r, for any variable x. In other words, I is a model of P if and only if for any ground instance $A_1, \dots, A_n \Longrightarrow A$ of a clause r of P, $\emptyset \underset{I}{\models} [A_1, \dots, A_n \Longrightarrow A]$, i.e. if and only if for any ground instance $A_1, \dots, A_n \Longrightarrow A$ of a clause r of P, $\emptyset \underset{I}{\models} A_1, \dots, \emptyset \underset{I}{\models} A_n$ imply $\emptyset \underset{I}{\models} A$, that is if and only if $T_P(I) \subset I$.

3. Immediate by the two preceding questions, and the fact that the least fixed point of T_P is defined by $\inf\{I \in \mathcal{P}(B_H) \,/\, T_P(I) \subset I\}$.

4. Let $\{K_i\}_{i \in N}$ be any increasing sequence of subsets of $\mathcal{P}(B_H)$. Because T_P is monotone : $\sup_i T_P(K_i) \subset T_P(\sup_i K_i)$.

Let us prove the reverse inclusion : $\sup_i T_P(K_i) \supset T_P(\sup_i K_i)$; let $A \in T_P(\sup_i K_i)$, then there is a ground instance $(A_1, \dots, A_n \Longrightarrow A)$ of a clause r of P, with $A_1 \in \sup_i K_i, \dots, A_n \in \sup_i K_i$. We assume that $A_1 \in K_{i_1}, \dots, A_n \in K_{i_n}$; because K_i is an increasing sequence, if we let $l = \sup\{i_1, \dots, i_n\}$, we have $K_{i_1} \subset K_l, \dots, K_{i_n} \subset K_l$ and hence $A_1 \in K_l, \dots, A_n \in K_l$; thus $A \in T_P(K_l) \subset \sup_i T_P(K_i)$.

5. As demonstrated in question 3, the least Herbrand model of P is the least fixpoint of T_P. By Theorem 2.40, the least fixpoint of T_P is $\sup(\{T_P^n(\emptyset) \,/\, n \in \mathbb{N}\})$.

6. By induction on n, we can see that the sequence $T_P^n(B_H)$ is decreasing, hence $T_P(T_P^n(B_H)) = T_P^{n+1}(B_H) \subset T_P^n(B_H)$; in light of question 2, $T_P^n(B_H)$ is a model of P.

7. K is a model of P because $T_P(K) \subset K$.

8. The following example shows that K is not a fixpoint of P. Let P be defined by :

$$\begin{array}{ll} r_1 : & p(x) \Longrightarrow q(a) \ , \\ r_2 : & p(x) \Longrightarrow p(f(x)) \ , \\ r_3 : & q(x) \Longrightarrow q(f(x)) \ , \\ r_4 : & q(x) \Longrightarrow q(b) \ . \end{array}$$

Then $I_M = \emptyset$ and

$$\begin{aligned}
B_H &= \Big\{ p(X), q(X) \,/\, X \in \{f^n(a) \,,\, f^n(b) \,,\, n \in \mathbb{N}\} \Big\} \\
T_P(B_H) &= \Big\{ q(X), p(Y) \,/\, X \in \{f^n(a) \,,\, f^n(b) \,,\, n \in \mathbb{N}\} \,,\, Y \in \{f^k(a) \,,\, f^k(b) \,,\, k \geq 1\} \Big\} \\
T_P^2(B_H) &= \Big\{ q(X), p(Y) \,/\, X \in \{f^n(a) \,,\, f^n(b) \,,\, n \in \mathbb{N}\} \,,\, Y \in \{f^k(a) \,,\, f^k(b) \,,\, k \geq 2\} \Big\} \\
&\dots \\
K &= \Big\{ q(X) \,/\, X \in \{f^n(a) \,,\, f^n(b) \,,\, n \in \mathbb{N}\} \Big\} \\
T_P(K) &= \{ q(X), q(Y) \,/\, X = f^n(a) \,,\, Y = f^p(b) \,,\, n \geq 1 \,,\, p \geq 0 \} \\
T_P^2(K) &= \{ q(X), q(Y) \,/\, X = f^n(a) \,,\, Y = f^p(b) \,,\, n \geq 2 \,,\, p \geq 0 \} \\
&\dots \\
\nu(T_P) &= \{ q(Y) \,/\, Y = f^p(b) \,,\, p \geq 0 \}
\end{aligned}$$

Then $T_P(K) \neq K$, and the greatest fixpoint of T_P is $\nu(T_P) \subsetneq K$. Note that the least fixpoint of T_P is defined by $I_M = \emptyset$.

More generally, it can be shown that if $\nu(T_P)$ is the greatest fixpoint of T_P, then $\nu(T_P) \subset K$.

Chapter 6

6.1. We have n possible choices for the first element, then $n-1$ possible choices for the second element, etc. Hence $A_n^k = n(n-1)(n-2)\cdots(n-k+1) = \dfrac{n!}{(n-k)!}$.

6.2. Consider a partition of a set E with $a+b$ elements in $E = A \cup B$, where $A \cap B = \emptyset$, $|A| = a$, and $|B| = b$. Then $\binom{a+b}{p}$ is the number of subsets with p elements of E ; any subset with p elements of E can be obtained by choosing k elements in A and $n-k$ elements in B, for $0 \leq k \leq \inf(p, a)$.

6.3. 1. Apply Exercise 6.2 with $a = b = p = n$:

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}.$$

Hence, since $\binom{n}{k} = \binom{n}{n-k}$,

$$\binom{2n}{n} = \sum_{k=0}^{n} (\binom{n}{k})^2.$$

2. We apply the same method as in Exercise 6.2. $\binom{3n}{n}$ is the number of subsets with n elements of $E = A \cup B \cup C$, where $|A| = |B| = |C| = n$ and A, B, C are pairwise disjoint. We have $\sum_{i+j+k=n}^{n} \binom{n}{k}\binom{n}{i}\binom{n}{j} = \binom{3n}{n} = \sum_{k=0}^{n} \sum_{i=0}^{n-k} \binom{n}{k}\binom{n}{i}\binom{n}{n-i-k} = \sum_{k=0}^{n} \sum_{i=0}^{n-k} \binom{n}{k}\binom{n}{i}\binom{n}{i+k}$.
We might also directly apply the result of Exercise 6.2 by saying that a subset with n elements of $E = A \cup B \cup C$ can be obtained by choosing a subset with p elements in A and $n-p$ elements in $B \cup C$; i.e. $\sum_{k=0}^{n} \binom{n}{k} \sum_{i=0}^{n-k} \binom{n}{i}\binom{n}{n-i-k} = \sum_{k=0}^{n} \binom{n}{k} \sum_{i=0}^{n-k} \binom{n}{i}\binom{n}{i+k}$.

6.4. The number of n-tuples of disjoint subsets with p elements of a set with np elements is $\binom{np}{p} \times \binom{(n-1)p}{p} \times \binom{(n-2)p}{p} \times \cdots \times \binom{p}{p}$. Because the ordering of the subsets in the partition does not matter, $n!$ n-tuples of subsets correspond to a single partition, and we have

$$N = \frac{\binom{np}{p} \times \binom{(n-1)p}{p} \times \binom{(n-2)p}{p} \times \cdots \times \binom{p}{p}}{n!}.$$

6.5. $S = \binom{n}{p} \sum_{q=0}^{p} (-1)^q \binom{p}{q} = \binom{n}{p} \sum_{q=0}^{p} \binom{p}{q} (-1)^q 1^{p-q} = \binom{n}{p}(1-1)^p = 0$.

6.6. 1. By induction on k. For $k = 0$, the identity is clearly true. Assume it holds for k ; i.e. $\sum_{p=0}^{k} \binom{n+p}{p} = \binom{n+k+1}{k}$. Then, for $k+1$, $\sum_{p=0}^{k+1} \binom{n+p}{p} = \sum_{p=0}^{k} \binom{n+p}{p} + \binom{n+k+1}{k+1} = \binom{n+k+1}{k} + \binom{n+k+1}{k+1} = \binom{n+k+2}{k+1}$, by the identity (6.1) of Proposition 6.5. To intuitively motivate this identity, consider Pascal's triangle : the sum of the values at the black dots is to be found in the white square (see figure 15.3).

Figure 15.3

2. By induction on n. For $n = p$ the identity is trivially true. Assume it is true for n. Then $\binom{p}{p} + \binom{p+1}{p} + \cdots + \binom{n}{p} + \binom{n+1}{p} = \binom{n+1}{p+1} + \binom{n+1}{p} = \binom{n+2}{p+1}$. A look at Pascal's triangle will support intuition here as well.
Let $S_p = \sum_{k=1}^{n} k^p$.

- For $p = 1$, we have $S_1 = \sum_{k=1}^{n} k = \sum_{k=1}^{n} \binom{k}{1} = \binom{n+1}{2} = \dfrac{n(n+1)}{2}$.

- For $p=2$, we have $\binom{k}{2} = \dfrac{k(k-1)}{2} = \dfrac{k^2}{2} - \dfrac{k}{2}$; hence

$$2\binom{n+1}{3} = 2\Big(\sum_{k=2}^{n}\binom{k}{2}\Big) = (S_2-1)-(S_1-1) \qquad \text{and}$$

$$S_2 = S_1 + 2\binom{n+1}{3} = \frac{n(n+1)(n-1)}{3} + \frac{n(n+1)}{2} = \frac{n(n+1)(2n+1)}{6}$$

- For $p=3$, we have $\binom{k}{3} = \dfrac{k(k-1)(k-2)}{6} = \dfrac{k^3-3k^2+2k}{6}$, and thus

$$6\binom{n+1}{4} = (S_3-9)-3(S_2-5)+2(S_1-3) = S_3 - 3S_2 + 2S_1\,;$$

hence, finally,

$$S_3 = \frac{(n+1)n(n-1)(n-2)}{4} + \frac{n(n+1)(2n+1)}{2} - n(n+1) = \frac{n^2(n+1)^2}{4} = S_1^2.$$

6.7. By induction on the degree of P.

- If P has degree 0, (i.e. if $\forall x, \quad P(x)=c$), then : $\sum_{i=0}^{n+1}(-1)^i\binom{1}{i}P(x+i) = c\sum_{i=0}^{n+1}(-1)^i\binom{n+1}{i} = 0.$
- If P has degree $d+1$, then P can be written $P = xQ + c$, where Q has degree d. Let $n \geq d+1$. Hence,

$$\sum_{i=0}^{n+2}(-1)^i\binom{n+2}{i}P(x+i) = x\sum_{i=0}^{n+2}(-1)^i\binom{n+2}{i}Q(x+i) \\ + \sum_{i=0}^{n+2}(-1)^i\binom{n+2}{i}iQ(x+i) + c\sum_{i=0}^{n+2}(-1)^i\binom{n+2}{i}$$

By the induction hypothesis, the first summand of this sum is zero ; the third summand is trivially zero. We only have to compute $\sum_{i=0}^{n+2}(-1)^i i\binom{n+2}{i}Q(x+i)$, which can also be written

$$\sum_{i=0}^{n+1}(-1)^{i+1}(i+1)\binom{n+2}{i+1}Q(x+i+1).$$

Since $(i+1)\binom{n+2}{i+1} = (n+2)\binom{n+1}{i}$, we have

$$\sum_{i=0}^{n+1}(-1)^{i+1}(i+1)\binom{n+2}{i+1}Q(x+i+1) = -(n+2)\sum_{i=0}^{n+1}(-1)^i\binom{n+1}{i}Q(x+i+1) = 0\,.$$

6.8. The required probability distribution is

$$p = \frac{\text{number of favourable cases}}{\text{number of possible cases}} = \frac{n_f}{n}$$

There are twenty-seven cubes, each one having twenty-four possible orientations in the space, and they can be set in $(27)!$ possible ways. Thus, there are altogether $n = 24^{27}(27)!$ rebuilding possibilities.

In order to compute n_f, we consider the various types of cube and the ways in which they can be set up in order to rebuild a big red cube :

- There are eight cubes with three red sides ; each one can be oriented in three different ways in the space, and they can be permuted in 8! ways, and hence there are $3^8!$ 'right ways' to set up these eight cubes.
- There are twelve cubes with two red sides ; each one can be oriented in two different ways in the space, and they can be permuted in (12)! ways, and hence there are $2^{12}(12)!$ 'right ways' to set up these eight cubes.
- There are six cubes with one red side ; each one can be oriented in four different ways in the space, and they can be permuted in 6! ways, and hence there are $4^6 6!$ 'right ways' to set up these eight cubes.
- There is one white cube (the central cube), it can be oriented in twenty-four different ways, and hence, finally, $n_f = 3^8 \times 2^{12} \times 4^6 \times 24 \times 8! \times (12)! \times 6!$.

For the inquiring reader, $p \simeq 1,83 \times 10^{-37}$.

6.9. 1. There are eight possible choices for the face value of four cards of the same kind, and, as all four cards of the chosen face value are in the hand, it only remains to choose the fifth card of the hand among the twenty-eight remaining cards. Hence : 8×28 hands containing a four-of-a-kind.

2. There are eight possible choices for the face value of the three cards of the same kind and $\binom{4}{3}$ possible choices for the cards of the three-of-a-kind among the four cards of the chosen face value in the deck. We then have to choose the fourth and fifth cards in the hand. These fourth and fifth cards must have face values different from the face value of the three-of-a-kind (otherwise we would have a four-of-a-kind) and must not be of equal face values (otherwise we would have a three-of-a-kind **and** a pair). They can thus be chosen in $\binom{7}{2} \times 4 \times 4$ possible ways ($\binom{7}{2}$ choices for two face values and four choices for the face values of the fourth and fifth cards). Hence, finally : $8 \times \binom{4}{3} \times \binom{7}{2} \times 4^2$ hands containing a three-of-a-kind.

3. There are eight possible choices for the strength of the pair, then $\binom{4}{2}$ possible choices for the cards of the pair, and finally $\binom{7}{3} \times 4 \times 4 \times 4$ possible choices for the remaining three cards. Hence : $8 \times \binom{4}{2} \times \binom{7}{3} \times 4^3$ hands containing a pair.

6.10. $\binom{16}{8}$. It suffices to choose the place of the eight bits equal to 1.

6.11. 1. There corresponds such a generalized characteristic function for each pair (A_1, A_2) verifying (6.2) ; conversely, for any function $f\colon E \to \{0, 1, 2\}$, if we let $A_1 = f^{-1}(1)$ and $A_2 = f^{-1}(\{1, 2\})$, then (A_1, A_2) verifies (6.2). There are 3^n such functions ; thus $N_1 = 3^n$.

2. Similarly, we define a function $f\colon E \to \{0, 1, 2, 3\}$ for each triple (A_1, A_2, A_3) verifying (6.3), and we deduce that $N_2 = 4^n$.

6.12. 1. There are n_1 possible choices for the element of A and n_2 possible choices for the element of B. After that we can choose $p - 2$ elements in $\overline{A \cup B}$; hence

$$N = n_1 n_2 \binom{n - (n_1 + n_2)}{p - 2}, \qquad \text{letting } \binom{m}{q} = 0 \text{ if } q > m\,.$$

2. There are altogether $\binom{n}{p}$ subsets with p elements. Let C (resp. D) be the subsets with p elements having no element of A (resp. B). We have

$$|C \cup D| = |C| + |D| - |C \cap D| = \binom{n - n_1}{p} + \binom{n - n_2}{p} - \binom{n - (n_1 + n_2)}{p},$$

since $C \cap D$ is the set of subsets with p elements having no element from $A \cup B$. Thus $N = \binom{n}{p} - \binom{n-n_1}{p} - \binom{n-n_2}{p} + \binom{n-(n_1+n_2)}{p}$.

6.13. 1. 4^n.

2. Let A_1 (resp. A_2, A_3, A_4) be the set of strings of length n where the letter a (resp. b, c, d) does not occur. We want to count the number of elements in the complement of $A_1 \cup A_2 \cup A_3 \cup A_4$, i.e. $N = |\overline{A_1 \cup A_2 \cup A_3 \cup A_4}|$. We have $N = 4^n - |A_1 \cup A_2 \cup A_3 \cup A_4|$, and, by Proposition 6.13,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4| &= \sum |A_1| - \sum_{i<j} |A_i \cap A_j| \\ &\quad + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - |A_1 \cap A_2 \cap A_3 \cap A_4| \\ &= 4 \times 3^n - 6 \times 2^n + 4, \qquad \text{since } |A_1 \cap A_2 \cap A_3 \cap A_4| = 0\,. \end{aligned}$$

Thus $N = 4^n - 4 \times 3^n + 6 \times 2^n - 4$.

6.14. Let A (resp. B) be the permutations of $\{a, b, c, d, e, f\}$ containing 'ac' (resp. 'bde'). We want to count $\overline{A} \cap \overline{B} = \overline{A \cup B}$. By Proposition 6.13, $|A \cup B| = |A| + |B| - |A \cap B|$, and

- $|A| = 4! \times 5$, since in a permutation containing 'ac' there are 5 possible positions of 'ac' and $4\,!$ permutations of b, d, e, and f,
- $|B| = 3! \times 4$, since there are $3\,!$ permutations of a, c, and f and 4 possible positions of 'bde', and
- $|A \cap B| = 3! = 6$, since we have to permute the three subsequences 'ac', 'bde', and f.

Hence, finally : $N = |\overline{A \cup B}| = 6! - 4! \times 5 - 3! \times 4 + 6 = 582$.

6.15. $u_0 = 1$, $u_1 = 2$, $u_2 = 3$ and $u_n = 4$, for $n \geq 3$. The only possible strings are thus

$$1\underbrace{0\ldots0}_{n-2}\left\{\begin{matrix}0\\1\end{matrix}\right. \qquad \text{and} \qquad 0\underbrace{0\ldots0}_{n-2}\left\{\begin{matrix}0\\1\end{matrix}\right. \quad .$$

6.16. 1. An increasing mapping is necessarily injective ; thus, we must have $n \leq m$. With each increasing function, we can associate a unique set with n distinct values between 1 and m, namely, $\{f(1), \ldots, f(n)\}$. Conversely, with each set of n distinct values between 1 and m, we can associate a unique increasing sequence $f(1) < \cdots < f(n)$. There is thus a one-to-one correspondence between the set of subsets consisting of n elements between 1 and m and the set of increasing mappings from $\{1, \ldots, n\}$ to $\{1, \ldots, m\}$. Hence, the number of increasing mappings from $\{1, \ldots, n\}$ to $\{1, \ldots, m\}$ is $\binom{m}{n}$.

2. We want to count the number of increasing mappings such that the element $k + 1$ has a preimage. This boils down to determining the number of subsets with n elements between 1 and m containing $k + 1$. There are $\binom{n-1}{m-1}$ such subsets. (It remains, after choosing $k + 1$, to choose $n - 1$ elements among the $m - 1$ elements left.)

3. We wish to determine the number of increasing functions such that

$$|\{a \,/\, f(a) < k\}| = |\{a \,/\, f(a) > k\}|\,.$$

We must distinguish two cases here, according to the parity of n.

- If n is even, k has no preimage. The elements between 1 and $n/2$ have their images between 1 and $k - 1$, and the elements between $(n/2) + 1$ and n have their images between $k + 1$ and m. It is thus sufficient to choose $n/2$ values in $\{1, \ldots, k - 1\}$ and $n/2$ values in $\{k + 1, \ldots, m\}$. This is possible only if $(n + 1)/2 \leq k \leq m - n/2$ holds. The required number of functions is then $\binom{k-1}{n/2}\binom{m-k}{n/2}$.
- If $n = 2p + 1$ is odd, then the p first values of f are in $\{1, \ldots, k - 1\}$, the $(p + 1)$th value is k, and the p last values of f are in $\{k + 1, \ldots, m\}$. The required number of functions is thus $\binom{k-1}{p}\binom{m-k}{p} = \binom{k-1}{E\lfloor n/2 \rfloor}\binom{m-k}{E\lfloor n/2 \rfloor}$, where $E\lfloor n/2 \rfloor$ denotes the largest integer less than or equal to $n/2$.

4. We now wish to compute the number of injections verifying

$$|\{a \,/\, f(a) < k\}| = |\{a \,/\, f(a) > k\}|\,.$$

To cover all of them, it suffices to consider all possible permutations of increasing functions verifying the condition. We thus have $n!\,\binom{k-1}{p}\binom{m-k}{p}$ functions, with $n = 2p$ or $n = 2p + 1$.

6.17. 1. We will construct strings of length n. We thus have n positions, q_1 letters $a_1, \ldots$, and q_p letters a_p. Let us first place the letters a_1 in the string. There are $\binom{n}{q_1}$ ways of placing them. After all the letters a_1 are placed, there are $n - q_1$ places left. We then place the letters a_2. There are $\binom{n-q_1}{q_2}$ ways of positioning them, and there are $n - q_1 - q_2$ available positions afterwards. We place all the letters successively. The number of solutions is thus $\binom{n}{q_1}\binom{n-q_1}{q_2}\ldots\binom{n-(q_1+\cdots+q_{p-1})}{q_p}$.

(a) The formal polynomial $(X_1 + X_2 + \cdots + X_p)^n$ can be written, assuming that the variables $X_1, \ldots, X_n$ commute, as

$$(X_1+X_2+\cdots+X_p)^n = \sum_{q_1+q_2+\cdots+q_p=n} \binom{n}{q_1}\cdot\binom{n-q_1}{q_2}\ldots\binom{n-q_1-\cdots-q_{p-1}}{q_p} X_1^{q_1}X_2^{q_2}\cdots X_p^{q_p}.$$

(b) We could have done a direct computation by noticing that, among the $n!$ ways of placing n letters in n places, the q_i letters a_i can be permuted in $q_i!$ ways. We thus obtain $\dfrac{n!}{q_1!\cdots q_p!}$ and therefore deduce $\binom{n}{q_1}\binom{n-q_1}{q_2}\ldots\binom{n-(q_1+\cdots+q_{p-1})}{q_p} = \dfrac{n!}{q_1!\cdots q_p!} = \binom{n}{q_1,\ldots,q_p}$.

2. We apply the result of question 1 (b) with $n = k!$, $p = (k-1)!$, and $\forall i = 1, \ldots, p$, $q_i = k$. We obtain $\dfrac{(k!)!}{k!^{(k-1)!}}$, which is an integer.

3. 1287.

6.18. Let $f(x) = (1+x)^{2n} + (1-x)^{2n}$. Note that

$$(1+x)^{2n} = \sum_{p=0}^{2n}\binom{2n}{p}x^p, \qquad \text{and}$$
$$(1-x)^{2n} = \sum_{p=0}^{2n}(-1)^p\binom{2n}{p}x^p; \qquad \text{thus}$$
$$f(x) = (1+x)^{2n} + (1-x)^{2n} = 2\sum_{p=0}^{n}\binom{2n}{2p}x^{2p}.$$

Taking derivatives, we have

$$f'(x) = 4\sum_{p=1}^{n}p\binom{2n}{2p}x^{2p-1}, \qquad \text{and}$$
$$f''(x) = 4\sum_{p=1}^{n}p(2p-1)\binom{2n}{2p}x^{2p-2} = 8\sum_{p=1}^{n}p^2\binom{2n}{2p}x^{2p-2} - 4p\sum_{p=1}^{n}\binom{2n}{2p}x^{2p-2},$$
$$= 8g(x) - \frac{1}{x}f'(x).$$

Because we defined $g(x) = \sum_{p=1}^{n} p^2\binom{2n}{2p}x^{2p-2}$, we thus have

$$g(x) = \frac{1}{8}\left(f''(x) + \frac{1}{x}f'(x)\right).$$

Since

$$f'(x) = 2n\big((1+x)^{2n-1} - (1-x)^{2n-1}\big), \qquad \text{and}$$
$$f''(x) = 2n(2n-1)\big((1+x)^{2n-2} + (1-x)^{2n-2}\big),$$

we have
$$\begin{aligned} g(1) &= \frac{1}{8}\big(2n(2n-1)2^{2n-2} + 2n2^{2n-1}\big) \\ &= n(2n+1)2^{2n-4} = \sum_{p=0}^{n} p^2 \binom{2n}{2p}. \end{aligned}$$

But
$$g(1) = \sum_{p=1}^{n} p^2 \binom{2n}{2p} = \sum_{p=0}^{n} p^2 \binom{2n}{2p}.$$

6.19. Method 1

(a) x_{p+1} can take all the values from 0 to n. For each fixed value of x_{p+1}, $x_1+\cdots+x_p = n-x_{p+1}$, and there are thus $F(n-x_{p+1},p)$ solutions. Hence $F(n,p+1) = \sum_{k=0}^{n} F(k,p)$.

(b) By induction on n. If $n=0$, then $\binom{p}{p} = \binom{p-1}{p-1} = 1$; and if $\binom{n+p}{p} = \sum_{k=0}^{n}\binom{k+p-1}{p-1}$, then :

$$\begin{aligned} \sum_{k=0}^{n+1}\binom{k+p-1}{p-1} &= \sum_{k=0}^{n}\binom{k+p-1}{p-1} + \binom{n+1+p-1}{p-1} \\ &= \binom{n+p}{p} + \binom{n+p}{p-1} \qquad \text{(by the induction hypothesis)} \\ &= \binom{n+1+p}{p} \qquad \text{(by equation (6.1)).} \end{aligned}$$

We can also write $\sum_{k=0}^{n}\binom{k+p-1}{p-1} = \sum_{k=p-1}^{n+p-1}\binom{k}{p-1}$, and then apply the result of Exercise 6.6, 2.

(c) We show that $F(n,p) = \binom{n+p-1}{p-1}$ by induction on p. If $p=1$, then $F(n,p) = 1 = \binom{n}{0}$; the verification of the recurrence immediately follows from questions (a) and (b).

Method 2

(a) Let $E_{n,p}$ be the set of p-tuples $(x_1,\dots,x_p) \in \mathbb{N}^p$ such that $x_1+\cdots+x_p = n$; so $F(n,p) = |E_{n,p}|$. We can decompose $E_{n,p+1}$ in a partition : $E_{n,p+1} = A \cup B$, with $A = \{(x_1,\dots,x_p,0) \in \mathbb{N}^{p+1} \ / \ x_1+\cdots+x_p = n\}$ and $B = \{(x_1,\dots,x_p,x_{p+1}) \in \mathbb{N}^{p+1} \ / \ x_{p+1} > 0 \text{ and } x_1+\cdots+x_p+x_{p+1} = n\}$. Therefore,

- $|A| = |E_{n,p}|$, since any element of A can be obtained by adding a 0 component to a p-tuple in $E_{n,p}$.
- $|B| = |E_{n-1,p+1}|$, since B is in a one-to-one correspondence with $E_{n-1,p+1}$ as follows : if $(x_1,\dots,x_p,x_{p+1}) \in B$, subtract 1 from x_{p+1} in order to obtain $(x_1,\dots,x_p, x_{p+1}-1) \in E_{n-1,p+1}$.

We therefore deduce that $F(n,p+1) = F(n,p) + F(n-1,p+1)$.

(b) By induction on $k = n+p$. If $k=1$, then $n=0$, $p=1$, and $F(n,p) = 1 = \binom{0}{0}$. Assume the result is true for k, and let us compute $F(n,p)$ with $n+p = k+1$. By (a) we have $F(n,p) = F(n,p-1) + F(n-1,p)$, and by the recurrence, which can be applied because $n+p-1 = n-1+p = k$, we have $F(n,p) = \binom{n+p-2}{n} + \binom{n+p-2}{n-1} = \binom{n+p-1}{n}$.

Chapter 7

7.1. 1. $b_0 = 2$ (the empty tree $\emptyset$ and the tree $(a, \emptyset, \emptyset)$), $b_1 = 3$, $b_2 = 12$.

2. For $n \geq 2$, $b_n = \sum_{k=0}^{n-1} b_k \times b_{n-1-k}$.

7.2. 1.

- $u_0 = 1$ (the only binary tree of depth 0 is $\emptyset$),
- and for $n \geq 1$, $u_n = 1 + ku_{n-1}^2$: indeed a binary tree of depth less than or equal to n is of the form $\emptyset$ or (x, b_l, b_r) with $x \in \Sigma$ and with b_l, b_r binary trees of depth less than or equal to $n-1$.

2.

- $v_0 = 1$,
- for $n \geq 1$, $v_n = k(v_{n-1}^2 + 2v_{n-1}u_{n-2})$; indeed a binary tree of depth exactly n with $n \geq 1$, is of the form (x, b_l, b_r) with $x \in \Sigma$ and
  - either b_l, b_r binary trees of depth exactly $n-1$,
  - or $b_l \in U_{n-2}$ and $b_r \in AB_{n-1}$ (b_l is of depth strictly less than $n-1$, namely, b_l is of depth less than or equal to $n-2$, and b_r is of depth exactly $n-1$),
  - or, symmetrically, $b_r \in U_{n-2}$ and $b_l \in AB_{n-1}$.

7.3. If the nth line intersects the preceding lines in i distinct points, it will determine $i+1$ new regions, the first and the $(i+1)$th region will be infinite, the $i-1$ intermediate regions will be bounded. We advise the reader to draw a picture to support his/her intuition. The maximum possible number of bounded regions determined is thus, assuming that each new line is not parallel to any of the others,

$$\text{for} \quad n > 2 : \qquad r_n = (n-2) + r_{n-1} = (n-2) + (n-3) + \cdots + 1 = (n-1)(n-2)/2\,.$$

7.4. If there is a single circle it will obviously define two regions in the plane. Assume that $n-1$ circles define r_{n-1} regions, and add a new circle ; it will intersect each of the old $n-1$ circles in two points, and each crossing of an intersection point will define a new region, hence $2(n-1)$ new regions. We deduce, summing equations (7.3) for $i = 2, \ldots, n-1$, that $r_n = n(n-1) + 2$.

7.5. For $n = 2^k$, $k = 1, \ldots, l$, we write

$$\begin{array}{lrl}
(\times 2^{k-1}) & t_2 & = 1 \\
(\times 2^{k-2}) & t_4 & = 2t_2 + 1 \\
 & \vdots & \\
(\times 2) & t_{2^{k-1}} & = 2t_{2^{k-2}} + 1 \\
 & t_{2^k} & = 2t_{2^{k-1}} + 1
\end{array}$$

and we sum the above equalities multiplied by the indicated summation factors, hence :

$$t_{2^n k} = 2^k - 1$$

We can also show by induction that $t_{2^k} = 2^k - 1$.

(B) $t_2 = 2^1 - 1 = 1$,

(I) $t_{2^{k+1}} = 2t_{2^k} + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 1$.

For $n \neq 2^k$, the solution t_n is not uniquely defined (see Proposition 7.8).

7.6. $s_p = -p, \quad \forall p \in \mathbb{N}$, since $s_1 = 1 - 2$ and $s_{p+1} = s_p + 2p + 1 - (2p + 2) = s_p - 1$.

7.7. $u_n = u_{n-1} + u_{n-2}$, with $u_0 = u_1 = u_2 = 1$.

Similarly, with other types of recurrence, it suffices to impose initial conditions that are too stringent.

7.8. In general, it is enough to have initial conditions that are too weak.

$u_n = u_{n-1} + u_{n-2}$, with $u_0 = 1$.

$u_n = 2u_{n/2}$ with $u_1 = 1$; we then have the solutions $u_{2^n} = 2^n$ and $u_{(2k+1)2^n} = f(2k + 1)2^n$, where f can be an arbitrary function.

7.9. Notice that : $u_n - u_{n-1} = 3u_{n-1}$, hence :

$$u_n = 4u_{n-1} = 4^2 u_{n-2} = \ldots = 4^n u_0.$$

7.10. The characteristic polynomial of the recurrence is $r^3 - 5r^2 + 8r - 4 = 0$; it has a simple root 1 and a double root 2 ; the solution of the recurrence is thus of the form : $u_n = a + (b + cn)2^n$, the initial conditions allow us to determine a, b, c, since for $n = 0, 1, 2$, we obtain

$$\begin{aligned} a + b &= 0, \\ a + 2(b + c) &= 1, \\ a + 4(b + 2c) &= 2. \end{aligned}$$

hence : $a = -b = -2$ and $c = -1/2$ and, finally,

$$u_n = 2^{n+1} - n2^{n-1} - 2.$$

7.11. 1. a, b, aba, abb, baa, bab.

2. By induction on $|w|$. If $|w| \leq 1$, the result is true. Assume $w \in B$ and $|w| \leq n \Longrightarrow |w|$ is odd. Let $w' \in B$ and $|w'| = n+1$; then $w' = abw$ or $w' = baw$, with $w \in B$ and $|w| = |w'| - 2 \leq n - 1$, thus $|w|$ is odd by the recurrence, and thus $|w'| = |w| + 2$ is also odd.

The converse is not true ; for instance $w = aaa \notin B$.

3. $u_1 = 2$ and $u_2 = 0$; the recurrence relation is $u_n = 2u_{n-2}$.

Solving it directly, we obtain $u_{2n} = 0$, $u_{2n+1} = 2^{n+1}$. The characteristic polynomial method gives the characteristic polynomial : $r^2 - 2 = 0$, hence $u_n = \lambda(\sqrt{2})^n + \mu(-\sqrt{2})^n$, with $\lambda = -\mu = 1/\sqrt{2}$.

7.12. 1. $L_0 = \{\varepsilon\}$, $L_1 = \{a, b, c, d\}$, $L_2 = \{xy \,/\, x, y \in \Sigma, xy \neq ab\} = \Sigma^2 - \{ab\}$. $u_0 = 1$, $u_1 = 4$, $u_2 = 15$.

2. $w' \in L_{n-1}$, and, moreover, $w' \notin bL_{n-2}$ if $x = a$.

3. $L_n = \{a, b, c, d\}L_{n-1} - \{ab\}L_{n-2}$. Since $bL_{n-2} \subsetneq L_{n-1}$,

$$|L_n| = |\{a, b, c, d\}L_{n-1}| - |\{ab\}L_{n-2}| = 4|L_{n-1}| - |L_{n-2}|.$$

4. Characteristic polynomial : $r^2 - 4r + 1 = 0$, roots $r = 2 \pm \sqrt{3}$, hence :

$$u_n = \lambda(2 + \sqrt{3})^n + \mu(2 - \sqrt{3})^n$$

with

$$\begin{aligned} \lambda + \mu &= u_0 = 1 \\ \lambda(2 + \sqrt{3}) + \mu(2 - \sqrt{3}) &= u_1 = 4 \end{aligned}$$

$$\lambda = \frac{\sqrt{3} + 2}{2\sqrt{3}}, \qquad \mu = \frac{\sqrt{3} - 2}{2\sqrt{3}}$$

5. We obtain $u_n = \dfrac{\sqrt{2} + 1}{2}(2 + \sqrt{2})^n + \dfrac{1 - \sqrt{2}}{2}(2 - \sqrt{2})^n$.

7.13. The general solution of (7.11) (page 131) is of the form $u_n = ac^n e^{nit} + bc^n e^{-nit}$. Recall that

$$e^{iz} = \cos z + i \sin z \qquad \text{and} \qquad e^{-iz} = \cos z - i \sin z$$

We thus have

$$\begin{aligned} u_n &= ac^n(\cos(nt) + i\sin(nt)) + bc^n(\cos(nt) - i\sin(nt)) \\ &= (a+b)c^n \cos(nt) + i(a-b)c^n \sin(nt)) \end{aligned}$$

hence the result with $\lambda = a + b$ and $\mu = i(a - b)$; if the initial values are real, then the solution of (7.11) will be of the form $u_n = ac^n e^{nit} + bc^n e^{-nit}$, with a and b conjugate, and we will thus finally obtain $u_n = \text{Re }(a)c^n \cos(nt) + \text{Im }(a)c^n \sin(nt)$.

7.14. 1. The associated characteristic polynomial $r^2 - r + 2$ has the following two conjugate complex roots : $(1 \pm i\sqrt{7})/2$. We thus have

$$u_n = \alpha\left(\frac{1 + i\sqrt{7}}{2}\right)^n + \beta\left(\frac{1 - i\sqrt{7}}{2}\right)^n$$

If u_0 and u_1 are real, α and β are conjugate ; indeed in this case, if $\alpha = a + ia'$ and $\beta = b + ib'$,

$$\begin{aligned} &\alpha + \beta = u_0 \ , \\ &\alpha\left(\frac{1 + i\sqrt{7}}{2}\right) + \beta\left(\frac{1 - i\sqrt{7}}{2}\right) = u_1 \ ; \end{aligned}$$

hence $a + b = u_0$, $a' = -b'$, and finally, after solving the second equation,

$$a = b = \frac{u_0}{2} \qquad a' = -b' = -\frac{2u_1 - u_0}{2\sqrt{7}}$$

In this case we thus have

$$u_n = \text{Re}\left(\alpha\left(\frac{1 + i\sqrt{7}}{2}\right)^n\right)$$

2. Letting $v_n = u_n + 2$, v_n verifies the recurrence : $v_n = v_{n-1} - 2v_{n-2}$, and we are back to case 1.

7.15. 1. The characteristic polynomial of the recurrence is : $2r^2 - 3r + 1 = 0$; it has the roots $r = 1$ and $r = 1/2$; the general solution is thus of the form $u_n = a + b/2^n$.

2. The characteristic polynomial of the recurrence is : $r^2 - 4r + 4 = 0$; it has the double root $r = 2$; the general solution is thus of the form $u_n = (an + b)2^n$.

7.16. 1. We have

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = M \times \begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ -3 & -1 \end{pmatrix} \times \begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix} .$$

The eigenvalues of M are 1 and 2, and the associated eigenvectors are

$$V_1 = \begin{pmatrix} -2 \\ 3 \end{pmatrix} \qquad \text{and} \qquad V_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

we deduce that

$$M = N \times \Delta \times N^{-1} = N \times \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \times N^{-1} ,$$

with

$$N = \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix} \quad \text{and } N^{-1} = \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$$

hence

$$\begin{aligned} \begin{pmatrix} u_n \\ v_n \end{pmatrix} &= N \times \Delta^n \times N^{-1} \times \begin{pmatrix} a \\ b \end{pmatrix} = N \times \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix} \times \begin{pmatrix} a + b \\ 3a + 2b \end{pmatrix} \\ &= \begin{pmatrix} -2a - 2b + 2^n(3a + 2b) \\ 3a + 3b - 2^n(3a + 2b) \end{pmatrix} \end{aligned}$$

2. Letting $u'_n = \log u_n$, $v'_n = \log v_n$, we are back to case 1.

7.17. 1. $u_1 = 0$, $v_1 = 1$, $w_1 = 0$, $u_2 = 1$, $v_2 = 0$, $w_2 = 1$.

2. For $x \in \Sigma$, and $f \in \Sigma^n$, with $n \geq 1$, we have

$$fx \in L_0 \quad \Longleftrightarrow \quad \begin{cases} \text{either } f \in L_0 & \text{and } x = 0, \\ \text{or } f \in L_1 & \text{and } x = 1. \end{cases}$$

we thus have $u_{n+1} = u_n + v_n$; similarly $v_{n+1} = u_n + w_n$ and $w_{n+1} = w_n + v_n$.

3. Note that $\forall n \geq 1$, $u_{n+1} - w_{n+1} = u_n - w_n$; as, moreover, $u_1 = w_1 = 0$, we deduce $\forall n \geq 1$, $u_n = w_n$.

Thus,

$$\forall n \geq 1, \qquad v_{n+1} = 2u_n \,,$$
$$\forall n \geq 2, \qquad u_{n+1} = u_n + 2u_{n-1} \,.$$

We can then compute u_n ; the characteristic polynomial is $r^2 - r - 2 = (r-2)(r+1) = 0$; hence $u_n = a2^n + b(-1)^n$; from the initial conditions $u_1 = 0$ and $u_2 = 1$ we deduce $a = 1/6$ and $b = 1/3$; we obtain finally :

$$\forall n \geq 1, \qquad u_n = w_n = \frac{2^{n-1} + (-1)^n}{3} \,,$$
$$v_n = \frac{2^{n-1} - 2(-1)^n}{3} \,.$$

The matrix method here would give

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = M \times \begin{pmatrix} u_{n-1} \\ v_{n-1} \\ w_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} u_{n-1} \\ v_{n-1} \\ w_{n-1} \end{pmatrix} \,.$$

The eigenvalues of M are -1, 1 and 2, and associated eigenvectors are

$$V_{-1} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \quad , \quad V_1 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \quad \text{and} \quad V_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} .$$

We deduce that

$$M = N \times \Delta \times N^{-1} = N \times \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \times N^{-1} , \qquad \text{with}$$

$$N = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -2 & 1 \\ -1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad N^{-1} = \frac{1}{6} \begin{pmatrix} 3 & 0 & -3 \\ 1 & -2 & 1 \\ 2 & 2 & 2 \end{pmatrix} .$$

7.18. Let $u_n = |L_n|$, where

$$L_n = \{w \,/\, w \in L \text{ and } |w| = n\}$$

and construct L_n from L_{n-1}. Then we can write :

$$L_n = \{w = w'a \;/\; w' \in \{a,c,d\}^{n-1}\} \cup \{w = w'x \;/\; w' \in L_{n-1} \,,\; x \in \{b,c,d\}\} \,,$$

thus $u_n = 3u_{n-1} + 3^{n-1}$, with $u_0 = 1$, $u_1 = 4$. The characteristic polynomial is $(r-3)^2 = 0$, and thus $u_n = \lambda 3^n + \mu n 3^n$, with (because of the initial conditions) $\lambda = 1$ and $\mu = 1/3$, i.e. $u_n = 3^n + n3^{n-1}$.

7.19. This is a recurrence of the form (7.14) with $l = 1$, $b_1 = -1$ and $P_1(n) = 1$. The characteristic equation is $(r^2 - r - 2)(r + 1) = (r - 2)(r + 1)^2 = 0$; the general solution of the recurrence is thus $u_n = a2^n + (bn + c)(-1)^n$. Letting $n = 0, 1, 2$, we obtain the linear system in a, b, c :

$$\begin{aligned} a + c &= 1, \\ 2a - b - c &= 1, \\ 4a + 2b + c &= 4, \end{aligned}$$

giving the same result (fortunately !).

7.20. The characteristic polynomial is $(x^2 - 3x + 2)(x - 1)^2 = 0$, or $(x - 2)(x - 1)^3 = 0$. The general solution is thus of the form $u_n = \lambda 2^n + a + bn + cn^2$; to determine a, b, c, we first use the recurrence for computing $u_2 = 0$ and $u_3 = 4$; we then deduce : $\lambda = 4$, $a = -4$, $b = -2$, $c = -2$.

7.21. Letting $v_k = u_{2^k}$, we have $v_k = 4v_{k-1} + 2^{2k}$, hence $u_{2^k} = v_k = (u_1 + k)2^{2k}$.

7.22. 1. Let $v_n = 1/u_n$, hence $2v_n = v_{n-1} + v_{n-2}$, and we obtain a linear recurrence. The characteristic polynomial is $(2r + 1)(r - 1) = 0$, hence $v_n = \lambda(-1/2)^n + \mu$; we find $\lambda = 2/3(1/a - 1/b)$ and $\mu = 1/3(1/a + 2/b)$.

2. Let $v_n = \log u_n$, hence $2v_n = v_{n-1} + v_{n-2}$, $v_0 = 0$, $v_1 = \log 2$. We finally obtain $u_n = 2^{2/3(1-1/2^n)}$.

3. Let a_n be the solution of $v_n = v_{n-1} + v_{n-2}$, with $v_0 = a_0$ and $v_1 = a_1$, and let b_n be the solution of $v_n = v_{n-1} + v_{n-2}$, with $v_0 = b_0$ and $v_1 = b_1$. We check that $u_n = a_n/b_n$ verifies recurrence 3.

7.23. $(\Delta u)_n = \dfrac{-k}{(n-1)n(n+1)\cdots(n+k-1)} = \dfrac{-k}{(n-1)} u_n\,,\quad$ for $n > 0$.

Chapter 8

8.1. The sequence $u_0 = 1$, $u_1 = 0$, $u_2 = 0$, ..., $u_n = 0$, ... , represented by the polynomial $U(X) = 1$.

8.2. $\mathbf{u}(X) = (1 + X)^r \times (1 + X^2)^r = (1 + X + X^2 + X^3)^r$. We have

$$\begin{aligned} (1 + X)^r &= 1 + rX + \cdots + r(r-1)\cdots(r-k+1)\frac{X^k}{k!} + \cdots + X^r \\ &= \sum_{p=0}^{r} \binom{r}{p} X^p \\ (1 + X^2)^r &= 1 + rX^2 + \cdots + r(r-1)\cdots(r-k+1)\frac{X^{2k}}{k!} + \cdots + X^{2r} \\ &= \sum_{p=0}^{r} \binom{r}{p} X^{2p} \end{aligned}$$

hence
$$\begin{aligned} (1 + X)^r \times (1 + X^2)^r &= (1 + X + X^2 + X^3)^r \\ &= \sum_n \Big(\sum_{k'+2k=n} \binom{r}{k'}\binom{r}{k} \Big) X^n \\ &= \sum_n \Big(\sum_{k=0}^{n} \binom{r}{k}\binom{r}{n-2k} \Big) X^n \end{aligned}$$

No simpler form is known for the coefficients of this series.

8.3. Let : $\mathbf{v}_1 = 1$, and $\mathbf{v}_n = 0$ for all $n \neq 1$, namely, $\mathbf{v} = X$.

8.4. 1. Let $\mathbf{u}$ be an invertible series, $\exists \mathbf{w} \in \mathbb{C}[\![X]\!]$ with $\mathbf{uw} = \mathbb{1}$; hence $a_0 w_0 = 1$ and a_0 is invertible.

2. Conversely, assume a_0 invertible with inverse w_0, i.e. $w_0 a_0 = 1$. Then, as $\mathbf{u} = a_0 + X\mathbf{u}_l$, $w_0\mathbf{u} = 1 + Xw_0\mathbf{u}_l = 1 + \mathbf{v}$ with $\mathbf{v} = w_0 X\mathbf{u}_l$. As in Lemma 8.8, we can show that

$$w_0\mathbf{u}(\mathbb{1} - \mathbf{v} + \cdots + (-1)^n \mathbf{v}^n + \cdots) = \mathbb{1}\,.$$

Hence $\mathbf{u}$ is invertible.

8.5. Assuming that all the series considered converge for value x, lines (2) – (7) are consequences of the rules giving the power series expansions of derivatives, integrals, $\dfrac{1}{1-x}$, and of the definition convolution product of series.

8.6. 1. By induction on n.

(B) For $n = 0$, $\int_0^\infty e^{-t}dt = -\big[e^{-t}\big]_0^\infty = 1 = 0!$.

(I) Assuming the result is true for $n-1$, an integration by parts gives

$$\int_0^\infty t^n e^{-t}dt = \int_0^\infty nt^{n-1}e^{-t}dt - \big[t^n e^{-t}\big]_0^\infty = n\int_0^\infty t^{n-1}e^{-t}dt = n!$$

2. It is an immediate consequence : $\hat{u}(xt) = \sum_{n\geq 0} \dfrac{u_n}{n!}x^n t^n$, whence

$$\int_0^\infty \hat{u}(xt)e^{-t}dt = \sum_{n\geq 0}\Big(\frac{u_n}{n!}x^n \int_0^\infty t^n e^{-t}dt\Big) = \sum_{n\geq 0} u_n x^n.$$

8.7. The restriction $deg(U) < deg(V)$ can easily be deleted. If $deg(U) \geq deg(V)$, we can divide polynomial U by polynomial V and obtain : $g(x) = P_1(x) + \dfrac{U_1(x)}{V(x)}$ with $deg(U_1) < deg(V)$.

8.8. 1. Note that

$$\frac{x^{2^k}}{1 - x^{2^{k+1}}} = \sum_{p=0}^{\infty} x^{2^k + p2^{k+1}} = \sum_{p=0}^{\infty} x^{2^k(1+2p)}\ .$$

Furthermore, note that if $n \geq 1$, then there are unique integers $k \geq 0$ and $p \geq 0$, such that $n = 2^k(1+2p)$. Thus in the sum

$$\sum_{k=0}^{\infty} \frac{x^{2^k}}{1 - x^{2^{k+1}}} = \sum_{k=0}^{\infty}\sum_{p=0}^{\infty} x^{2^k(1+2p)},$$

each formal product x^n appears exactly once for each $n \geq 1$. Thus, we have

$$\sum_{k=0}^{\infty} \frac{x^{2^k}}{1 - x^{2^{k+1}}} = \frac{x}{1-x}$$

2. Recall that the Fibonacci numbers F_n are defined by : $F_n = \dfrac{r_1^n - r_2^n}{\sqrt{5}}$, where $r_1 = \dfrac{1+\sqrt{5}}{2}$ and $r_2 = \dfrac{1-\sqrt{5}}{2}$ are the roots of the equation $r^2 = r+1$, and satisfy $r_1 r_2 = -1$. Thus

$$\begin{aligned}
\sum_{k=0}^{\infty} \frac{1}{F^{2^k}} &= \sqrt{5}\left(\sum_{k=0}^{\infty} \frac{1}{r_1^{2^k} - r_2^{2^k}}\right) = \sqrt{5}\left(\sum_{k=0}^{\infty} \frac{r_2^{2^k}}{(r_1 r_2)^{2^k} - r_2^{2^{k+1}}}\right)\\
&= \sqrt{5}\left(\frac{r_2}{-1-r_2^2} + \sum_{k=1}^{\infty} \frac{r_2^{2^k}}{1-r_2^{2^{k+1}}}\right) = \sqrt{5}\left(\frac{r_2}{-1-r_2^2} + \frac{r_2}{1-r_2} - \frac{r_2}{1-r_2^2}\right)\\
&= \sqrt{5}\left(\frac{r_2}{-2-r_2} + \frac{r_2}{1-r_2} + 1\right) && \text{(since } r_2^2 = r_2+1\text{)}\\
&= \sqrt{5}\left(\frac{\sqrt{5}}{5} + \frac{\sqrt{5}-3}{2} + 1\right) = \frac{7-\sqrt{5}}{2}
\end{aligned}$$

8.9. The sequence of Fibonacci numbers has generating series

$$F(z) = \frac{P_1(z) - zP_0(z)}{1-z-z^2} = \frac{z}{1-z-z^2}\ ;$$

hence

$$\begin{aligned}
\sum_{n\geq 0} F_{2n} z^{2n} &= \frac{1}{2}\left(\frac{z}{1-z-z^2} + \frac{-z}{1+z-z^2}\right)\\
&= \frac{1}{2}\left(\frac{2z^2}{1-3z^2+z^4}\right)
\end{aligned}$$

and

$$\sum_{n\geq 0} F_{2n} z^n = \frac{z}{1-3z+z^2}$$

8.10. 1. Let $u(z) = \sum_{n\geq 0} u_n z^n$; then the recurrence equation implies

$$2(u(z) - u_0 - u_1 z) = 3z(u(z) - u_0) - z^2 u(z)\ ;$$

hence

$$\begin{aligned}
u(z) &= \frac{pz+q}{2-3z+z^2} = \frac{pz+q}{(1-z)(2-z)}\\
&= \frac{a}{(1-z)} + \frac{b}{(2-z)} = a\sum_{n\geq 0} z^n + \frac{b}{2}\sum_{n\geq 0} \frac{z^n}{2^n}\ ,
\end{aligned}$$

with $u_0 = a + b/2$ and $u_1 = a + b/4$.

2. If $u(z) = \sum_{n\geq 0} u_n z^n$, then

$$\begin{aligned}
u(z) &= \frac{pz+q}{1-4z+4z^2} = \frac{pz+q}{(1-2z)^2}\\
&= \frac{a}{(1-2z)^2} + \frac{b}{(1-2z)} = 2a\sum_{n\geq 0} n2^n z^{n-1} + b\sum_{n\geq 0} 2^n z^n
\end{aligned}$$

with $u_0 = b$ and $u_1 = 4a + 2b$.

8.11. Let $u(z) = \sum_{n \geq 0} u_n z^n$; then the recurrence equation gives : $\forall n \geq 2$, $u_n z^n = 4u_{n-1}z^n - 4u_{n-2}z^n + (n-1)z^n$. As

$$\sum_{n\geq 2}(n-1)z^n = \sum_{n\geq 1} nz^{n+1} = \sum_{n\geq 0} nz^{n+1} = z^2\left(\sum_{n\geq 0} nz^{n-1}\right) = z^2/(1-z)^2,$$

we deduce $u(z) - 1 - z = 4z(u(z) - 1) - 4z^2u(z) + z^2/(1-z)^2$, and

$$\begin{aligned} u(z) &= \frac{z^2 + (1-3z)(1-z)^2}{(1-z)^2(1-2z)^2} \\ &= \frac{1}{(1-z)^2} + \frac{2}{(1-z)} + \frac{1}{2(1-2z)^2} - \frac{5}{2(1-2z)} \\ &= \sum_{n\geq 0}(n+1)z^n + 2\sum_{n\geq 0} z^n + \frac{1}{2}\sum_{n\geq 0}(n+1)2^n z^n - \frac{5}{2}\sum_{n\geq 0} 2^n z^n \end{aligned}$$

Let $u_n = n + 3 + (n+1)2^{n-1} - 5 \times 2^{n-1}$. The reader can also solve the recurrence equation using the characteristic polynomial method and check that the same result is obtained.

8.12. We have $u(x) = 2xv(x) + x^2u(x) + 1$, and $v(x) = xu(x) + x^2v(x)$. The second equation gives $v(x) = xu(x)/(1-x^2)$; hence

$$u(x) = \frac{1-x^2}{1-4x^2+x^4}\ , \qquad v(x) = \frac{x}{1-4x^2+x^4}\ .$$

Noting that the common denominator is a function of x^2 we introduce

$$\begin{aligned} w(z) &= \frac{1}{1-4z+z^2} \\ &= \sum_{n\geq 0}\Big(\frac{3+2\sqrt{3}}{6}(2+\sqrt{3})^n + \frac{3-2\sqrt{3}}{6}(2-\sqrt{3})^n\Big)z^n, \end{aligned}$$

and we have $u(x) = (1-x^2)w(x^2)$ and $v(x) = xw(x^2)$. Finally : $u_{2n+1} = v_{2n} = 0$, $v_{2n+1} = w_n$ and $u_{2n} = w_n - w_{n-1} = (2+\sqrt{3})^n/(3-\sqrt{3}) + (2-\sqrt{3})^n/(3+\sqrt{3})$.

8.13. Let $u(x) = \sum_{n\geq 0} u_n x^n$; the recurrence equation yields $u(x) - 1 = 3x(u(x)-1) - 2x^2u(x) + 2x^2/(2-x)^2$, i.e.

$$\begin{aligned} u(x) &= \frac{(1-3x)(2-x)^2 + 2x^2}{(2-x)^2(1-x)(1-2x)} \\ &= \frac{(1-3x)(2-x)^2 + 2x^2}{2(2-x)^2(x-1)(x-1/2)}\ , \end{aligned}$$

which could be expanded to

$$u(x) = \frac{\alpha}{(2-x)^2} + \frac{\beta}{(2-x)} + \frac{\gamma}{(1-x)} + \frac{\delta}{(1-2x)}.$$

Instead we will apply Proposition 8.13 directly, which enables us to conclude

$$u(x) = \frac{(1-3x)(2-x)^2 + 2x^2}{2(2-x)^2(x-1)(x-1/2)} = \sum_{n\geq 0}\left(a + b2^n + \frac{cn+d}{2^n}\right)x^n, \tag{E}$$

with $a = 0$, $b = -5/9$, and $c = 2/3$. In order to determine d, let $x = 0$ in equation (E) ; we have $b + d = 4/4 = 1$ (also equal to u_0), and thus $d = 14/9$; hence, finally,

$$u_n = -\frac{5}{9}2^n + \left(\frac{2}{3}n + \frac{14}{9}\right)\frac{1}{2^n}\ .$$

One could also compute the characteristic polynomial $(x-1)(x-2)(x-1/2)^2 = 0$, and this gives a general solution of the form $u_n = a + b2^n + (cn+d)/2^n$. But then, one is left with the problem of finding a, b, c, d by solving a system of linear equations. Note that the constants a, b, c, d are not equal to $\alpha, \beta, \gamma, \delta$.

8.14. Let p be the number of tokens of value 2 and q the number of tokens of value 3. The problem amounts to finding the number of solutions of the equation $2p + 3q = n$. This is the same type of problem as given in Section 8.2.3. We will, however, solve the equation $2p+3q = n$ directly, without computing the partial fraction expansion. Indeed, here,

$$\begin{aligned} u(x) &= 1 + x^2 + x^4 + \cdots + x^{2p} + \cdots \ . \\ w(x) &= 1 + x^3 + x^6 + \cdots + x^{3q} + \cdots \ . \\ v(x) &= u(x) \times w(x) = \sum_{n\geq 0} \Big(\sum_{i+j=n} u_i w_j \Big) x^n \ . \end{aligned}$$

Since $u_i = \begin{cases} 1 & \text{if } i = 2k, \\ 0 & \text{otherwise,} \end{cases}$ and $w_j = \begin{cases} 1 & \text{if } j = 3k, \\ 0 & \text{otherwise,} \end{cases}$ it follows that the number v_n of ways of bringing up a total of n with tokens of value 2 and 3 is given by

$$v_n = \sum_{i+j=n} u_i w_j = \sum_{i=0}^{n} u_i w_{n-i} = \sum_{k=0}^{\lfloor n/2 \rfloor} w_{n-2k} \ ,$$

where $\lfloor n/2 \rfloor$ is the largest integer less than or equal to $n/2$. Finally,

- for n even, $w_{n-2k} = 1 \iff n - 2k$ is a multiple of 6,
- for n odd, $w_{n-2k} = 1 \iff n-2k$ is an odd multiple of 3 $\iff$ the remainder of the division of $n - 2k$ by 6 is 3.

Hence,

- for n even, v_n is the number of multiples of 6 between 0 and n,
- for n odd, v_n is the number of odd multiples of 3 between 0 and n.

8.15. Let us first find the recurrence equation defining the number u_n of Morse code words taking n time units : the last letter of the word is

- either a dot, and there are then u_{n-2} possibilities for the beginning of the word,
- or a dash, and there are then u_{n-3} possibilities for the beginning of the word,

hence $u_n = u_{n-2} + u_{n-3}$ for $n \geq 4$, with $u_0 = u_1 = 0$, $u_2 = u_3 = 1$.

The characteristic polynomial is given by $r^3 - r - 1 = 0$ and the generating series is given by

$$u(z) = \frac{z^2 + z^3}{1 - z^2 - z^3} = -1 + \frac{1}{1 - z^2 - z^3} \ .$$

We thus must find the roots of $V(z) = z^3 + z^2 - 1$. To this end, we will use the so-called Cardan method : letting $r = 1/z$ gives us the characteristic polynomial (see also Remark 8.15). We then look for a solution of the form $r = u + v$, which yields $u^3 + v^3 + 3u^2v + 3uv^2 - (u + v) - 1 = 0$, or $u^3 + v^3 + (u + v)(3uv - 1) - 1 = 0$. Assuming that $3uv - 1 = 0$ we have to solve

$$\begin{cases} 3uv = 1, \\ u^3 + v^3 = 1, \end{cases} \tag{15.1}$$

hence $v = 1/3u$ and $u^3 + 1/27u^3 = 1$. Hence u^3 and v^3 are roots of $u^6 - u^3 + 1/27 = 0$, with the conditions (15.1). We thus have $u^3 = 1/6(3 \pm \sqrt{23/3})$ and the roots r_1, r_2, r_3 of $r^3 - r - 1 = 0$ are, letting $\psi = \sqrt[3]{1/6(3 + \sqrt{23/3})}$ and $\psi' = \frac{1}{3}\psi^{-1} = \sqrt[3]{1/6(3 - \sqrt{23/3})}$,

$$r_1 = \psi + \psi', \qquad r_2 = j\psi + j^2\psi', r_3 = j^2\psi + j\psi'$$

where j and j^2 are the cubic roots of 1.

Finally, let us apply Proposition 8.11 and write

$$\frac{1}{1-z^2-z^3}=\sum_{n\geq 0}\left(\sum_{i=1}^{3}a_i r_i^{n+1}\right)$$

with for $i=1,2,3$

$$a_i=\frac{1}{V'(1/r_i)}=\frac{1}{3/r_i^2+2/r_i}=\frac{r_i^2}{3+2r_i}$$

Z The solution is different from the one of the preceding exercise because different sequences of dots and dashes taking the same total amount of time result in different words u_n.

8.16. Reasoning as in Section 8.2.3, we can check that the number of ways of changing n\$ with \$1, \$2 and \$5 bills is the coefficient of x^n in the series

$$\begin{aligned}v(x)&=\frac{\alpha_3}{(1-x)^3}+\frac{\alpha_2}{(1-x)^2}+\frac{\alpha_1}{1-x}+\frac{\beta}{1+x}\\&\qquad+\frac{\gamma}{1-e^{i\alpha}x}+\frac{\bar{\gamma}}{1-e^{-i\alpha}x}+\frac{\delta}{1-e^{2i\alpha}x}+\frac{\bar{\delta}}{1-e^{-2i\alpha}x}\\&=\sum_{n\geq 0}\big((a_2n^2+a_1n+a_0)+(-1)^nb\\&\qquad+(ce^{ni\alpha}+\bar{c}e^{-ni\alpha})+(de^{2ni\alpha}+\bar{d}e^{-2ni\alpha})\big)x^n\ .\end{aligned}$$

We can find the coefficients a_2,b,c,d of the above partial fraction expansion by using Proposition 8.11 and Proposition 8.13. We find $a_2=1/20$, $b=1/8$, $c=e^{2i\alpha}/(5(1-e^{-i\alpha})(1-e^{-2i\alpha}))$, $d=e^{-i\alpha}/(5(1-e^{-2i\alpha})(1-e^{i\alpha}))$. Finally a_1 and a_0 can be determined by assigning values to x.

The coefficient v_n of x^n can, however, be determined using slightly simpler computations ; writing

$$\begin{aligned}v(x)=(u\times w)(x)&=\frac{1}{(1-x)(1-x^2)(1-x^5)}=\frac{1}{(1-x)(1-x^2)}\times\frac{1}{(1-x^5)}\\&=(1+x)\times\frac{1}{(1-x^2)^2}\times\frac{1}{(1-x^5)}\\&=\sum_{n\geq 0}\big((n+1)x^{2n}(1+x)\times\sum_{n\geq 0}x^{5n}\big)=\sum_{n\geq 0}\big(\sum_{j=0}^{n}u_jw_{n-j}\big)\,,\end{aligned}$$

we deduce that $v_n=\sum_{k=0}^{\lfloor n/5\rfloor}w_{5k}u_{n-5k}$; as $u_{2n}=u_{2n+1}=n+1$. We have, after computations,

$$v_n=\sum_{0\leq i\leq\lfloor n/5\rfloor}(1+5i)+\sum_{0\leq i<\lfloor n/5\rfloor}(3+5i)\ ,$$

which immediately yields

$$v_n=5(\lfloor n/5\rfloor)^2+4\lfloor n/5\rfloor-3\,.$$

For $n=100$, we find $v_{100}=2077$.

8.17. Let $u(x)=\sum_{n\geq 0}u_nx^n$; then $u'(x)=\sum_{n\geq 0}nu_nx^{n-1}$ hence $2u'(x)=u(x)+e^x$; solving the differential equation $2y'-y=e^x$ yields $y=e^x+ce^{x/2}$, and the initial condition $y(0)=2$ implies $c=1$; thus, finally, $u(x)=e^x+e^{x/2}$, and $u_n=\dfrac{1}{n!}\left(1+\dfrac{1}{2^n}\right)$.

We could also have applied the summation factors technique : multiplying the equation giving u_k by $2^{k-1}(k-1)!$ and summing for k ranging from 0 to n, we find $2^nn!u_n=\sum_{k=0}^{n-1}2^k+2=2^n+1$.

8.18. 1. By structural induction.

2. It immediately follows, from the inductive definition of the words in the Dyck language, that $u_n = \sum_{i=0}^{n-1} u_i u_{n-i-1}$ for $n \geq 1$, and $u_0 = 1$. u_n is thus the nth Catalan number.

3. The words of the Dyck language on the alphabet A_k always have an even length ; if v_n is the number of words of length $2n$ in the Dyck language on A_k, we obtain the recurrence equation $v_n = k\sum_{i=0}^{n-1} v_i v_{n-i-1}$ for $n \geq 1$, and $v_0 = 1$. This recurrence equation can be solved in two different ways :

- Noting that $v_1 = ku_1$ we can show by induction on n that $\forall n \geq 1$, $v_n = k^n u_n$.
- Computing as for the sequence b_n we will obtain the equation

$$kxv^2 - v + 1 = 0$$

defining the generating series $v = v(x)$ of the sequence v_n. Solving, we find

$$v(x) = \frac{1 - \sqrt{1-4kx}}{2kx} = b(kx),$$

wherefrom it follows that

$$\forall n \geq 0, \qquad v_n = \frac{k^n}{n+1}\binom{2n}{n} = \frac{k^n}{n+1}\frac{(2n)!}{n!n!}\ .$$

8.19. Multiplying the equation $u_n = u_{n-1} + 2u_{n-2} + \cdots + nu_0$ by x^n for each $n > 0$ in $\mathbb{N}$, and summing the equalities thus obtained we have

$$\begin{aligned} u(x) - 1 &= xu(x) + 2x^2u(x) + \cdots + nx^n u(x) + \cdots \\ &= x\frac{1}{(1-x)^2}u(x) \end{aligned}$$

and

$$u(x) = \frac{xu(x)}{(1-x)^2} + 1,$$

hence

$$u(x) = \frac{1-2x+x^2}{1-3x+x^2} = 1 + \frac{x}{1-3x+x^2}\ ,$$

and thus (see Exercise 8.9), $u_0 = 1$, and $u_n = F_{2n}$ for $n > 0$.

8.20. For all $n \geq 2$ in $\mathbb{N}$, let us multiply the equation $u_n = -2nu_{n-1} + \sum_{k=0}^{n}\binom{n}{k}u_k u_{n-k}$ by $\dfrac{x^n}{n!}$, and then sum the equalities thus obtained ; we have :

$$\begin{aligned} \hat{u}(x) - x &= -2x\hat{u}(x) + \sum_n \Big(\sum_k \binom{n}{k} u_k u_{n-k}\Big)\frac{x^n}{n!} \\ &= -2x\hat{u}(x) + \sum_n \Big(\sum_k \frac{n!}{k!(n-k)!}u_k u_{n-k}\Big)\frac{x^n}{n!} \\ &= -2x\hat{u}(x) + \sum_n \Big(\sum_k \frac{u_k x^k}{k!}\frac{u_{n-k}x^{n-k}}{(n-k)!}\Big) \\ &= -2x\hat{u}(x) + (\hat{u}(x))^2 \end{aligned}$$

Hence $\hat{u}(x) = -2x\hat{u}(x) + (\hat{u}(x))^2 + x$; and finally, $\hat{u}(x) = 1/2(1 + 2x - \sqrt{1+4x^2}$, and thus : $\forall n \geq 1$, $u_{2n+1} = 0$ and $u_{2n} = (-1)^n(2n)!b_{n-1}$, where b_{n-1} is the $(n-1)$th Catalan number.

8.21. 1.(a) $t_1 = 3$ (no constraint) ; $t_2 = 3^2 = 9$ (no constraint) ; $t_3 = 3.3.2 = 18$ (we choose the first two colours in A : 3×3 choices, we then choose the third colour in $A\backslash\{a\}$: two choices.

1.(b) Recurrence equation ; in order to form a size n solution, with $n \geq 3$:

- we first form a size $(n-1)$ solution ; we can do this in t_{n-1} different ways ;
- we then choose the last colour in $A\backslash\{a_{n-2}\}$; this can be done in two different ways.

We thus have, for $n \geq 3$, $t_n = 2t_{n-1}$.

1.(c) We have $t_1 = 3$. We deduce from (b) that $t_n = 2^{n-2}t_2$, hence, since $t_2 = 9$,

$$t_n = 9.2^{n-2} \text{ if } n \geq 2.$$

2.(a) $s_1 = 3$ (no constraint) ; $s_2 = 9$ (no constraint) ; for s_3, if $a_1 \neq a_3$ there are eighteen possible choices, and if $a_1 = a_2 = a_3$, three possible choices, hence $s_3 = 18 + 3 = 21$; for s_4, there are six solutions of the form $aaab$, six solutions of the form $abbb$, with $a \neq b$ and three solutions of the form $aaaa$; hence $s_4 = t_4 + 6 + 6 + 3 = 51$.

2.(b) Recurrence equation ; consider a size n solution $a_1, a_2, \ldots, a_n$ with $n \geq 3$.

Two cases are possible :

(α) $a_{n-2} \neq a_n$. In this case, we form a size $(n-1)$ solution : s_{n-1} choices are possible for doing so, we then choose the last colour in $A\backslash\{a_{n-2}\}$ and two choices are possible for this last colour.

(β) $a_{n-2} = a_{n-1} = a_n$. In this case, we form a size $(n-2)$ solution ; s_{n-2} choices are possible for doing so. We then complete by two occurrences of the last letter a_{n-2}.

We thus obtain the recurrence equation

$$s_n = 2s_{n-1} + s_{n-2}, \qquad \text{for } n \geq 3.$$

2.(c) Associated generating series. Let $s(z) = \sum_{n\geq 1} s_n z^n$. By the above formula, we have

$$\sum_{n\geq 3} s_n z^n = 2\sum_{n\geq 3} s_{n-1}z^n + \sum_{n\geq 3} s_{n-2}z^n ,$$

thus

$$s(z) - s_1 z - s_2 z^2 = 2z(s(z) - s_1 z) + z^2 s(z)$$

or

$$s(z)(z^2 + 2z - 1) = -3(z^2 + z)$$

and

$$s(z) = \frac{-3z(z+1)}{z^2 + 2z - 1} .$$

Then find the partial fraction expansion of $s(z)$:

$$\begin{aligned} s(z) &= z\Big(-1 + \frac{1+\sqrt{2}}{2(z+1+\sqrt{2})} + \frac{1-\sqrt{2}}{2(z+1-\sqrt{2})}\Big) \\ &= z\Big(-1 + \frac{1}{2} \times \frac{1}{1-z(1-\sqrt{2})} + \frac{1}{2} \times \frac{1}{1-z(1+\sqrt{2})}\Big) , \end{aligned}$$

we find

$$s_n = \frac{3}{2}[(1-\sqrt{2})^n + (1+\sqrt{2})^n] \quad \text{for } n \geq 1.$$

8.22. 1. $b_1 = 0$, $b_2 = 1$ (transposition), $b_3 = 2$.

2. Let f be defined by $f(e_i) = c_j$ if and only if pupil e_i receives the exercise c_j of e_j.

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \xrightarrow{f} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} .$$

Let $c_i = f(e_1)$ be the exercise given to pupil e_1 : we have $(n-1)$ choices for c_i. Two disjoint cases are possible : $f(e_i) = c_1$, or $f(e_i) = c_j$ with $j \neq 1, i$.

- In the first case, pupils $\{e_1, e_i\}$ interchange the exercises $\{c_1, c_i\}$; hence e_1 and e_i interchange their exercises and $n-1$ choices are possible for e_i ; b_{n-2} choices remain to redistribute the $n-2$ remaining exercises amongst the $n-2$ remaining pupils. Hence, $(n-1)b_{n-2}$ possible choices altogether.
- In the second case, we delete the pair $\{e_i, c_i\}$. The $(n-1)$ remaining pupils distribute the $(n-1)$ remaining exercises : we have b_{n-1} possible choices. Pupil e_1 then obtains exercise c_j with $j \neq 1, i$. This exercise is in fact for pupil e_i. e_1 thus gives exercise c_j to e_i, and obtains exercise c_i in exchange $(i \neq 1)$. There are thus $(n-1)b_{n-1}$ possible choices.

Finally,

$$b_n = (n-1)(b_{n-1} + b_{n-2}), \qquad \text{for } n \geq 2. \tag{I}$$

(with $b_0 = 1$ and $b_1 = 0$).

3. Let us prove the equation

$$b_n - nb_{n-1} = (-1)^n, \qquad \text{for } n \geq 2. \tag{II}$$

by an inductive proof.

- If $n = 2$, $b_2 - 2b_1 = b_2 = 1 = (-1)^2$. The formula is true in this case.
- Assuming the formula is true for n, let us form $b_{n+1} - (n+1)b_n$. Applying formula (I), which is possible because $n + 1 \geq 2$, we have

$$\begin{aligned} n(b_n + b_{n-1}) - nb_n - b_n &= nb_{n-1} - b_n \\ &= -(-1)^n \ \text{(by the induction hypothesis)} \\ &= (-1)^{n+1} \end{aligned}$$

The formula is thus indeed proved for all $n > 1$. We can note that, letting $b_0 = 1$, the formula is also true for $n = 1$.

4. Let $b(z) = \sum_{n \geq 0} \frac{b_n z^n}{n!}$.

Applying formula (II), true for $n \geq 1$,

$$\sum_{n \geq 1} \frac{b_n z^n}{n!} - \sum_{n \geq 1} nb_{n-1} \frac{z^n}{n!} = \sum_{n \geq 1} \frac{(-1)^n z^n}{n!} ,$$

i.e. $b(z) - b_0 - zb(z) = e^{-z} - 1$, or $b_0 = 0$; hence $b(z) = \dfrac{e^{-z}}{1-z}$.

Chapter 9

9.1. The constant c such that $kn \leq cn$ is different for each term kn ; on the other hand, when writing :$\sum_{k=1}^{n} O(n) = nO(n)$, we implicitly assume that **all** the $O(n)$s refer to the same constant c. In other words, when $k = n$, $kn \neq O(n)$.

A correct argument would be : $\sum_{k=1}^{n} kn = \sum_{k=1}^{n} O(n^2) = O(n^3)$.

9.2. 1. Yes.

2. No, for instance : $f(n) = n + \log_2 n = O(n)$, but $2^{f(n)} = 2^{n+\log_2 n} = n2^n$ is not an $O(2^n)$ since $2^{f(n)}/2^n$ goes to infinity when n goes to infinity.

9.3. No : if $g_1(n) = n^2$ and $g_2(n) = 1$, $n = O(g_1(n) + g_2(n))$, but $n \notin g_1(n) + O(g_2(n))$.

9.4. Similar to the proof of case (i).

9.5. 1. By recurrence on n it can be checked that $u_n \geq 1$ for all n. Let, for $n \geq 1$,

$$\begin{aligned} u_n^2 - u_{n-1}^2 &= (u_n - u_{n-1})(u_n + u_{n-1}) \ , \\ &= \frac{1}{u_{n-1}}(2u_{n-1} + \frac{1}{u_{n-1}}) = 2 + \frac{1}{u_{n-1}^2} \geq 2 \ . \end{aligned}$$

As $u_n \geq 1$,

$$\frac{1}{u_{n-1}^2} \leq \frac{1}{u_{n-1}} \ .$$

2. From 1 it follows that

$$2 \leq u_n^2 - u_{n-1}^2 \leq 2 + \frac{1}{u_{n-1}} = 2 + u_n - u_{n-1} \ ,$$

whence the inequalities (9.1).

3. Finally, summing the inequalities (9.1), we have $2n \leq u_n^2 - c^2 \leq 2n + u_n - c$. We deduce that :

- $\lim_{n\to\infty} u_n^2 = \infty$,
- hence, $u_n = o(u_n^2)$ and $u_n^2 = \Omega(2n)$,
- from $2n \leq u_n^2 - c^2 \leq 2n + u_n - c$ we deduce, since $u_n = o(u_n^2)$ and $c = o(u_n^2)$, that

$$2n + o(u_n^2) \leq u_n^2 \leq 2n + o(u_n^2) \ ,$$

i.e. $u_n \sim \sqrt{2n}$.

9.6. $\left(e^{an^b} \times n^c \times (\log n)^d\right) \prec \left(e^{a'n^{b'}} \times n^{c'} \times (\log n)^{d'}\right)$ if and only if

- either $a > 0, a' > 0$, and $bacd < b'a'c'd'$ in the lexicographic ordering,
- or $a < 0, a' < 0$, and
  - $b > b'$,
  - or $b = b'$ and $acd < a'c'd'$, in the lexicographic ordering,
- or $a = 0$ or $a' = 0$, and $a < a'$ (car $b > 0$),
- or $a = 0$ and $a' = 0$, and $cd < c'd'$ in the lexicographic ordering,
- or $a < 0$ and $a' > 0$.

9.7. By induction on k ; let $k=1$, and assume there are two principal parts of f with respect to E. We thus have : $f=a_1g_1+o(g_1)$ and $f=a_2g_2+o(g_2)$; hence : $\lim_{n\to\infty}\dfrac{f(n)}{a_1g_1(n)}=1=\lim_{n\to\infty}\dfrac{f(n)}{a_2g_2(n)}$ and thus, $\lim_{n\to\infty}\dfrac{a_2g_2(n)}{a_1g_1(n)}=1$. Hence $\lim_{n\to\infty}\dfrac{g_2(n)}{g_1(n)}=\dfrac{a_1}{a_2}$, with $0\neq\dfrac{a_1}{a_2}\neq\infty$. Henceforth g_1 and g_2 have the same order of magnitude ; by condition (ii) of Definition 9.19, we deduce that $g_1=g_2$ and $a_1=a_2$. The inductive step of the induction is proved in a similar way.

9.8. Note that

$$(1+n)^{1/n}=e^{\frac{log(1+n)}{n}},$$

and that

$$\begin{aligned}\log(1+n)&=\log\Big(n\Big(1+\frac{1}{n}\Big)\Big)=\log n+\log\Big(1+\frac{1}{n}\Big)\\&=\log n+\frac{1}{n}-\frac{1}{2n^2}+O(n^{-2})\,.\end{aligned}$$

Let

$$u(n)=\frac{\log n}{n}+\frac{1}{n^2}-\frac{1}{2n^3}+O(n^{-3})\,,$$

then $\lim_{n\to\infty}u(n)=0$, and squaring, then cubing, the asymptotic power series expansion of $u(n)$, we have

$$\begin{aligned}(u(n))^2&=\frac{(\log n)^2}{n^2}+\frac{2\log n}{n^3}+o\Big(\frac{\log n}{n^3}\Big)\,,\\(u(n))^3&=\frac{(\log n)^3}{n^3}+o\Big(\frac{(\log n)^3}{n^3}\Big)\,.\end{aligned}$$

We deduce

$$\begin{aligned}f(n)=e^{u(n)}&=1+u(n)+\frac{(u(n))^2}{2!}+\frac{(u(n))^3}{6}+o((u(n))^3)\\&=1+\frac{\log n}{n}+\frac{1}{2}\frac{(\log n)^2}{n^2}+\frac{1}{n^2}+\frac{1}{6}\frac{(\log n)^3}{n^3}+o\Big(\frac{(\log n)^3}{n^3}\Big)\,.\end{aligned}$$

9.9. 1. Nothing valuable ; we would obtain a term of the form

$$\sum_{0<k<n}\frac{1}{k^2(n-k)}=\frac{1}{n}H_{n-1}^2+\frac{2}{n^2}H_{n-1}\,,$$

implying only that $u_n=\Omega(1/n)$.
2. Note, first, that

$$u(1)=\exp\left(\sum_{k\geq 1}\frac{1}{k^2}\right)=e^{\pi^2/6}\,;$$

Writing

$$nu_n=\sum_{0\leq k<n}\frac{u_k}{n}+\sum_{0\leq k<n}u_k\Big(\frac{1}{n-k}-\frac{1}{n}\Big)\,,$$

i.e.

$$nu_n=\frac{1}{n}\sum_{0\leq k}u_k-\frac{1}{n}\sum_{n\leq k}u_k+\frac{1}{n}\sum_{0\leq k<n}\frac{ku_k}{n-k}\,. \qquad (S)$$

The first sum in (S) returns $u(1)$, and we can show that :

$$\sum_{n\leq k}u_k=O\Big(\frac{(\log n)^2}{n}\Big)\quad\text{and}\quad O\Big(\sum_{0\leq k<n}\frac{(\log n)^2}{k(n-k)}\Big)=O\Big(\frac{(\log n)^3}{n}\Big)\,;$$

this enables us to bound the second and third terms of the sum (S) by $O\left(\frac{(\log n)^3}{n^3}\right)$; bootstrapping once more we obtain

$$u_n = \frac{e^{\pi^2/6}}{n^2} + O\left(\frac{\log n}{n^3}\right).$$

9.10. It is easy to see that $u_n < \sum_0^n n = n^2 = O(n^2)$. Assuming

$$u_n = an^2 + bn + c \qquad (I)$$

and plugging in the recurrence defining u_n, we have

$$u_n = n + u_{n-1} = an^2 + (1 + b - 2a)n + a - b + c\,,$$

wherefrom we deduce, identifying with (I),

- that $a = b = 1/2$,
- and that, *if* (I) is true for u_{n-1} with $a = b = 1/2$, *then* (I) is also true for u_n; writing that (I) is true for u_0, we have $c = 0$ and thus $u_n = n(n+1)/2$.

Chapter 10

10.1. We prove this result for the case of undirected graphs. The case of directed graphs is quite similar.

Let $G = (V, E, \delta)$ and $G' = (V', E', \delta')$. It is easy to see that if

- either G' is a subpartial graph of G,
- or G' is a partial graph of a subgraph of G,

then

$$V' \subseteq V, E' \subseteq E \quad \text{and} \quad \forall e \in E', \delta'(e) = \delta(e).$$

It thus suffices to prove the converse of this property.

(a) Let H be the graph (V', E'', δ'') with $A'' = \{e \in E \,/\, \delta(e) \subseteq V'\}$ and $\forall e \in A'', \delta''(e) = \delta(e)$. Then, by definition, H is a subgraph of G. Because $\forall a \in A', \delta'(e) = \delta(e) \subseteq V'$, $A' \subseteq A''$ and G' is a partial graph of H.

(b) Let H' be the graph (V, E', δ') which clearly is a partial graph of G. Then, $\forall e \in E'$, $\delta'(e) \subseteq V'$ and thus G' is a subgraph of H'.

10.2. Each edge of a directed graph is counted once in the outdegree of its origin and once in the outdegree of its target. The sum of all indegrees is thus equal to the sum of all outdegrees and is also equal to the number of edges.

10.3. 1. Let V_k, for $0 \le k \le K$, be the set of the vertices of degree k. By definition, $|V_k| = n_k$. As $V = \bigcup_{k=0}^K V_k$ and as the V_ks are pairwise disjoint, $n = |V| = \sum_{k=0}^K n_k$.

The sum of the degrees of the vertices is

$$p = \sum_{v \in V} d(v) = \sum_{k=0}^{K} \sum_{v \in V_k} d(v) = \sum_{k=0}^{K} k|V_k| = \sum_{k=0}^{K} kn_k.$$

Moreover, we know that $p = 2m$.

2. Since $n_K \neq 0$, $K \le Kn_K \le \sum_{k=0}^K kn_k = 2m$. This bound is reached for the graph with one vertex and m edges that all are loops.

3. Let v be any fixed vertex. For all vertices v' of the graph (including vertex v), denote by $E_{v'}$ the set of edges connecting v and v', i.e.

$$\begin{cases} E_{v'} = \{e \,/\, \delta(e) = \{v, v'\}\} & \text{if } v \neq v', \\ E_v = \{e \,/\, \delta(e) = \{v\}\}. \end{cases}$$

The degree of v is thus equal to $2|E_v| + \sum_{v' \neq v} |E_{v'}|$. Because the graph has no loop, $E_v = \emptyset$, and because the graph has no multiple edges, $E_{v'}$ has at most one element for $v' \neq v$. Hence, $d(v) \le \sum_{v' \neq v} 1 = n - 1$. The bound is reached for complete graphs, i.e. graphs such that $\forall v, v' \in V,\, v \neq v' \Longrightarrow \exists e \in E : \delta(e) = \{v, v'\}$.

10.4. Because the graph is simple, the degree of a vertex v is the number of vertices $t \neq v$ that are adjacent to v, i.e. connected to v by an edge.

1. Let v be a vertex. There are $n-1$ other vertices ; at most $n-1$ among them are adjacent to v, and hence $d(v) \leq n-1$.

2. If a vertex v has degree $n-1$, it is adjacent to $n-1$ other vertices, i.e. to all other vertices ; consequently, all other vertices (each of which is adjacent to v) are of degree ≥ 1.

3. Assume that the degrees are pairwise different. They form a sequence $d_1 < d_2 < \cdots < d_n$. We have that $d_1 \geq 0$, and 1 implies that $d_n < n$. Because the d_is are integers, this gives $d_1 = 0, d_2 = 1, \ldots, d_n = n-1$ which contradicts 2. Hence, there are at least two equal degrees.

10.5. 1. Let V_x be the set of vertices of $V - \{x, y\}$ which are adjacent to x, and let V_y be the set of the vertices of $V - \{x, y\}$ which are adjacent to y. We assume that $z \in V_x \cap V_y$. Then x, y, z, which are mutually adjacent, form a triangle, a contradiction. Thus $V_x \cap V_y = \emptyset$. We also have $V_x \cup V_y \subseteq S - \{x, y\}$ by definition. Hence,

$$n_x + n_y = |V_x| + |V_y| = |V_x \cap V_y| \leq |V - \{x, y\}| = |V| - 2.$$

2. By induction on $n = |V|$

- Initialization : It holds for $n = 1, 2$:

$$n = 1 : |E| = 0 \leq \frac{1}{4} = \frac{|V|^2}{4} ,$$
$$n = 2 : |E| \leq 1 \leq \frac{4}{4} = \frac{|V|^2}{4} .$$

- We assume that the property is true for n. We show that it is true for $n+2$. Let $|V| = n+2$. If there are no edges, then $|E| = 0 \leq |V|^2/4$. If there is at least one edge, consider two adjacent vertices x and y. Let $V' = V - \{x, y\}$ and $A' = \{a \in A \mid \delta(e) \subseteq V'\}$. The graph (V', E', δ) has no triangle, and $|V'| = n$. By the induction hypothesis we have $|E'| \leq |V'|^2/4 = \frac{n^2}{4}$. The edges of E are
  - those of E',
  - the edge between x and y,
  - those between x and the vertices of V', and
  - those between y and the vertices of V'.

Thus $|E| = |E'| + 1 + n_x + n_y$. Since $|E'| \leq \frac{n^2}{4}$ and $n_x + n_y \leq |V| - 2 = |V'|$ (by 1), we have

$$|E| \leq \frac{n^2}{4} + 1 + n = \frac{n^2 + 4n + 4}{4} = \frac{(n+2)^2}{4}.$$

The property is also true for $n + 2$.

By induction it is thus true for all $n \in \mathbb{N}$.

10.6. Let $c = v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n$ be a chain of minimal length connecting v_0 and v_n with $v_0 \neq v_n$. If this chain were not elementary, there would exist $i < j$ such that $v_i = v_j$. Consider the sequence c' defined by

$$c' = \begin{cases} v_j, e_{j+1}, v_{j+1}, \ldots, v_{n-1}, e_n, v_n & \text{if } v_i = v_0, \\ v_0, e_1, v_1, \ldots, v_{i-1}, e_i, v_i & \text{if } v_j = v_n, \\ v_0, e_1, v_1, \ldots, v_i, e_{j+1}, v_{j+1}, \ldots, v_{n-1}, e_n, v_n & \text{if } v_0 \neq v_i = v_j \neq v_n. \end{cases}$$

This sequence is indeed a chain connecting v_0 and v_n and it has a length strictly less than c, a contradiction.

The same result can be obtained, with the same proof, for paths in directed graphs.

10.7. If $v = v''$, then $d(v, v'') = 0$, and the inequality is verified. If $v = v'$ or if $v' = v''$, the result is straightforward. Consider now the case when $v \neq v'', v \neq v'$, and $v' \neq v''$.

If $d(v, v') = \infty$ or if $d(v', v'') = \infty$, the result is clear. Otherwise, there exists a chain of length $d(v, v')$ connecting v to v' and a chain of length $d(v', v'')$ connecting v' to v''. Concatenating these two chains yields a chain of length $d(v, v') + d(v', v'')$ connecting v to v''. The shortest chain connecting v to v'' thus has length less than or equal to $d(v, v') + d(v', v'')$.

10.8. 1. The number of vertices is the number of ways of choosing two elements among five. It is $\binom{5}{2} = \dfrac{5!}{2!3!} = 10$. Each vertex $v = \{n, m\}$ is connected to three others by an edge ; these three other vertices are those obtained by choosing two elements in $\{0, 1, 2, 3, 4\} \setminus \{n, m\}$. The number of edges is equal to the half-sum of the degrees, i.e. $\frac{1}{2}(10 \times 3) = 15$. Lastly, let $\{n, m\}$ and $\{p, q\}$ be two distinct vertices ; if $\{n, m\} \cap \{p, q\} = \emptyset$, these two vertices are at distance 1 ; otherwise their intersection is reduced to a single element and we may write $\{a, b\}$ and $\{b, c\}$. Let d and e be the two remaining elements. $\{d, e\}$ is disjoint from $\{a, b\}$ and from $\{b, c\}$ and is thus at distance 1 from each one of them. The diameter of the graph is thus 2.

2. To increase the readability we have labelled only a subset of the graph (figure 15.4).

Figure 15.4

10.9. 1. The result is true for $k = 1$ by the definition of M. Assume that the $m_{ij}^{(k)}$ entry of M^k is the number of paths of length k from v_i to v_j. Let C_{ij}^k be the set of paths of length k from v_i to v_j, and let P_{ilj}^{k+1} be the subset of C_{ij}^{k+1} consisting of the paths whose last edge has origin v_l. It is easy to see that $C_{ij}^{k+1} = \bigcup_{l=1}^n P_{ilj}^{k+1}$, and since the sets P_{ilj}^{k+1} are disjoint, $|C_{ij}^{k+1}| = \sum_{l=1}^n |P_{ilj}^{k+1}|$. Moreover, every path of P_{ilj}^{k+1} is obtained by extending a path of C_{il}^k by one edge with origin v_l and target v_j. Hence, $|P_{ilj}^{k+1}| = |C_{il}^k| \times m_{lj}$. Since by the induction hypothesis $|C_{il}^k| = m_{il}^{(k)}$ holds, we have

$$|C_{ij}^{k+1}| = \sum_{l=1}^{n} m_{il}^{(k)} \times m_{lj},$$

i.e. $|C_{ij}^{k+1}| = m_{ij}^{(k+1)}$.

2. Yes. We associate with (V, E, δ) having the n vertices $v_1, \ldots, v_n$ the matrix M defined in the following way. Each entry $M_{i,j} = m_{ij}$ of M (for $1 \leq i \leq n$ and $1 \leq j \leq n$) is the number of edges e of E such that $\delta(e) = \{v_i, v_j\}$. We note that the matrix M is symmetrical, i.e. $m_{ij} = m_{ji}$, and we reason by induction as in case 1.

10.10. 1. The set of the edges of G_4 is the union of a set H of ‘horizontal’ edges and of a set V of ‘vertical’ edges. With each pair $\{(x, y), (x+1, y)\}$ of elements of $\mathbb{Z}^2$ is associated a horizontal edge connecting them. Similarly, a vertical edge connects all pairs of elements $\{(x, y), (x, y+1)\}$.

If c is any chain connecting (x, y) and (x', y'), it is easy to see that $|x - x'|$ is less than or equal to the number of horizontal edges of c and that $|y - y'|$ is less than or equal to the number of vertical edges of c. Hence, $|x - x'| + |y - y'| \leq d_{G_4}\big((x, y), (x', y')\big)$.

It is also easy to see that there exists a ‘horizontal’ chain of length $|x - x'|$ connecting (x, y) and (x', y), and a ‘vertical’ chain of length $|y - y'|$ connecting (x', y) and (x', y'). There thus exists a chain of length $|x - x'| + |y - y'|$ connecting (x, y) and (x', y'). Hence, $d_{G_4}\big((x, y), (x', y')\big) \leq |x - x'| + |y - y'|$.

2. In order to obtain G_8, we add to G_4 the ‘oblique’ edges connecting (x, y) and $(x+1, y+1)$ and those connecting (x, y) and $(x+1, y-1)$. If c is any chain of length n connecting (x, y) and (x', y'), we easily show that $|x - x'| \leq n$ and $|y - y'| \leq n$, and hence $\max\big(|x - x'|, |y - y'|\big) \leq d_{G_8}\big((x, y), (x', y')\big)$.

Let (x, y) and (x', y') be two elements of $\mathbb{Z}^2$. We assume that $|x - x'| \leq |y - y'|$ and let $n = |x - x'|$. The proof would be similar if $|y - y'| \leq |x - x'|$. Through oblique chains of length

n we may connect (x,y) to $(x+n, y+n)$, to $(x-n, y-n)$, to $(x+n, y-n)$ and to $(x-n, y+n)$. We now assume that $x \leq x'$, i.e. $x' = x+n$. The symmetrical case could be dealt with similarly. Then we may connect (x', y') to $(x', y+n)$ by a vertical chain of length $|y' - y - n|$ and to $(x', y-n)$ by a vertical chain of length $|y' - y + n|$. Because the least of the two numbers $|y' - y + n|$ and $|y' - y - n|$ is $|y - y'| - n$ we may connect (x,y) to (x', y') by a chain of length $n + |y - y'| - n = \max\bigl(|x - x'|, |y - y'|\bigr)$. Hence, $\max\bigl(|x - x'|, |y - y'|\bigr) \geq d_{G_8}\bigl((x,y),(x',y')\bigr)$ (figure 15.5).

Figure 15.5

10.11. 1. Each vertex v_i is indeed the endpoint of two edges, which are

$$\begin{cases} \{e_i, e_{i+1}\} & \text{if } i < n, \\ \{e_1, e_n\} & \text{if } i = n. \end{cases}$$

2. By induction on n. Recall that the sum of the degrees of an undirected graph is equal to twice its number of edges. If each one of the n vertices of a graph is of degree 2, this graph thus has n edges.

- If $n = 1$, G has a single edge e and a single vertex v with $\delta(e) = \{v\}$. G is thus isomorphic to C_1.
- If $n = 2$, G has two vertices v and v' and two edges e and e'. Since G is connected, v is connected to v' by one of the two edges. Assume that it is edge e. We then have $\delta(e) = \{v, v'\}$. If $\delta(e') = \{v\}$ then v is of degree 3 ; if $\delta(e') = \{v'\}$ then v' is of degree 3. We thus have $\delta(e') = \{v, v'\}$, and G is isomorphic to C_2.
- Assume that G has $n+1$ vertices, with $n \geq 2$. Let v be a vertex of G and e' an edge with endpoint v.
  - If $\delta(e') = \{v\}$, then since v is of degree 2, v is neither the origin nor the target of any other edge, and $\{v\}$ is a connected component of G, which is excluded.
  - If $\delta(e') = \{v, v'\}$ with $v \neq v'$, there thus exists another edge e'' with endpoint v'. Hence $\delta(e'') = \{v''\}$ cannot hold for the same reasons as previously. Thus $\delta(e'') = \{v, v''\}$, with $v \neq v''$.
  - Thus $\delta(e') = \{v, v'\}$ with $v \neq v'$, and $\delta(e'') = \{v, v''\}$, with $v \neq v''$. If $v' = v''$, then v' can be neither the origin nor the target of any edge other than e' and e''. The set $\{v, v'\}$ is a connected component of G which is not equal to the whole of G because G has strictly more than two vertices, and this is excluded.
  - The remaining case is that $\delta(e') = \{v, v'\}$ and $\delta(e'') = \{v, v''\}$, with $v \neq v'$, $v \neq v''$ and $v' \neq v''$. Consider the graph G' obtained from G by deleting vertex v and edges e' and e'' and by adding an edge e with $\delta(e) = \{v', v''\}$. It is a graph with n vertices each of which is of degree 2. By the induction hypothesis, G' is isomorphic to C_n. We then easily see that G is obtained from G' by inserting v between v' and v'', and thus that G is isomorphic to C_{n+1}.

3. Let G be a graph and let $V_1, V_2, \ldots, V_k$ be its connected components. Let G_i be the subgraph of G whose set of vertices is V_i. Then G is the disjoint union of the G_is. Moreover, each G_i is a connected graph all of whose vertices have degree 2 ; it is thus isomorphic to some C_{n_i}.

10.12. The chromatic number of the complete graph K_4 with four vertices, and where all distinct pairs of vertices are connected by an edge, is 4.

This graph is indeed planar. Assume that it can be coloured with strictly less than four colours. There would then be two distinct vertices of the same colour, which is impossible since these two vertices are connected by an edge.

10.13. If one of the two connected components were not a tree, it would necessarily contain a simple cycle which would also be in the initial graph. This is impossible because the initial graph is a tree.

10.14. Let s be the sum of the degrees of the n vertices of G. Because G is a tree, it has $n-1$ edges and $s = 2(n-1)$. Let k be the number of vertices of degree 2 and let k' be the number of vertices of degree greater than or equal to 3. Then $n = k + k' + 2$ and $s \geq 2 + 2k + 3k'$. As $k' = n - 2 - k$ and $s = 2n - 2$, we have $2n - 2 \geq 2 + 2k + 3n - 6 - 3k$, i.e. $k \geq n - 2$. As $k \leq n - 2$, we have $k = n - 2$.

Because G is connected, there exists an elementary chain connecting the two vertices of degree 1 (see Exercise 10.6). Assume that this chain does not contain all the vertices of the graph. Since the vertices in this chain are of degree 2 and since they already belong to two edges and since the endpoints belong to one edge, no vertex of this chain can be connected by an edge to a vertex which is not in the chain. In this case the graph would not be connected, which is excluded.

10.15. Let $V = \{v_1, \ldots, v_n\}$ be the set of vertices of tree G. We show by induction on the number n of vertices the following more precise result : $\forall v_i \in V$, $\forall \alpha > 0$, $\forall R > 0$; we may always draw G on a circular segment with angle α and radius R in such a way that the edges consist of linear segments without cross-sections except at the endpoints, and that vertex v_i is the origin of the circular segment.

- If $n \leq 2$ the result is clear, because for $n = 1$, G is reduced to a point, and for $n = 2$, G is reduced to a single edge. (In fact it suffices to consider the case in which $n = 1$ as the basis case.)

- If $n > 2$, let e be an edge such that $\delta(e) = \{v_i, v_j\}$. Delete e from tree G. We obtain two trees G_1 and G_2 such that G_i has $n_i < n$ vertices for $i = 1, 2$, $v_i \in G_1$ and $v_j \in G_2$. By the induction hypothesis, we may thus draw G_1 (resp. G_2) in a circular segment with origin v_i (resp. v_j), angle $\alpha/2$, and radius $R/2$ in such a way that the edges consist of linear segments without cross-sections except at the endpoints. It then suffices to first draw G_1 and to then draw the edge e connecting v_i and v_j in such a way that it forms an $\alpha/2$ angle with the picture of G_1 and that it has a length of $R/2$, and to finally draw G_2 starting from v_j (figure 15.6).

Figure 15.6

Planarity is an immediate consequence.

10.16. Let Pref(L) be the set $\{u \in A^* \,/\, \exists v \in A^* : uv \in L\}$ (see Exercise 11.10). We construct a directed graph G whose vertices are the strings of Pref(L) and whose edges connect all the pairs (u, ua) with $a \in A$ and both u and $ua \in$ Pref(L).

The outdegree of each vertex of this graph is indeed finite since it is always less than or equal to the number of elements of A.

By the definition of Pref(L), any string $a_0 \cdots a_n$ of L is the target of the path $\varepsilon, a_0, a_0a_1, \ldots, a_0a_1 \cdots a_n$ with origin ε. Since L is infinite, ε is the origin of infinitely many paths of G.

Applying Proposition 10.25, we deduce the existence in G of an infinite path $\varepsilon, a_0, a_0a_1, \ldots, a_0a_1 \cdots a_n, \ldots$ with origin ε. Because each string $a_0a_1 \cdots a_n$ is in Pref(L), the infinite string $a_0a_1 \cdots a_n \cdots$ does indeed have the required property.

10.17. Let F_n be the set of the injections $f_n : \{0, 1, \ldots, n\} \to \mathbb{N}$ such that $\forall i \in \{0, 1, \ldots, n\}$, $(i, f_n(i)) \in S$. By (i), F_n is non-empty, and it is clear that if $n \neq m$ then $F_n \cap F_m = \emptyset$.

On the other hand, each F_n is finite. If k_n is the cardinality of the finite set $\{m \in \mathbb{N} \,/\, (n, m) \in V\}$, we easily show by induction on n that the number of elements of F_n is less than or equal to $k_0 \times k_1 \times \cdots \times k_n$.

We define the relation R on $\cup_{n \geq 0} F_n$ by $f \; R \; g$ if and only if there is an $n \geq 0$ such that $f \in F_n$, $g \in F_{n+1}$, and $\forall i \in \{0, 1, \ldots, n\}$, $f(i) = g(i)$.

If g is in F_{n+1}, its restriction g' to $\{0, 1, \ldots .n\}$ is indeed such that $g' \; R \; g$. Proposition 10.26 can thus be applied : there exists a sequence of injections $f_0, f_1, \ldots, f_n, \ldots$ such that $f_n \in F_n$ and $f_n \; R \; f_{n+1}$.

We then define $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = f_n(n)$. Thus $(n, f(n)) = (n, f_n(n)) \in V$. Finally, f is an injection. Indeed, we easily show by induction on m that $\forall n, m \in \mathbb{N}, \forall i \leq n$, $f_n(i) = f_{n+m}(i)$. If there were $n < m$ such that $f(n) = f(m)$, then $f_m(n) = f_n(n) = f(n) = f(m) = f_m(m)$ and thus f_m would not be injective, a contradiction.

10.18. Both questions can be proved by induction on the number of vertices of the tree.

1. If the complete binary tree G has only one vertex, it has indeed an odd number of vertices. If it has $n+1$ vertices, its root r must necessarily have two children v and v'. Graphs $G(v)$ and $G(v')$ are again complete binary trees having, respectively, p and p' vertices, with $p+p'=n$. We thus have $1 \leq p \leq n-1$ and $1 \leq p' \leq n-1$. By the induction hypothesis, p and p' are odd numbers. Hence $n = p+p'$ is even and $n+1$ is odd.

2. If a complete binary tree has a single vertex, it has a single leaf, and the property is true. For a tree with $2n-1$ vertices, we proceed as previously : $G(v)$ is a tree with $2p-1$ vertices and p leaves, $G(v')$ is a tree with $2p'-1$ vertices and p' leaves and G is a tree with $2p-1+2p'-1+1 = 2(p+p')-1$ vertices and with $p+p'$ leaves.

Chapter 11

11.1. 1. YES. The composition of mappings is indeed associative and has a unit that is the identity mapping.

2. NO. The 'power' operation is not associative : $(2^1)^2 = 2^2 = 4$, $2^{(1^2)} = 2^1 = 2$.

3. YES. The empty string is an even length string, and the (associative) product of two even length strings is again an even length string.

4. YES. Let $|u|_a$ and $|u|_b$ be the number of occurrences of a and b in u. Indeed $|\varepsilon|_a = |\varepsilon|_b = 0$; if $|u|_a = |u|_b$ and $|v|_a = |v|_b$, then $|uv|_a = |u|_a + |v|_a = |u|_b + |v|_b = |uv|_b$.

5. YES. Union is associative and its unit is the empty set.

6. YES and NO. The intersection of the subsets of a set E is an associative operation. Its unit is is E ; indeed, if Z is this unit, $\forall e \in E, \{e\} \cap Z = \{e\}$ should hold (i.e. $\forall e \in E, e \in Z$). Since the unit must be a finite subset, we have a monoid if and only if E is finite.

11.2. 1. The matrices I, A and B have determinant $+1$, and a product of matrices with determinant $+1$ is again a matrix with determinant $+1$. If $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ is a matrix with non-negative integral coefficients, then $MA = \begin{pmatrix} x & x+y \\ z & z+w \end{pmatrix}$ and $MB = \begin{pmatrix} x+y & y \\ z+w & w \end{pmatrix}$ are matrices with non-negative integral coefficients.

2. Let $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Its determinant Δ is equal to $xw - yz$. Let $y = x+p$ and $w = z+q$, with $p, q \in \mathbb{Z}$. Then $\Delta = x(z+q) - (x+p)z = xq - pz$. If $\Delta = 1$, we have $xq = 1 + pz$. If $y \geq x$, then $p \geq 0$ and, since x and z are non-negative, $q > 0$ and thus $w > z$. If $w \leq z$, then $q \leq 0$, and hence $p < 0$ and $y < x$.

3. It is easy to see that

$$A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \text{ and } B^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Let $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. If the first column is greater that the second column, the matrix $MB^{-1} = \begin{pmatrix} x-y & y \\ z-w & w \end{pmatrix}$ has determinant $+1$ and non-negative integral coefficients. The sum of its coefficients is $x+z$, strictly less than $x+y+z+w$. (If $y+w=0$, M has determinant zero.) $M' = MB^{-1}$ is thus an element of $\mathcal{M}_1$, and so is $M = M'B$. The uniqueness of the decomposition of M in a product of matrices A and B follows from the fact that M cannot be written as $M''A$, with $M'' \in \mathcal{M}_1$, because $M'' = MA^{-1} = \begin{pmatrix} x & y-x \\ z & w-z \end{pmatrix}$ with $y - x \leq 0$ and $w - z \leq 0$, and if $M'' \in \mathcal{M}_1$ we have $y-x=0$ and $w-z=0$, which is impossible if the determinant of M'' is 1.

If the second column of M is greater than the first column, the argument is similar modulo the interchange of A and B.

4. The equality of $\mathcal{M}_1$ and $\mathcal{M}_2$ easily follows from the above.

11.3. Let $h(a) = A$ and $h(b) = B$. This homomorphism is surjective by the definition of $\mathcal{M}_1$. It is injective because the decomposition of any matrix M of $\mathcal{M}_1 = \mathcal{M}_2$ into a product of matrices A and B is unique.

11.4. 1. It is necessary and sufficient that $\forall x \in A$, $h(x)$ is a length 2 string.

2. It is necessary and sufficient that $\forall x \in A$, $h(x)$ is a string containing no bs.

3. Let, for instance, the two homomorphisms

$$h\colon (A \setminus \{a\})^* \longrightarrow (A \setminus \{b\})^* \text{ and } g\colon (A \setminus \{b\})^* \longrightarrow (A \setminus \{a\})^*$$

be defined as follows :

$$\begin{aligned} &h(b) = a\ , \\ &h(x) = x, \quad \forall x \notin \{a, b\}\ , \\ &g(a) = b\ , \\ &g(x) = x, \quad \forall x \notin \{a, b\}\ . \end{aligned}$$

Then $gh\colon (A \setminus \{a\})^* \longrightarrow (A \setminus \{a\})^*$ is the identity, and h is thus an isomorphism.

11.5. It is clear that if one of the following three cases holds then $uv = xy$. See Figure 15.7.

(i) If $u = x$ and $v = y$ then $uv = xy$.

(ii) If $ut = x$ and $v = ty$ then $uv = uty = xy$.

(iii) If $u = xt$ and $tv = y$ then $uv = xtv = xy$.

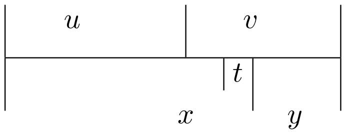

Figure 15.7

The converse is proved by complete induction on $n = |u| + |x|$:

- If $n = 0$ then $|u| = |x| = 0$. Hence $u = x = \varepsilon$, and thus $u = y$.
- Assume that $|u| + |x| = n + 1$.
  - If $|u| = 0$ then case (ii) holds and we let $t = x$.
  - If $|x| = 0$ then case (iii) holds and we let $t = u$.
  - If both $|u|$ and $|x|$ are strictly positive, and $uv = xy$, we have $u = au'$, $x = ax'$, and $u'v = x'y$. Since $|u'| + |x'| = n - 1$, we can apply the induction hypothesis :

    (i) If $|u| = |x|$, then $|u'| = |x'|$. Hence $u' = x'$, $v = y$, and thus $u = x$.

    (ii) If $|u| < |x|$, then $|u'| < |x'|$. Hence $u't = x'$ and $v = ty$, and also $ut = au't = ax' = x$.

    (iii) If $|u| > |x|$, then $|u'| > |x'|$. Hence $u' = x't$ and $tv = t$, and also $u = au' = ax't = xt$.

11.6. 1. If $u = w^m$ and $v = w^n$, it is clear that $uv = vu$. To show the converse, we reason by complete induction on the length of uv.

- If $|uv| = 0$, then $u = v = \varepsilon$, and we let $w = \varepsilon, m = n = 1$.
- If $|u| = 0$, then $u = \varepsilon$, and we let $w = v, m = 1$, and $n = 0$. (Recall that $w^0 = \varepsilon$.)
- If $|v| = 0$, then $v = \varepsilon$, and we let $w = u$, $m = 0$, and $n = 1$.
- If $|uv| = n+1$ (with $|u|$ and $|v|$ strictly positive) then, by Levi's lemma, one of the following three cases holds.

– If $|u| = |v|$, then $u = v$; we then let $w = u = v$, and $p = q = 1$.

– If $|u| < |v|$, then $ut = v$ and $v = tu$, and hence $ut = tu$. As $|u| > 0$, $|u| + |t| = |v| < |u| + |v|$, and we can apply the induction hypothesis : $u = w^m$ and $t = w^n$, and thus $v = ut = w^{m+n}$.

– If $|u| > |v|$, then $u = tv$ and $tv = u$, and hence $vt = tv$. For the same reasons as the above, we can apply the induction hypothesis : $t = w^m$ and $v = w^n$, and thus $u = vt = w^{m+n}$.

2. Here again the necessary condition is straightforward. Thus, assume $u^p = v^q$.

- If $|u| = |v|$, we let $w = u = v$ and $m = n = 1$.
- If $|u| \neq |v|$, we can assume $|u| < |v|$ because the equation is symmetrical in u and v. Let k and r be integers such that $|v| = k|u| + r$, with $r < |u|$. We easily deduce that $v = u^k t$ and $u = tt'$ (with $|t| = r$, and thus $|t'| \neq 0$), and thus that $(tt')^p = ((tt')^k t)^q$. Deleting the $(tt')^k$ prefix common to both strings, we have $(tt')^{p-k} = t((tt')^k t)^{q-1}$. Noting also that $(|t| + |t'|)(p - k) = |t| + (q - 1)(|t| + k(|t| + |t'|))$, we have that $q - 1 > 0$, because otherwise $(|t| + |t'|)(p - k) = |t|$, which is impossible since both $|t|$ and $|t'|$ are non-zero. The string $t((tt')^k t)^{q-1}$ thus starts with ttt', and the string $(tt')^{p-k}$, which is equal, starts with $tt't$. Because these two prefixes have the same length, they are equal and thus $tt' = t't$. We can then apply the preceding result : $t = w^m$ and $t' = w^n$, and hence $u = w^{m+n}$ and $v = w^{k(m+n)+m}$.

3. By studying the conditions that the length of w satisfies, we find that $2|u| = |u|$, namely, $|u| = 0$ and thus $u = \varepsilon$.

4. Applying 1, we have $u = w^m$ and $a = w^n$. We must thus have $1 = |a| = n|w|$; hence $n = |w| = 1$, and thus $w = a$.

5. Since the condition $0 \neq 0$ is always false, this boils down to the condition that $ua = bu$ never holds (with $a \neq b$). Let n (resp. p, q) be the number of occurrences of a in u (resp. ua, bu). We have that $p = n + 1$ and $q = n$, and if ua were equal to bu, we would have that $p = q$, which would be impossible.

11.7. 1. The product of languages is associative :

$$(L \cdot L') \cdot L'' = L \cdot (L' \cdot L'') = \{uu'u'' \,/\, u \in L, u' \in L', u'' \in L''\}.$$

The language $\{\varepsilon\}$ is indeed the unit because

$$L \cdot \{\varepsilon\} = \{uv \,/\, u \in L, v \in \{\varepsilon\}\} = \{u\varepsilon \,/\, u \in L\} = L.$$

For the same reasons, $L = \{\varepsilon\} \cdot L$.

2. $u \in (\bigcup_{i\in I} L_i) \cdot L$ if and only if $\big(\exists v \in \bigcup_{i\in I} L_i, \exists w \in L\colon u = vw\big)$ if and only if $\big(\exists i \in I, \exists u \in L_i, \exists w \in L\colon u = vw\big)$ if and only if $\exists i \in I\colon u \in L_i \cdot L$.

3. It is easy to prove by induction that $(L + \{\varepsilon\})^n = \bigcup_{i=0}^n L^i$. It holds for $n = 0$. Applying the induction hypothesis, we have $(L + \{\varepsilon\})^{n+1} = (\bigcup_{i=0}^n L^i) \cdot (L \cup \{\varepsilon\})$, which is equal to $\bigcup_{i=0}^{n+1} L^i$ by the result of the preceding question and the fact that $\{\varepsilon\}$ is the unit of the product.

4. $\emptyset^* = \{\varepsilon\} + \emptyset \cdot L^* = \{\varepsilon\}$.

11.8. 1. X^* is the set of strings (including the empty string) consisting only of bs.

Y is the set of non-empty strings whose first letter is not a b and whose other letters are all bs. Indeed, $u \in Y$ if and only if $u = vw$ with $u \in A \setminus \{b\}$ and $v \in \{b\}^*$.

Y^* is the set consisting of the empty string and of all the non-empty strings which do not start with b.

2. Let u be a string of A^* whose first letter is not a b. It can thus be written

$$x_1 b^{p_1} x_2 b^{p_2} \cdots b^{p_{n-1}} x_n b^{p_n},$$

with $x_i \in A \setminus \{b\}$. Each of the strings $x_i b^{p_i}$ is in Y, and thus $u \in Y^*$.

3. Let u be a string in A^*. If it contains at least one letter different from b, it can be written $b^p xu'$. By 1, $b^p \in X^*$, and by 2, $xu' \in Y^*$. If u contains only bs, then it is in X^*, and as $\varepsilon \in Y^*$, we have that $u \in X^* \cdot Y^*$. This decomposition is unique : because u contains only bs, the only string of Y^* that can occur in u is the empty string.

11.9. The only paths with trace ε are the empty paths, which are in the set of paths whose source and target are equal.

11.10. Let $\mathcal{A} = (S, T, I, F)$ be a finite-state automaton recognizing L. We will obtain a finite-state automaton $\mathcal{A}' = (S, T, I, F')$ recognizing $\mathrm{Pref}\,(L)$ by including in F' any state s of $\mathcal{A}$ such that there exists a path c whose source is a state of I and whose target is s, and a path c' whose source is s and whose target is a state of F.

11.11. Let L be a finite non-empty language. Let $P(L)$ be the set $\{u \in A^* \,/\, \exists v \in A^*\colon uv \in L\}$. This set is finite because any string of L has but a finite number of prefixes, and it is non-empty because it contains L and the empty string ε. Define the finite-state automaton $\mathcal{A} = (S, T, \{i\}, F)$ as follows :

- $S = P(L)$,
- $T = \{(u, a, ua) \,/\, u, ua \in P(L)\}$,
- $i = \varepsilon$,
- $F = L$.

It is clear that this automaton is deterministic. It is also easy to see that there exists a path with source ε and with trace u if and only if $u \in P(L)$, and then the target state of this path is u. We thus have $L(\mathcal{A}) = L$.

If L is the empty language, then it is recognized by the empty automaton, which is a deterministic finite-state automaton.

11.12. If there exists a circuit going through a state which is on a path going from an initial state to a final state, then there exist three paths : c' going from an initial state s_i to a state s, c, non-empty, going from s to s, and c'' going from s to a final state s_f. Let u, v and w be the traces of these three paths. Since for any $n \geq 0$, $c_1 c^n c_2$ is a path with trace $uv^n w$ in the automaton, and since v is not the empty string, the language recognized by the automaton contains infinitely many strings.

Conversely, if there is no circuit going through a state which is on a path going from an initial state to a final state, then no path from an initial state to a final state can go twice through the same state. Such paths thus have, by the pigeonhole principle (see Proposition 1.8 and Exercise 1.16), a length strictly less than the number of states of the finite-state automaton.

If n is the number of states of the automaton, the recognized strings will have length strictly less than n. If k is the number of letters in the alphabet, the number of strings of length strictly less than n is $1 + k + k^2 + \cdots + k^{n-1}$, which is equal to

$$\begin{cases} n & \text{if } k = 1, \\ \dfrac{k^n - 1}{k - 1} & \text{if } k \geq 2. \end{cases}$$

This bound is the same for deterministic finite-state automata, and it is indeed reached, as the next example shows.

Let $S = \{0, 1, \ldots, n-1\}$, with initial state 0, final states $F = \{0, 1, \ldots, n-2\}$ and $T = \{(i-1, a, i) \,/\, 1 \leq i \leq n, a \in A\}$. It is easy to see that this automaton is deterministic and recognizes all the strings of length strictly less than n. Conversely, if a finite-state automaton with n states recognizes a number of strings equal to this bound, it must then recognize all the strings of length strictly less than n and it has the above-given form. Complete finite-state automata recognizing finite languages must have at least a non-final state. In this case the bound is

$$\begin{cases} n - 1 & \text{if } k = 1, \\ \dfrac{k^n - 2}{k - 1} & \text{if } k \geq 2. \end{cases}$$

The deterministic finite-state automaton reaching this bound is

$$S = \{0, 1, \ldots, n-1\}, \quad F = \{0, 1, \ldots, n-2\} \quad i = 0 \quad \text{and}$$

$$T = \{(i-1, a, i) \,/\, 1 \leq i \leq n-1, a \in A\} \cup \{(n-1, a, n-1) \,/\, a \in A\}.$$

11.13. 1. Because we add to $\mathcal{A}$ transitions (s, a, s) when there are no transitions (s, a, s') in $\mathcal{A}$, then we have that if $\mathcal{A}$ is deterministic, $\mathcal{A}'$ is also deterministic.

2. Any path of $\mathcal{A}$ is also a path of $\mathcal{A}'$, and hence $L(\mathcal{A}) \subseteq L(\mathcal{A}')$. This inclusion is strict. If $\mathcal{A}$ is the finite-state automaton over the alphabet $\{a, b\}$, whose only transition is (i, b, f), it recognizes the language $\{b\}$. Completing it as indicated, we add the transitions (i, a, i), (f, a, f) and (f, b, f), and the recognized language becomes $a^*b(a+b)^*$.

11.14.

$$\{i\}\xrightarrow{a}\emptyset,\quad \{i\}\xrightarrow{b}\{x,y\},\quad \{i\}\xrightarrow{c}\emptyset$$

$$\emptyset\xrightarrow{a}\emptyset,\quad \emptyset\xrightarrow{b}\emptyset,\quad \emptyset\xrightarrow{c}\emptyset$$

$$\{x,y\}\xrightarrow{a}\{f\},\quad \{x,y\}\xrightarrow{b}\{i,z\},\quad \{x,y\}\xrightarrow{c}\{f,z\}$$

$$\{f\}\xrightarrow{a}\emptyset,\quad \{f\}\xrightarrow{b}\emptyset,\quad \{f\}\xrightarrow{c}\emptyset$$

$$\{i,z\}\xrightarrow{a}\{f'\},\quad \{i,z\}\xrightarrow{b}\{x,y\},\quad \{i,z\}\xrightarrow{c}\{f'\}$$

$$\{f,z\}\xrightarrow{a}\{f'\},\quad \{f,z\}\xrightarrow{b}\emptyset,\quad \{f,z\}\xrightarrow{c}\{f'\}$$

$$\{f'\}\xrightarrow{a}\{z\},\quad \{f'\}\xrightarrow{b}\emptyset,\quad \{f'\}\xrightarrow{c}\{z\}$$

$$\{z\}\xrightarrow{a}\{f'\},\quad \{z\}\xrightarrow{b}\emptyset,\quad \{z\}\xrightarrow{c}\{f'\}$$

The initial state is $\{i\}$, and the final states are $\{f\}, \{f'\}$ and $\{f, z\}$.

11.15. Automata for questions 1, 2 and 8 are shown in figure 15.8.

Figure 15.8

11.16. 1. It is again an application of the pigeonhole principle (see Proposition 1.8 and Exercise 11.12).

2. If $z \in L_{q,q'}$ and $|z| \geq n$, there exists a path γ with trace z from q to q'. Because this path has a length greater than or equal to n, it must be true that the path consisting of its n first transitions contains a circuit and γ can thus be written $c'cc''$ with $|c'c| \leq n$, and c such that its source is equal to its target. We have the required result by taking u to be the trace of c', v to be the trace of c, and w to be the trace of c''.

3. This immediately follows from the preceding point, by using the fact that $z \in L(\mathcal{A})$ if and only if $\exists q \in I, q' \in F\colon z \in L_{q,q'}$.

11.17. We will reason by contradiction in all cases. We will assume that the given language is recognized by a finite-state automaton with k states, and, applying the iteration lemma, we will show that it must also contain strings other than the desired ones.

1. The string $a^k b^k$ can be written uvw with $|uv| \leq k$ and $v \neq \varepsilon$. We thus have $u = a^p, v = a^q$, and $w = a^r b^k$ with $q \neq 0$ and $p + q + r = k$. We deduce that the automaton also recognizes $a^{k+q}b^k$, which is not in the language.

2. The string a^{k^2} can be written as $a^p a^q a^r$ with $0 < q \leq k$. The string a^{k^2+q} is also recognized by the automaton, but $k^2 + q$ is not a square. (The least square strictly greater than k^2 is $(k+1)^2 = k^2 + 2k + 1$.)

3. Let m be a prime number greater than k. $p + q + r$ with $0 < q \leq k$ and a^{m+qm} is again recognized by the automaton even though $m + qm$ is obviously not a prime number.

4. Let $w = a^k b$. The string ww is thus decomposed as $a^p, a^q\ a^r bw$, with $q > 0$, and the string $a^{k+q}ba^k b$ is accepted by the automaton even though it is not of the form ww.

5. The string $a^k ba^k$ is a palindrome. For the same reasons as given above, the string $a^{k+q}ba^k$ will be accepted by the automaton even though it is not a palindrome.

11.18. Answers to questions 1 and 5 are given in figure 15.9 and to question 2 in figure 15.10.

Figure 15.9

2. The completion of the following finite-state automaton, where $F = \{1, 2, 4, 6\}$.

Figure 15.10

11.19. Let $A = \{a, b\}$.

Consider the complete non-deterministic finite-state automaton whose transitions are

$$(q, a, q), (q, b, q), (q', a, q') \text{ and } (q', b, q'),$$

where q is final, and where both q and q' are initial. This automaton recognizes A^*. The finite-state automaton $\mathcal{A}'$, whose final state is q', also recognizes A^*.

Consider the incomplete deterministic finite-state automaton whose transitions are (q, a, q'), and (q', b, q'), whose initial state is q, and whose only final state is q'. This automaton recognizes ab^* even though the automaton $\mathcal{A}'$, whose final state is q, recognizes $\{\varepsilon\}$, which is not the complement of ab^*.

11.20. Let $\{D_i \,/\, i \in I\}$ be an arbitrary set of mappings in $\mathcal{D}$ whose least upper bound is defined by $D(s, s') = \bigcup_{i \in I} D_i(s, s')$. Show that $\widehat{\mathcal{S}}(D)$ is the least upper bound of $\{\widehat{\mathcal{S}}(D_i) \,/\, i \in I\}$. To this end it is enough to verify that if $t = (s'', a, s')$, then $a \cdot \bigcup_{i \in I} D_i(s'', s') = \bigcup_{i \in I} a \cdot D_i(s'', s')$, and this is a straightforward consequence of Exercise 11.7 2.

11.21. $(0, a, 0), (0, b, 1), (1, a, 1), (1, b, 2), (2, a, 2), (2, b, 0)$ with initial state : 0, and with final state : 0.

$$\begin{aligned}
x_{0,0} &= ax_{0,0} + bx_{1,0} + \varepsilon \\
x_{0,1} &= ax_{0,1} + bx_{1,1} \\
x_{0,2} &= ax_{0,2} + bx_{1,2} \\
x_{1,0} &= ax_{1,0} + bx_{2,0} \\
x_{1,1} &= ax_{1,1} + bx_{2,1} + \varepsilon \\
x_{1,2} &= ax_{1,2} + bx_{2,2} \\
x_{2,0} &= ax_{2,0} + bx_{0,0} \\
x_{2,1} &= ax_{2,1} + bx_{0,1} \\
x_{2,2} &= ax_{2,2} + bx_{0,2} + \varepsilon
\end{aligned}$$

We deduce $x_{0,0} = a^*(bx_{1,0} + \varepsilon)$, $x_{1,0} = a^*bx_{2,0}$, $x_{2,0} = a^*bx_{0,0}$; hence

$$x_{0,0} = a^* + a^*ba^*ba^*bx_{0,0} \text{ and thus } x_{0,0} = (a^*ba^*ba^*b)^*a^*.$$

11.22. L is recognized by the finite-state automaton

$$(0, a, 1), (1, a, 2), (2, a, 3), (3, a, 3), (0, b, 0), (1, b, 0), (2, b, 0), (3, b, 3)$$

with initial state : 0, and with final states : 0,1,2. See figure 15.11.

Figure 15.11

The equation system associated with this automaton has sixteen equations. We will thus write only those equations that are useful for determining the language recognized by this automaton :

$$\begin{aligned}
x_{0,0} &= ax_{1,0} + bx_{0,0} + \varepsilon\\
x_{0,1} &= ax_{1,1} + bx_{0,1}\\
x_{0,2} &= ax_{1,2} + bx_{0,2}\\
x_{1,0} &= ax_{2,0} + bx_{0,0}\\
x_{1,1} &= ax_{2,1} + bx_{0,1} + \varepsilon\\
x_{1,2} &= ax_{2,2} + bx_{0,2}\\
x_{2,0} &= ax_{3,0} + bx_{0,0}\\
x_{2,1} &= ax_{3,1} + bx_{0,1}\\
x_{2,2} &= ax_{3,2} + bx_{0,2} + \varepsilon\\
x_{3,0} &= ax_{3,0} + bx_{3,0}\\
x_{3,1} &= ax_{3,1} + bx_{3,1}\\
x_{3,2} &= ax_{3,2} + bx_{3,2}
\end{aligned}$$

Consider the system consisting of the last three equations. Its least solution is $(\emptyset, \emptyset, \emptyset)$. This system can thus be simplified to

$$\begin{aligned}
x_{0,0} &= ax_{1,0} + bx_{0,0} + \varepsilon\\
x_{0,1} &= ax_{1,1} + bx_{0,1}\\
x_{0,2} &= ax_{1,2} + bx_{0,2}\\
x_{1,0} &= ax_{2,0} + bx_{0,0}\\
x_{1,1} &= ax_{2,1} + bx_{0,1} + \varepsilon\\
x_{1,2} &= ax_{2,2} + bx_{0,2}\\
x_{2,0} &= bx_{0,0}\\
x_{2,1} &= bx_{0,1}\\
x_{2,2} &= bx_{0,2} + \varepsilon
\end{aligned}$$

which can also be written

$$\begin{aligned}
x_{0,0} &= ax_{1,0} + bx_{0,0} + \varepsilon\\
x_{0,1} &= ax_{1,1} + bx_{0,1}\\
x_{0,2} &= ax_{1,2} + bx_{0,2}\\
x_{1,0} &= (ab + b)x_{0,0}\\
x_{1,1} &= (ab + b)x_{0,1} + \varepsilon\\
x_{1,2} &= a + (ab + b)x_{0,2}
\end{aligned}$$

or

$$\begin{aligned}
x_{0,0} &= (aab + ab + b)x_{0,0} + \varepsilon\\
x_{0,1} &= a + (aab + ab + b)x_{0,1}\\
x_{0,2} &= aa + (aab + ab + b)x_{0,2}
\end{aligned}$$

we have

$$\begin{aligned}
x_{0,0} &= (aab + ab + b)^*\\
x_{0,1} &= (aab + ab + b)^*a\\
x_{0,2} &= (aab + ab + b)^*aa
\end{aligned}$$

Chapter 12

12.1. (ii) is true by hypothesis; it is enough to verify (i) and (iii); for (i), $\forall A \in \mathcal{T}$, $0 \leq P(A) \leq \sum_{\omega\in\Omega} P(\omega) = P(\Omega) = 1$. For (iii), $\forall n$, $P(A_n) = \sum_{\omega\in A_n} P(\omega)$, and thus $\sum_{n\in\mathbb{N}} P(A_n) = \sum_{n\in\mathbb{N}} \big(\sum_{\omega\in A_n} P(\omega)\big) = \sum_{\omega\in(\cup_{n\in\mathbb{N}} A_n)} P(\omega) = P(\cup_{n\in\mathbb{N}} A_n)$.

12.2. Let a = 'A hits the target' and b = 'B hits the target'. We have : $P(a \cup b) = P(a) + P(b) - P(a\cap b)$, and we obtain, assuming that a and b are independent (i.e. assuming that a and b are such that $P(a\cap b) = P(a)P(b)$) : $P(a\cup b) = P(a) + P(b) - P(a)P(b) = \dfrac{11}{20}$.

12.3. Let $X_n \in \{B, R\} = \Omega$ be the colour of the ball obtained at the nth drawing. We have

$$\begin{aligned}
P(X_1 = R) &= \frac{r}{b+r}\\
P(X_2 = R\,/\,X_1 = R) &= \frac{r-1}{b+r-1+c}\\
&\vdots\\
P(X_{n+1} = R\,/\,X_n = R, \ldots, X_2 = R, X_1 = R) &= \frac{r-n}{b+r-n+nc}\\
&\vdots
\end{aligned}$$

By Proposition 12.19 we deduce that

$$P(X_1 = X_2 = \cdots = X_k = R) = \frac{r(r-1)\cdots(r-k+1)}{(b+r)(b+r+c-1)\cdots(b+r+(k-1)c-(k-1))}\ .$$

12.4. Let $p_n = P(X_n = \text{'yes'}\ )$. We have

$$\begin{aligned}
p_1 &= 1, \qquad \text{and, for } n \geq 2,\\
p_n &= P(X_{n-1} = \text{'yes' and } X_n = \text{'yes'}\ ) + P(X_{n-1} = \text{'no' and } X_n = \text{'yes'}\ )\\
&= P(X_n = \text{'yes'}\ /\,X_{n-1} = \text{'yes'}\ )P(X_{n-1} = \text{'yes'}\ )\\
&\qquad + P(X_n = \text{'no'}\,/\,X_{n-1} = \text{'yes'}\ )P(X_{n-1} = \text{'no'})\\
&= pp_{n-1} + q(1-p_{n-1})\\
&= q + (p-q)p_{n-1}\ .
\end{aligned}$$

The recurrence equation $p_n = q + (p-q)p_{n-1}$ has the characteristic polynomial : $(r-(p-q))(r-1) = 0$. Assuming $p \neq 1$, we thus have a general solution $p_n = \lambda + \mu(p-q)^n$; $p_1 = 1$ and $p_2 = p$ give us

$$p_n = \frac{1}{2}\big(1 + (p-q)^{n-1}\big)\ .$$

If $p = 1$, then straightforwardly $p_n = 1$.

12.5. For all $n \in \mathbb{N}$, let B_n be the event $X^n = B$, and R_n be the event $X^n = R$.

(B) We indeed have : $P(B_1) = b/(b+r)$ and $P(R_1) = r/(b+r)$.

(I) Assume by induction that, **regardless of the initial values** of b, r, c, $P(B_n) = b/(b+r)$, and prove that $P(B_{n+1}) = b/(b+r)$. We have $P(B_{n+1}) = P(B_{n+1}\cap B_1) + P(B_{n+1}\cap R_1) = P(B_{n+1}/B_1)P(B_1) + P(B_{n+1}/R_1)P(R_1)$. By the induction hypothesis applied to the sequence $(X^n)_{n\geq 2}$, we have :

- $P(B_{n+1}/B_1) = (b+c)/(b+r+c)$, because in this case the sequence $(X^n)_{n\geq 2}$ corresponds to a Polya urn model with initial values $b+c, r, c$, and
- $P(B_{n+1}/R_1) = b/(b+r+c)$, because in this case the sequence $(X^n)_{n\geq 2}$ corresponds to a Polya urn model with initial values $b, r+c, c$.

Thus

$$P(B_{n+1}) \;=\; \frac{b+c}{b+r+c}\times\frac{b}{b+r} + \frac{b}{b+r+c}\times\frac{r}{b+r} \;=\; \frac{b}{b+r}\,.$$

12.6. Assuming both possible choices of the urn are equally probable,

$$\frac{r_1(b_2+r_2)}{r_1(b_2+r_2)+r_2(b_1+r_1)}\,.$$

Indeed, letting the events : V_i ='urn U_i was chosen', for $i = 1,\ 2$, R ='a red ball was drawn' : (V_1, V_2) is a partition, thus by Theorem 12.22

$$P(V_1/R) = \frac{P(V_1)P(R/V_1)}{P(V_1)P(R/V_1)+P(V_2)P(R/V_2)}\,.$$

$P(R/V_i) = \dfrac{r_i}{b_i+r_i}$, for $i = 1, 2$; moreover, both possible choices of the urn are equally probable, $P(V_1) = P(V_2) = 1/2$. Thus

$$\begin{aligned} P(V_1/R) &= \frac{P(V_1)P(R/V_1)}{P(V_1)P(R/V_1)+P(V_2)P(R/V_2)} \\ &= \frac{P(V_1)\dfrac{r_1}{b_1+r_1}}{P(V_1)\dfrac{r_1}{b_1+r_1}+P(V_2)\dfrac{r_2}{b_2+r_2}} \\ &= \frac{r_1(b_2+r_2)}{r_1(b_2+r_2)+r_2(b_1+r_1)}\,. \end{aligned}$$

12.7. This is a straightforward consequence of Theorem 12.22. Let the events : d ='the sample object is flawed', a ='the sample object comes from A', b ='the sample object comes from B'. Then,

$$P(a) = \frac{100}{100+200} = \frac{1}{3}, \quad P(b) = \frac{2}{3}, \quad P(d/a) = \frac{5}{100}, \quad P(d/b) = \frac{6}{100};$$

therefore

$$P(a/d) = \frac{P(a)P(d/a)}{P(b)P(d/b)+P(a)P(d/a)} = \frac{5}{17}\;.$$

12.8. Define the events

$i = \{$voter e is from area $i\}$,

$c = \{$voter e voted for candidate $C\}$.

1. $P(c) = \sum_{i=1}^{3} P(i\cap c) = \sum_{i=1}^{3} P(i)P(c/i) = 3/10\times 2/5 + 1/2\times 24/50 + 1/5\times 3/5 = 48\%$.

2. We have

$$\begin{aligned} P(3/c) &= \frac{P(3)P(c/3)}{\sum_{i=1}^{3} P(i)P(c/i)} \\ &= \frac{1/5\times 3/5}{3/10\times 2/5+1/2\times 24/50+1/5\times 3/5} = \frac{12}{12+24+12} = 1/4\,. \end{aligned}$$

12.9. We have $\Omega_2 = \{MM, MF, FM, FF\}$, with the uniform probability $P(\omega) = 1/4$, $\forall\omega\in\Omega_2$; $A = \{MM, MF, FM\}$ and $B = \{MF, FM\} = A\cap B$, hence $P(A\cap B) = 1/2$, but $P(B) = 1/2$ and $P(A) = 3/4$, thus $P(A\cap B)\neq P(A)P(B)$.

On the other hand, in the set of families with three children, we have

$$\Omega_3 = \{MMM, MMF, MFM, FMM, MFF, FMF, FFM, FFF\}$$

together with the uniform probability $P(\omega) = 1/8$, $\forall\omega\in\Omega_3$; hence $A = \{MMM, MMF, MFM, FMM\}$ and $B = \{MMF, MFM, FMM, MFF, FMF, FFM\}$, and thus $P(B) = 3/4$ and $P(A) = 1/2$, $P(A\cap B) = P(MMF, MFM, FMM) = 3/8 = P(A)P(B)$.

12.10. 1. $P(M) = 2/3$, $P(\overline{M}) = 1/3$;

$$P(D/M) = 0.7 \Longrightarrow P(\overline{D}/M) = 0.3 \qquad P(D/\overline{M}) = 0.2 \Longrightarrow P(\overline{D}/\overline{M}) = 0.8$$
$$P(F/M) = 0.2 \Longrightarrow P(\overline{F}/M) = 0.8 \qquad P(F/\overline{M}) = 0.9 \Longrightarrow P(\overline{F}/\overline{M}) = 0.1$$

2. We must compute $P(M/D \cap F)$. This conditional probability is equal to

$$P(M/D \cap F) = \frac{P(M \cap D \cap F)}{P(D \cap F)} = \frac{P(M \cap D \cap F)}{P(M \cap D \cap F) + P(\overline{M} \cap D \cap F)} \;.$$

But $P(M \cap D \cap F) = P(M)P(D \cap F/M)$. The fact that, given that a student likes maths, events D and F are independent is expressed by : $P(D \cap F/M) = P(D/M)P(F/M)$. Hence, $P(M \cap D \cap F) = P(M)P(D \cap F/M) = P(M)P(D/M)P(F/M)$. Similarly, substituting $\overline{M}$ for M, $P(\overline{M} \cap D \cap F) = P(\overline{M})P(D/\overline{M})P(F/\overline{M})$. Hence,

$$\begin{aligned} P(M/D \cap F) &= \frac{P(M)P(D/M)P(F/M)}{P(M)P(D/M)P(F/M) + P(\overline{M})P(D/\overline{M})P(F/\overline{M})} \\ &= \frac{2/3 \times 0.7 \times 0.2}{2/3 \times 0.7 \times 0.2 + 1/3 \times 0.2 \times 0.9} = 0.936 \,. \end{aligned}$$

Furthermore, the independence of the conditional events D and F on the hypothesis that a student likes maths implies

$$P(F/D \cap M) = P\big((F/M)/(D/M)\big) = P(F/M)$$

which is the equation corresponding to the independence of the conditional events D/M and F/M.

12.11. 1. Let Ω be the sample space constituted by the six permutations of the letters a, b, c, together with the three tuples (a, a, a), (b, b, b), (c, c, c), and the uniform probability ; each sample point thus has the probability 1/9. Let A_k be the event : 'letter a appears at the kth place, for $k = 1, 2, 3$'. $P(A_k) = 3/9 = 1/3$, for $k = 1, 2, 3$; moreover $P(A_1 \cap A_2) = P(A_1 \cap A_3) = P(A_3 \cap A_2) = 1/9$; the events A_1, A_2, A_3 are thus pairwise independent, but they are not independent because $P(A_1 \cap A_2 \cap A_3) = 1/9$; thus A_3 is not independent of $A_1 \cap A_2$.

2. Consider the experiment consisting of tossing two dice ; $\Omega = \{1, 2, \dots, 6\}^2$ with uniform probability. Let A_1 : 'the first die is a one', A_2 : 'the second die is even', A_3 : 'the total score of both dice is 7'. $P(A_1) = 1/6$, $P(A_2) = 1/2$, $P(A_3) = 1/6$, $P(A_1 \cap A_2) = 1/12$, $P(A_1 \cap A_3) = 1/36$, $P(A_3 \cap A_2) = 1/12$; the events A_1, A_2, A_3 are thus pairwise independent, but $P(A_1 \cap A_2 \cap A_3) = 1/36 \neq 1/6 \times 1/2 \times 1/6$.

12.12. 1. It is enough to verify that

$$\sum_{\omega=(i,j,k)\in\Omega} P(\omega) = 1 \;.$$

The event '$i + j + k$ is even' consists of the tuples $(0, 0, 0)$, $(0, 1, 1)$, $(1, 0, 1)$ and $(1, 1, 0)$; we are thus left with four tuples each having probability 1/4.

2.
$$\begin{aligned} A = \{i = 0\} &= \{(0, j, k) \,/\, (j, k) \in \{0, 1\}^2\} \\ &= \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1)\}; \end{aligned}$$

thus $P(A) = 1/2$. Similarly $P(B) = P(C) = 1/2$. Finally, it is easy to see that $P(A \cap B) = P(A \cap C) = P(B \cap C) = 1/4$; the three events $A = \{i = 0\}$, $B = \{j = 0\}$, $C = \{k = 0\}$ are thus pairwise independent.

3. No, because $A \cap B \cap C = (0, 0, 0)$ and thus $P(A \cap B \cap C) = 0 \neq P(A \cap B)P(C) = 1/4 \times 1/2 = 1/8$.

12.13. It is enough to prove that, $\forall \omega = (\omega_1, \ldots, \omega_n) \in \Omega$, $0 \leq P(\omega) \leq P(\Omega)$, which is straightforward, and that $\sum_{\omega \in \Omega} P(\omega) = 1$; but

$$\begin{aligned}\sum_{\omega\in\Omega} P(\omega) &= \sum_{\omega_1\in\Omega_1}\sum_{\omega_2\in\Omega_2}\cdots\sum_{\omega_n\in\Omega_n} P_1(\omega_1)\times P_2(\omega_2)\cdots\times P_n(\omega_n)\\ &= \sum_{\omega_2\in\Omega_2}\cdots\sum_{\omega_n\in\Omega_n} P_2(\omega_2)\times\cdots\times P_n(\omega_n)\Big(\sum_{\omega_1\in\Omega_1} P_1(\omega_1)\Big)\\ &= \sum_{\omega_2\in\Omega_2}\cdots\sum_{\omega_n\in\Omega_n} P_2(\omega_2)\times\cdots\times P_n(\omega_n) = \cdots\\ &= \sum_{\omega_n\in\Omega_n} P_n(\omega_n) = 1.\end{aligned}$$

12.14. We have $\Omega_k = \{1, 2, \ldots, k\}^n$, $\mathcal{T} = \mathcal{P}(\Omega_k)$ and for $\omega \in \Omega_k$ such that $|\omega_1| = i_1$, $\ldots$, $|\omega_k| = i_k$, $P(\omega) = p_1^{i_1} \cdots p_k^{i_k}$.

12.15. 1. Obvious since for $x \leq x'$, $F(x') = F(x) + \sum_{x \leq d < x'} P_X(d)$; since, moreover, $\sum_{x \leq d < x'} P_X(d) \geq 0$ (recall that probabilities are always non-negative), $F(x') \geq F(x)$.

2. We have : $\lim_{x\to\infty} F(x) = \lim_{x\to\infty} \sum_{d<x} P_X(d) = \sum_{d\in D} P_X(d) = P_X(D) = 1$. Suppose to simplify that X assumes values in $\mathbb{Z}$. Then, $\forall \varepsilon$, $\exists N$, $\sum_{d=-N}^{N-1} P_X(d) > 1 - \varepsilon$, and thus $F(-N) = \sum_{d<-N} P_X(d) < \varepsilon$, hence $\lim_{x\to-\infty} F(x) = 0$.

12.16. It suffices to check that $\sum_{(d,d')\in\{0,1\}^2} P_{(X,Y)}(d, d') = 4/4 = 1$, and similarly for Q, and that $\sum_{d\in\{0,1\}} P_X(d) = 1$. But, for $d \in \{0, 1\}$, $P_X(d) = \sum_{d'\in\{0,1\}} P_{(X,Y)}(d, d') = P_{(X,Y)}(d, 0) + P_{(X,Y)}(d, 1) = P(X = d, Y = 0) + P(X = d, Y = 1) = 1/2$. Thus $\sum_{d\in\{0,1\}} P_X(d) = 2/2 = 1$. Similarly for Q_X.

12.17. Yes, provided that $f(X)$ and $g(Y)$ be defined, and to this end it suffices that f (resp. g) be defined on the image of X (resp. Y). We indeed have

$$\begin{aligned}P\big(f(X) = i, g(Y) = j\big) &= \sum_{\substack{x\in f^{-1}(i)\\ y\in g^{-1}(j)}} P\big(X = x, Y = y\big)\\ &= \sum_{\substack{x\in f^{-1}(i)\\ y\in g^{-1}(j)}} P(X = x)P(Y = y)\\ &= P\big(g(X) = i\big)P\big(g(Y) = j\big)\,.\end{aligned}$$

12.18. 1. The distribution of W can be represented as follows :

x	1	2	3
$P_W(x)$	1/3	1/3	1/3

U can assume the values 2, 3, 4, 5, 6 ; in order to find $P(U = k)$, we look for the elementary events $(X = i) \cap (Y = j)$ satisfying $U = k$, i.e. such that $i + j = k$; for instance

$$\begin{aligned}P(U = 3) &= P\big((X = 1) \cap (Y = 2)\big) + P\big((X = 2) \cap (Y = 1)\big)\\ &\qquad\text{(since we have a subdivision into mutually exclusive events)}\\ &= P(X = 1)P(Y = 2) + P(X = 2)P(Y = 1)\\ &\qquad\text{(since } X \text{ and } Y \text{ are independent)}\\ &= 2/9\,.\end{aligned}$$

We have the table

x	2	3	4	5	6
$P_U(x)$	1/9	2/9	1/3	2/9	1/9

Similarly, we have

x	-2	-1	0	1	2
$P_V(x)$	1/9	2/9	1/3	2/9	1/9

2. The values of (U, V) depend upon those of the tuple (X, Y, Z) which can assume $27 = 3^3$ distinct values ; we find the table :

$P_{(U,V)}$ u v	2	3	4	5	6
-2	a	a	a	0	0
-1	a	$2a$	$2a$	a	0
0	a	$2a$	$3a$	$2a$	a
1	0	a	$2a$	$2a$	a
2	0	0	a	a	a

where $a = 1/27$.

For instance, to compute $P\big((U = 3) \cap (V = -1)\big)$, note that

$$(U = 3) = (X = 1 \text{ and } Y = 2) \cup (X = 2 \text{ and } Y = 1),$$

and

$$(V = -1) = (X = 1 \text{ and } Z = 2) \cup (X = 2 \text{ and } Z = 3)\,;$$

hence :

$$\begin{aligned} P\big((U = 3) \cap (V = -1)\big) &= P\big((X = 1) \cap (Y = 2) \cap (Z = 2)\big) \\ &\quad + P\big((X = 2) \cap (Y = 1) \cap (Z = 3)\big) = 1/27 + 1/27\,. \end{aligned}$$

U and V are not independent, because, e.g.,

$$0 = P\big((U = 5) \cap (V = -2)\big) \neq P(U = 5)P(V = -2) = \frac{2}{9} \times \frac{1}{9}\,.$$

12.19. Let the r.v.'s $X_1, \ldots, X_n$ assume values in $D_1, \ldots, D_n$; we will say that $X_1, \ldots, X_n$ are independent if and only if for all $A_1 \subseteq D_1, \ldots, A_n \subseteq D_n$, the events $X_1 \in A_1, \ldots, X_n \in A_n$ are independent.

12.20. 1. $A \in \mathcal{T}$; this will occur if $\mathcal{T} = \mathcal{P}(\Omega)$.
2. We then have $E(\chi_A) = \sum_{d \in \mathbb{B}} dP(\chi_A = d) = P(\chi_A = 1) = P(A)$.

12.21. 1. We have $E(U) = 4$, and $E(V) = 0$.
2. $E(UV) = \sum_i \sum_j ijP\big((U = i) \cap (V = j)\big) = 2/3$. On the other hand,

$$\begin{aligned} \sigma(U) &= \sqrt{E(U^2) - (E(U))^2} = \sqrt{156/9 - 16} = (2/3)\sqrt{3}, \\ \sigma(V) &= \sqrt{E(V^2) - (E(V))^2} = \sqrt{E(V^2)} = (2/3)\sqrt{3}; \end{aligned}$$

hence $\rho(U, V) = 1/2$, and this indeed confirms that U and V are not independent.

12.22. 1.(a) $E(Z) = (1-a)\sum_{k=1}^{\infty} ka^{k-1} = (1-a)\big(\sum_{k=0}^{\infty} a^k\big)' = \dfrac{1-a}{(1-a)^2} = \dfrac{1}{1-a}$. (see Chapter 8.) We can also have a direct computation : $(1-a)\sum_{k=1}^{\infty} ka^{k-1} = \sum_{k=1}^{\infty} ka^{k-1}$ $-\sum_{k=1}^{\infty} ka^k = 1 + \sum_{k=1}^{\infty}(k+1)a^k - \sum_{k=1}^{\infty} ka^k = \sum_{k=1}^{\infty} a^k = \dfrac{1}{1-a}$.

(b) $P(Z \geq k) = a^{k-1}(1-a)\big(\sum_{i=0}^{\infty} a^i\big) = a^{k-1}$.

2.(a) Note that the event $(T \geq k)$ is the disjoint union of the mutually exclusive events $(T = k)$ and $(T \geq k+1)$; we deduce that $P(T \geq k) = P(T = k) + P(T \geq k+1)$.

It suffices to note that

- $(T \geq k) \iff (\inf(X,Y) \geq k) \iff (X \geq k \text{ and } Y \geq k)$,
- X and Y being independent, $P(X \geq u \text{ and } Y \geq v) = P(X \geq u)P(Y \geq v)$; and thus

$$\begin{aligned} P(T = k) &= P(T \geq k) - P(T \geq k+1) \\ &= P(X \geq k \text{ and } Y \geq k) - P(X \geq k+1 \text{ and } Y \geq k+1) \\ &= P(X \geq k)P(Y \geq k) - P(X \geq k+1)P(Y \geq k+1) \end{aligned}$$

(b) We deduce then from 2 (a) that $p(T = k) = p^{k-1}q^{k-1} - p^k q^k = (pq)^{k-1}(1-pq)$.

3.(a) Firstly, note that

$$\begin{aligned} T_n = \inf(X_1, \ldots, X_n) \geq k \quad &\iff \quad T_n = \inf(T_{n-1}, X_n) \geq k \\ &\iff (T_{n-1} \geq k \text{ and } X_n \geq k) \end{aligned}$$

Then check that, if $X_1, \ldots, X_n$ are independent, then T_{n-1} and X_n are independent ; indeed

$$\begin{aligned} P(T_{n-1} \geq u \text{ and } X_n \geq v) &= P(X_1 \geq u \text{ and } \ldots \text{and } X_{n-1} \geq u \text{ and } X_n \geq v) \\ &= P(X_1 \geq u) \cdots P(X_{n-1} \geq u)P(X_n \geq v) \\ &= P(T_{n-1} \geq u)P(X_n \geq v) \; . \end{aligned}$$

We can then apply 2 and generalize it by induction on n :

- for $n = 1$, $T_1 = X_1$ has a geometric distribution of ratio p ;
- for the induction, use 2 and the above two remarks.

(b) By 1 (b) we know that $P(T_n > 1) = P(T_n \geq 2) = p^n$, hence the result.

12.23. Let X be the r.v. which, to each individual in the population, associates its height. Then $E(X) = 1.65$ and $\sigma(X) = 0.04$.

Markov's inequality will give us the rather rough upper bound $P(X \geq 1.80) \leq \dfrac{1.65}{1.80} = 0.916$.

Chebyshev's inequality will gives us the much better upper bound

$$\begin{aligned} P(X \geq 1.80) &\leq P(|X - 1.65| \geq 0.15) \\ &\leq \Big(\frac{0.04}{0.15}\Big)^2 = 0.071 \end{aligned}$$

12.24. We want to determine integers n such that

$$P\Big(S_n \leq -\frac{1}{2}\Big) \leq \frac{1}{100} \; .$$

The r.v.'s $X_1, \dots, X_n$ are independent, and X_i has the same distribution as $-X_i$; thus S_n has the same distribution as $-S_n$, hence, for all $a > 0$

$$P(S_n \le -a) = P(S_n \ge a) = \frac{1}{2} P(|S_n| \ge a)$$

Moreover, we have

$$\begin{gathered} E(X_i) = 0 \quad \Longrightarrow \quad E(S_n) = 0\,, \\ var(X_i) = E(X_i^2) - \big(E(X_i)\big)^2 = 1\,, \end{gathered}$$

$$\begin{aligned} X_1, \dots, X_n \text{ independent } &\Longrightarrow \ var(X_1 + \cdots + X_n) = n \\ \text{by Proposition 12.51 } &\Longrightarrow \ var(S_n) = \frac{1}{n^2} var(X_1 + \cdots + X_n) = \frac{1}{n}\,. \end{aligned}$$

Chebyshev's inequality then gives us the upper bound

$$\begin{array}{cl} \forall a > 0, & P(|S_n| \ge a) \le \dfrac{1}{na^2}\,, \\ \text{hence} & P(S_n \le -a) \le \dfrac{1}{2na^2}\,, \\ \text{and for } a = \dfrac{1}{2}\,, & P(S_n \le -\dfrac{1}{2}) \le \dfrac{2}{n}\,, \\ \text{and lastly} & P(S_n \le -\dfrac{1}{2}) \le \dfrac{1}{100}\,, \quad \forall n \ge 100\,. \end{array}$$

12.25. $E(X) = d(-1)$; $var(X) = d(-2) - d(-1)^2$; $E(\log X) = -d'(0)$.

12.26.

$$\begin{aligned} g_{X+Y}(z) &= \sum_{n=0}^{\infty} P(X + Y = n) z^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} P(X = i, Y = j) z^n \right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} P(X = i) P(Y = j) z^n \right) \\ &\qquad \text{(since the r.v.'s } X \text{ and } Y \text{ are independent)} \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} P(X = i) z^i P(Y = j) z^j \right) \\ &= \left(\sum_{i=0}^{\infty} P(X = i) z^i \right) \left(\sum_{j=0}^{\infty} P(Y = j) z^j \right) \\ &\qquad \text{(by the definition of the product of series)} \\ &= g_X(z) g_Y(z)\,. \end{aligned}$$

12.27. 1. $P(S_1 = k) = pq^{k-1}$, $g_{S_1}(z) = \displaystyle\sum_{k=1}^{\infty} pq^{k-1} z^k = \frac{p}{q} \sum_{k=1}^{\infty} (qz)^k = \frac{p}{q} \times \frac{1}{1 - qz}$.

2. $S_r = X_1 + \cdots + X_r$, the r.v.'s X_i are mutually independent with the distribution of S_1 as the common distribution, thus $g_{S_r}(z) = \big(g_{S_1}(z)\big)^r = \left(\frac{p}{q}\right)^r \times \left(\frac{1}{1 - qz}\right)^r$.

3. We deduce from 2 that

$$\begin{aligned}
P(S_r = k) &= \Big(\frac{p}{q}\Big)^r \frac{r(r+1)\cdots(r+k-1)}{k!} q^k\,,\\
E(S_r) &= g'_{S_r}(1) = rq\Big(\frac{p}{q}\Big)^r\Big(\frac{1}{1-q}\Big)^{r+1}\\
&= \frac{r}{pq^{r-1}}\,,\\
var(S_r) &= \frac{r(r+1)}{p^2q^{r-2}} + \frac{r}{pq^{r-1}} - \Big(\frac{r}{pq^{r-1}}\Big)^2.
\end{aligned}$$

12.28. 1. The event $V = k$ can be subdivided into the union $\bigcup_{j=1}^{n}\big((U = j)\cap((\sum_{i=1}^{j} X_i) = k)\big)$. These events being disjoint, we have

$$P(V = k) = \sum_{j=1}^{n} P\Big((U = j)\cap\Big(\sum_{i=1}^{j} X_i\Big) = k\Big)$$

U and X_i being independent,

$$P\Big((U = j)\cap\Big(\sum_{i=1}^{j} X_i\Big) = k\Big) = P(U = j)\times P\Big(\Big(\sum_{i=1}^{j} X_i\Big) = k\Big)$$

2. First note that, by Proposition 12.62 and the independence of the X_is, we can prove by induction on j that $\forall j = 1,\ldots,n$, the generating function of the r.v. $\sum_{i=1}^{j} X_i$ is given by : $g_{\sum_{i=1}^{j} X_i}(z) = (g(z))^j$. Compute the generating function of V :

$$\begin{aligned}
g_V(z) &= \sum_{k\in\mathbb{N}} P(V = k)z^k\\
&= \sum_{k\in\mathbb{N}}\Big(\sum_{j=1}^{n} P(U = j)\times P\Big(\Big(\sum_{i=1}^{j} X_i\Big) = k\Big)z^k\Big)\\
&= \sum_{j=1}^{n} P(U = j)\Big(\sum_{k\in\mathbb{N}} P\Big(\Big(\sum_{i=1}^{j} X_i\Big) = k\Big)z^k\Big)\\
&= \sum_{j=1}^{n} P(U = j)g_{\sum_{i=1}^{j} X_i}(z)\\
&= \sum_{j=1}^{n} P(U = j)(g(z))^j = f(g(z))\,.
\end{aligned}$$

3.

$$\begin{aligned}
\text{Since } g(1) = 1,\quad E(V) &= g'_V(1) = g'(1)f'\big(g(1)\big) = E(X_i)E(U)\,;\\
g''_V(z) &= g''(z)f'(g(z)) + \big(g'(z)\big)^2 f''\big(g(z)\big);\\
\text{hence}\quad var(V) &= var(U)\big(E(X_i)\big)^2 + E(U)var(X_i)\,.
\end{aligned}$$

12.29. 1. The generating functions of X and Y are given by

$$\begin{aligned}
g_X(z) &= \sum_{k=0}^{m}\binom{m}{k}p^k q^{m-k}z^k = (pz+q)^m,\\
g_Y(z) &= \sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k}z^k = (pz+q)^n.
\end{aligned}$$

and, since X and Y are independent,

$$g_{X+Y}(z) = g_X(z)g_Y(z) = (pz+q)^{n+m}.$$

$X+Y$ thus has a binomial distribution $b(p, m+n)$ of parameters $(p, m+n)$.
2. For $x \in \{1, 2, \dots, s\}$, we have

$$\begin{aligned} P(X = x \,/\, S = s) &= \frac{P(X = x\,,\, X+Y = s)}{P(X+Y = s)} = \frac{P(X = x\,,\, Y = s-x)}{P(X+Y=s)} \\ &= \frac{P(X=x)P(Y=s-x)}{P(X+Y=s)} \\ &\qquad\text{(since } X \text{ and } Y \text{ are independent)} \\ &= \frac{\binom{m}{x}p^x q^{m-k}\binom{n}{s-x}p^{s-x}q^{n-s+x}}{\binom{m+n}{s}p^s q^{m+n-s}} = \frac{\binom{m}{x}\binom{n}{s-x}}{\binom{m+n}{s}} \end{aligned}$$

for $x > s$, $P(X = x \,/\, S = s) = 0$.

The conditional distribution of X given S is thus a hypergeometric distribution (see Section 12.6.4).

12.30. Each sequence $(x_1, \dots, x_n)$ containing k people of type 1 has probability $p^k q^{n-k}$ of being obtained. Moreover, there are $n!$ ways of permuting $(x_1, \dots, x_n)$, but among the $n!$ ways, the $k!$ permutations of the k people of type 1 and the $(n-k)!$ permutations of the $n-k$ people of type 0 give the same result, hence : $P(S = k) = \dfrac{n!}{k!(n-k)!}p^k q^{n-k} = \dbinom{n}{k}p^k q^{n-k}$.

12.31. 1. To study the distribution of S_i, we can group together all the values $j = 1, \dots, n$, $j \neq i$, in a single value d_i ; then S_i has the binomial distribution $b(p_i, n)$.

$\Gamma(S_1, S_2) = E(S_1 S_2) - E(S_1)E(S_2)$, where S_1 and S_2 have binomial distributions with respective parameters p_1 and $p_2 = 1 - p_1$; we want to compute $E(S_1 S_2)$. Consider, for $i = 1, \dots, n$, the characteristic functions $\chi_i^1 = \chi_{(X_i=1)}$ and $\chi_i^2 = \chi_{(X_i=2)}$, and note that $S_1 = \sum_{i=1}^n \chi_i^1$ and $S_2 = \sum_{j=1}^n \chi_j^2$; hence

$$\begin{aligned} E(S_1 S_2) &= E\left(\left(\sum_{i=1}^n \chi_i^1\right)\left(\sum_{j=1}^n \chi_j^2\right)\right) \\ &= E\left(\sum_{i=1}^n \sum_{j=1}^n \chi_i^1 \chi_j^2\right) \\ &= n(n-1)p_1 p_2 \\ \text{and} \qquad \Gamma(S_1, S_2) &= n(n-1)p_1 p_2 - n^2 p_1 p_2 = -np_1 p_2 \end{aligned}$$

2. Let $(X_1, \dots, X_p)$ be discrete r.v.'s ; we can generalize the generating functions in order to represent the distribution of $(X_1, \dots, X_p)$. Let $\overline{X} = (X_1, \dots, X_p)$ and

$$g_{\overline{X}}(z_1, \dots, z_p) = \sum_{i_1, \dots, i_p} P(X_1 = i_1, \dots, X_p = i_p) z_1^{i_1} \cdots z_p^{i_p} = E\big((z_1^{X_1} \cdots z_p^{X_p})\big) \,.$$

Therefore,

$$\begin{aligned} g_{(S_1, \dots, S_r)}(z_1, \dots, z_r) &= \sum_{i_1, \dots, i_r} P(S_1 = i_1, \dots, S_r = i_r) z_1^{i_1} \cdots z_r^{i_r} \\ &= E\big((z_1^{S_1} \cdots z_r^{S_r})\big) \end{aligned}$$

and, noting that $S_k = \sum_{i=1}^n \chi_{(X_i=k)}$,

$$\begin{aligned}
g_{(S_1,\dots,S_r)}(z_1,\dots,z_r) &= E\big((z_1^{S_1}\cdots z_r^{S_r})\big)\\
&= E\Big(\Big(z_1^{\sum_{i=1}^n \chi(X_i=1)}\cdots z_r^{\sum_{i=1}^n \chi(X_i=r)}\Big)\Big)\\
&= E\Big(\prod_{j=1}^n (z_1^{\chi(X_j=1)}\cdots z_r^{\chi(X_j=r)})\Big)\\
&= \prod_{j=1}^n \big(E(z_1^{\chi(X_j=1)}\cdots z_r^{\chi(X_j=r)})\big)\\
&\qquad\text{(since the } X_j\text{s are independent)}\\
&= \prod_{j=1}^n \big(p_1z_1+\cdots+p_rz_r\big) = (p_1z_1+\cdots+p_rz_r)^n
\end{aligned}$$

We can easily prove the following properties of generating functions depending on many variables :

- $g_{X_i}(z) = g_{\overline{X}}(1,\dots,1,z,1,\dots,1)$, where $z_1=\cdots=z_{i-1}=z_{i+1}=\cdots=z_p=1$,
- $g_{X_1+\cdots+X_p}(z) = g_{\overline{X}}(z,\dots,z)$,
- $(X_1,\dots,X_p)$ are independent if and only if $g_{\overline{X}}(z_1,\dots,z_p) = \Pi_{k=1}^p g_{X_k}(z_k)$.

12.32. $X\colon\Omega \longrightarrow \mathbb{N}$, where Ω is the set of sequences $\{1^n0\,/\,n\in\mathbb{N}\}\cup\{111\cdots11\cdots\}$, with the convention $1^00=0$, and with $\mathcal{T}=\mathcal{P}(\Omega)$, $\forall n\in\mathbb{N}$, $P(1^n0)=p^nq$ and $P(111\cdots11\cdots)=0$.

12.33. 1. $1/2^{n-1}$.

2.
$$\sum_{i=2}^{5}\frac{1}{2^{i-1}} = \sum_{i=1}^{4}\frac{1}{2^i} = \frac{1/2(1-(1/2)^4)}{1/2} = \frac{15}{16}\,.$$

3. Let $A=$‘an even number of tosses is necessary’ and $B=$‘an odd number of tosses is necessary’. We have $P(A)+P(B)=1$, and

$$P(A) = \frac{1}{2}+\frac{1}{2^3}+\frac{1}{2^5}+\cdots = \sum_{n=1}^{\infty}\frac{1}{2^{2n-1}}\ ,$$
$$P(B) = \frac{1}{2^2}+\frac{1}{2^4}+\frac{1}{2^6}+\cdots = \frac{1}{2}P(A) = \sum_{n=1}^{\infty}\frac{1}{2^{2n}}\ .$$

Hence $P(A)=2/3$.

12.34. The methods are similar to the ones used in Exercise 12.31. Note, however, that here the χ_i are not independent.

1. We will apply Proposition 12.56. We have

(i) $$E(S_1) = E(\chi_1)+\cdots+E(\chi_n)$$

(ii) $$var(S_1) = var(\chi_1)+\cdots+var(\chi_n)+2\sum_{1\le i<j\le n}\Gamma(\chi_i,\chi_j)$$

Noting that

$$\begin{aligned}
\forall i = 1, \ldots, n, \qquad E(\chi_i) &= P(\chi_i = 1) = \frac{n_1}{N} = p_1 \,, \\
\forall i = 1, \ldots, n, \qquad var(\chi_i) &= E((\chi_i)^2) - E(\chi_i)^2 = p_1 - p_1^2 = p_1 p_2 \,, \\
E(\chi_i, \chi_j) &= P(\chi_i = 1, \chi_j = 1) = \frac{n_1(n_1-1)}{N(N-1)} \,, \\
\Gamma(\chi_i, \chi_j) &= \frac{n_1(n_1-1)}{N(N-1)} - \left(\frac{n_1}{N}\right)^2 = \frac{-n_1 n_2}{N^2(N-1)} \,.
\end{aligned}$$

Then applying (i) and (ii) we deduce

$$E(S_1) = np_1 \,, \quad var(S_1) = np_1 p_2 \Big(\frac{N-n}{N-1}\Big).$$

2. Grouping together all types which are different from j reduces the problem to case 1.

12.35. Let

$$F(k) = P(S_1 = k) = \binom{n}{k} \frac{\binom{N-n}{n_1-k}}{\binom{N}{n_1}} \,.$$

We have

$$\frac{n_1}{N} \to 0 \,, \; \frac{n}{N} \to 0 \,, \;\text{ and }\; F(0) = \frac{(N-n_1)(N-n_1-1)\cdots(N-n_1-n+1)}{N(N-1)\cdots(N-n+1)} \,;$$

hence

$$\begin{aligned}
&\log F(0) = \log\left(1 - \frac{n_1}{N}\right) + \log\left(1 - \frac{n_1}{N-1}\right) + \cdots + \log\left(1 - \frac{n_1}{N-n+1}\right) \,, \\
&n \log\left(1 - \frac{n_1}{N}\right) \le \log F(0) \le n \log\left(1 - \frac{n_1}{N-n+1}\right) \,.
\end{aligned}$$

Taking the limits, the right-hand side and left-hand side of the inequality go to $-\lambda$; thus $\log F(0) \to -\lambda$ and $F(0) \to e^{-\lambda}$. For $k \in \mathbb{N}$, $k \neq 0$, the ratio

$$\frac{F(k+1)}{F(k)} = \frac{(n-k)(n_1-k)}{(k+1)(N-n_1-n+k)}$$

is equivalent to $\dfrac{nn_1}{(k+1)N} \sim \dfrac{\lambda}{k+1}$; thus $F(k) \to e^{-\lambda}\dfrac{\lambda^k}{k!}$.

12.36.

1.
$$\begin{aligned}
\sum_{n \le m} P(X = n, Y = m) &= \sum_{m=0}^{\infty} \left(\sum_{n=0}^{m} \frac{m!}{n!(m-n)!} \right) \frac{\lambda^m}{m!} e^{-2\lambda} \\
&= \sum_{m=0}^{\infty} 2^m \frac{\lambda^m}{m!} e^{-2\lambda} \\
&= e^{2\lambda} e^{-2\lambda} = 1 \,.
\end{aligned}$$

The distribution of (X, Y) is thus entirely determined by the given probabilities.

2.
$$\begin{aligned}
P(X=n) &= \sum_{m=0}^{\infty} P(X=n, Y=m) \\
&= \sum_{m\geq n} \frac{\lambda^m}{n!(m-n)!} e^{-2\lambda} \\
&= \frac{\lambda^n}{n!} e^{-2\lambda} \left(\sum_{i=0}^{\infty} \frac{\lambda^i}{i!} \right) \\
&= \frac{\lambda^n}{n!} e^{-\lambda}.
\end{aligned}$$

X thus has a Poisson distribution with mean λ.

$$\begin{aligned}
P(Y=m) &= \sum_{n=0}^{\infty} P(X=n, Y=m) \\
&= \sum_{n=0}^{m} \frac{\lambda^m}{n!(m-n)!} e^{-2\lambda} \\
&= \frac{\lambda^m}{m!} e^{-2\lambda} \left(\sum_{n=0}^{m} \frac{m!}{n!(m-n)!} \right) \\
&= \frac{(2\lambda)^m}{m!} e^{-2\lambda}.
\end{aligned}$$

Y thus has a Poisson distribution with mean 2λ.

$$\begin{aligned}
P(X=0, Y=0) &= e^{-2\lambda}, \\
P(X=0)P(Y=0) &= e^{-\lambda}e^{-2\lambda} = e^{-3\lambda}.
\end{aligned}$$

Thus X and Y are not independent.

3. Note that $Y \geq X$, therefore $Y - X$ is integral-valued.

$$\begin{aligned}
P(Y-X=r) &= \sum_{n=0}^{\infty} P(X=n, Y=n+r) \\
&= \left(\sum_{n=0}^{\infty} \frac{\lambda^{n+r}}{n!r!} \right) e^{-2\lambda} \\
&= \frac{\lambda^r}{r!} e^{-\lambda}.
\end{aligned}$$

$Y - X$ thus has a Poisson distribution with mean λ.

$$\begin{aligned}
P(X=n, Y-X=r) &= P(X=n, Y=n+r) \\
&= \frac{\lambda^{n+r}}{n!r!} e^{-2\lambda} \\
&= P(X=n)P(Y-X=r).
\end{aligned}$$

Hence, the r.v.'s X and $Y - X$ thus are independent.

4.
$$\begin{aligned}\Gamma(X,Y) &= \Gamma(X, X+Y-X)\\ &= \Gamma(X,X) + \Gamma(X, Y-X)\\ &= \Gamma(X,X) \qquad \text{(because } X \text{ and } Y-X \text{ are independent)}\\ &= \sigma^2(X) = \lambda\,.\end{aligned}$$
$$\rho(X,Y) = \frac{\Gamma(X,Y)}{\sigma(X)\sigma(Y)} = \frac{\lambda}{\sqrt{\lambda}\sqrt{2\lambda}} = \frac{\sqrt{2}}{2}\,.$$

12.37. 1. $P(Z=z, N=n) = P(N=n)P(Z=z\,/\,N=n)$. Moreover the r.v. Z conditioned by N has a binomial distribution, i.e. $P(Z=z\,/\,N=n) = \binom{n}{z}p^z(1-p)^{n-z}$; hence
$$P(Z=z, N=n) = e^{-\lambda}\frac{\lambda^n}{n!}\binom{n}{z}p^z(1-p)^{n-z} = A(n,z)\,.$$

2.
$$\begin{aligned}P(Z=z) &= \sum_{n=z}^{\infty} P(Z=z, N=n) = \sum_{n=z}^{\infty} A(n,z)\\ &= e^{-\lambda}\frac{(\lambda p)^z}{z!}\left(\sum_{n=0}^{\infty}\lambda^{n-z}\frac{(1-p)^{n-z}}{(n-z)!}\right)\\ &= e^{-\lambda}\frac{(\lambda p)^z}{z!}e^{\lambda(1-p)}.\end{aligned}$$

Thus Z has a Poisson distribution with mean λp.

3. $P(N=n\,/\,Z=z) = \dfrac{P(N=n, Z=z)}{P(Z=z)}$. We deduce that the distribution of N conditioned by Z is a Poisson distribution with mean $\lambda(1-p)$.

4.
$$\rho(N,Z) = \frac{\Gamma(N,Z)}{\sigma(N)\sigma(Z)} = \frac{E(NZ) - E(N)E(Z)}{\sigma(N)\sigma(Z)}\,.$$

All the factors are known, except for $E(NZ)$.
$$\begin{aligned}E(NZ) &= \sum_{n=1}^{\infty}\sum_{z=0}^{n} nzP(N=n, Z=z)\\ &= \sum_{n=1}^{\infty} ne^{-\lambda}\frac{\lambda^n}{n!}\underbrace{\left(\sum_{z=0}^{n} z\frac{n!}{z!(n-z)!}p^z(1-p)^{n-z}\right)}_{\text{mean of a binomial distribution}}\\ &= \sum_{n=1}^{\infty} ne^{-\lambda}\frac{\lambda^n}{n!}np\\ &= p\sum_{n=1}^{\infty} n^2e^{-\lambda}\frac{\lambda^n}{n!} = pE(N^2)\end{aligned}$$

Since N has a Poisson distribution with mean λ, we have
$$\begin{aligned}\sigma^2(N) &= E(N^2) - E(N)^2 = \lambda\,, \qquad \text{hence}\\ E(N^2) &= \lambda + \lambda^2\,, \qquad \text{thus}\\ E(NZ) &= \lambda p(1+\lambda);\\ E(N) &= \lambda; \qquad E(Z) = \lambda p;\\ \sigma(N) &= \sqrt{\lambda}; \qquad \sigma(Z) = \sqrt{\lambda p}; \qquad \text{hence}\\ \rho(N,Z) &= \frac{p\lambda + p\lambda^2 - p\lambda^2}{\lambda\sqrt{p}} = \sqrt{p}\,.\end{aligned}$$

Chapter 13

13.1. We check by induction on n that the distribution of each X_n is entirely determined by conditions 1 and 2.

13.2. 1. Let $n \geq 1$. Assume that for $k \leq n-1$ the probability distribution of X_k is given by

$$P(X_k = \text{'yes'}) = P(X_k = \text{'no'}) = p = \frac{1}{2}\ .$$

Then

$$\begin{aligned} P(X_n = \text{'yes'}) &= P(X_n = \text{'yes' and } X_{n-1} = \text{'yes'}) \\ &\qquad + P(X_n = \text{'yes' and } X_{n-1} = \text{'no'}) \\ &= P(X_n = \text{'yes'}/X_{n-1} = \text{'yes'})P(X_{n-1} = \text{'yes'}) \\ &\qquad + P(X_n = \text{'yes'}/X_{n-1} = \text{'no'})P(X_{n-1} = \text{'no'}) \\ &= \frac{1}{2}p_{11} + \frac{1}{2}p_{21} = \frac{1}{2}p + \frac{1}{2}(1-p) = \frac{1}{2}. \end{aligned}$$

Hence we also have $P(X_n = \text{'no'}) = 1 - 1/2 = 1/2$.

We deduce, applying complete induction (Chapter 3, rule (I'_{n_0}) with $n_0 = 1$) that all the X_ns have the same distribution as X_0.

2. No : we have $P(X_n = \text{'yes'}) = 1/2$ whilst $P(X_n = \text{'yes'}/X_{n-1} = \text{'yes'}) = p$. In order for X_n and X_{n-1} to be independent $p = 1/2$ must hold. This necessary condition is also sufficient (see Exercise 13.6).

13.3. 1. $c = 0$. The condition is necessary (except if $b = 0$ or $r = 0$) by Example 13.3. It is clearly sufficient.

2. Yes. Indeed, we have, by Exercise 12.5 : $P(X^{n+1} = B) = (b/(b+r))$, and in this case we will have $Y_{n+1} = Y_n + c$ and $P(X^{n+1} = R) = (r/(b+r))$, and in that case we will have $Y_{n+1} = Y_n$. Letting $Y_n = k$, we deduce :

$$P(Y_{n+1} = m \,/\, Y_n = k) = \begin{cases} (b/(b+r)) & \text{if } m = k + c, \\ (r/(b+r)) & \text{if } m = k, \\ 0 & \text{otherwise.} \end{cases}$$

13.4. 1. Assume that the turrets are numbered from 1 to 4. The system is in state i at time n, i.e. $X_n = i$ if the nth move of the sentry led him to the ith turret ($i = 1, \ldots, 4$).

2. X_n is a Markov chain because, for all $n > 0$,

$$P(X_n = i) = \begin{cases} 1/2 & \text{if } X_{n-1} \equiv (i-1)\,[4] \text{ or } X_{n-1} \equiv (i+1)\,[4]\ . \\ 0 & \text{otherwise.} \end{cases}$$

Its transition matrix is

$$P = \begin{pmatrix} 0 & 1/2 & 0 & 1/2 \\ 1/2 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 1/2 \\ 1/2 & 0 & 1/2 & 0 \end{pmatrix}\ .$$

13.5.

1.
$$\begin{aligned}P(X_{n+1}=i) &= \sum_{j=1}^{r} P(X_{n+1}=i \text{ and } X_n=j)\\ &= \sum_{j=1}^{r} P(X_{n+1}=i/X_n=j)P(X_n=j)\\ &= \sum_{j=1}^{r} p_{ji}P(X_n=j)\ .\end{aligned}$$

Hence, $L_{n+1} = P^t \times L_n$, where P^t is the transpose matrix of P.

2. We deduce by induction on n that $L_{n+1} = (P^t)^{n+1}L_0\ , \quad \forall n \geq 0$.

3. If all the X_ns have the same distribution, we have in particular $L_1 = P^tL_0 = L_0$. L_0 is thus an eigenvector of the matrix P^t for the eigenvalue 1. Conversely, if the probability distribution L_0 of X_0 is an eigenvector associated with the eigenvalue 1 of the matrix P^t, we have $L_1 = P^tL_0 = L_0$ and, by induction on n, $L_n = L_0$ for all n.

13.6. 1. (i) $\Longrightarrow$ (ii) Let j be fixed column. X_k and X_{k+1} being independent, $\forall i, \quad p_{ij} = P(X_{k+1}=j/X_k=i) = P(X_{k+1}=j)$.
(ii) $\Longrightarrow$ (iii) For any k, $\forall i,j : P(X_{k+1}=j/X_k=i) = p_{ij} = p_j$. Moreover,

$$\begin{aligned}P(X_{k+1}=j) &= \sum_i P(X_{k+1}=j \text{ and } X_k=i)\\ &= \sum_i P(X_{k+1}=j/X_k=i) \times P(X_k=i)\\ &= \sum_i p_{ij}P(X_k=i) = \sum_i p_jP(X_k=i) = p_j\sum_i P(X_k=i)\\ &= p_j\ .\end{aligned}$$

Thus, for all k,
$$P(X_{k+1}=j/X_k=i) = P(X_{k+1}=j),$$
i.e. X_{k+1} and X_k are independent.
(iii) $\Longrightarrow$ (iv) Assume that for all k, X_k and X_{k+1} are independent and let us show that $\forall n \geq 1, \quad (X_0,\ldots,X_n)$ are independent.
(B) The result holds for $n=1$.
(I) Assume $(X_0,\ldots,X_n)$ are independent, and let us compute

$$\begin{aligned}&P(X_0=i_0,\ldots,X_n=i_n,X_{n+1}=i_{n+1})\\ &\quad= P(X_{n+1}=i_{n+1}/X_0=i_0,\ldots,X_n=i_n)\\ &\qquad\qquad \times P(X_0=i_0,\ldots,X_n=i_n)\\ &\quad= P(X_{n+1}=i_{n+1}/X_n=i_n)P(X_0=i_0,\ldots,X_n=i_n)\\ &\qquad\qquad \text{by the Markov property}\\ &\quad= P(X_{n+1}=i_{n+1}/X_n=i_n)P(X_n=i_n)\cdots P(X_0=i_0)\\ &\qquad\qquad \text{by the independence of } (X_0,\ldots,X_n)\\ &\quad= P(X_{n+1}=i_{n+1})P(X_n=i_n)\cdots P(X_0=i_0)\\ &\qquad\qquad \text{by the independence of } X_n \text{ and } X_{n+1}.\end{aligned}$$

$(X_0,\ldots,X_n,X_{n+1})$ are thus independent, hence the induction hypothesis and the result.
(iv) $\Longrightarrow$ (i) Straightforward.

2. The distribution of X_n is given by $\forall j\ , \quad P(X_n=j) = p_j$. All the X_ns thus have the same distribution, given by the row of the matrix P and independent of the probability distribution of X_0.

13.7. 1 and 2 are quite easy to verify by computations using the Markov property. Let us check the last equality, which is slightly more complex.

3. Let $B_n = (X_{n+1} \in A_1, \ldots, X_{n+k} \in A_k)$, $C_n = (X_n = E_{i_k})$, and $A = (X_0 \in A'_0, \ldots, X_{n-1} \in A'_{n-1})$; note that we can decompose A in a partition $A = \sum_{i\in I} A_i$, where each A_i is of the form $(X_0 = E_{i_0}, \ldots, X_{n-1} = E_{i_{n-1}})$. We then have

$$\begin{aligned}
P(X_{n+1} \in A_1, \ldots, X_{n+k} \in A_k \,/\, X_0 \in A'_0, \ldots, X_{n-1} \in A'_{n-1}, X_n = E_{i_k})& \\
= P(B_n \,/\, C_n \cap A) = P(B_n \,/\, C_n \cap {\textstyle\sum_{i\in I}} A_i)& \\
= \frac{\sum_{i\in I} P(B_n \cap C_n \cap A_i)}{\sum_{i\in I} P(C_n \cap A_i)}& \\
= \frac{\sum_{i\in I} P(B_n \,/\, C_n \cap A_i) \times P(C_n \cap A_i)}{\sum_{i\in I} P(C_n \cap A_i)}&\,.
\end{aligned}$$

By 2, we have $P(B_n \,/\, C_n \cap A_i) = P(B_0 \,/\, C_0)$, and hence

$$\begin{aligned}
P(X_{n+1} \in A_1, \ldots, X_{n+k} \in A_k \,/\, X_0 \in A'_0, \ldots, X_{n-1} \in A'_{n-1}, X_n = E_{i_k})& \\
= P(B_0 \,/\, C_0) \times \frac{\sum_{i\in I} P(C_n \cap A_i)}{\sum_{i\in I} P(C_n \cap A_i)}& \\
= P(B_0 \,/\, C_0)& \\
= P(X_1 \in A_1, \ldots, X_k \in A_k \,/\, X_0 = E_{i_k})&\,.
\end{aligned}$$

13.8. Decompose the event E_{ijn} = ‘the system starting from E_i is in E_j after n steps’ in the k disjoint events, $E^k_{ijn} = A^k_{ij} \cap E_{jj(n-k)}$, $k = 1, \ldots, n$, where

- A^k_{ij} =‘the system starting from E_i reaches E_j for the first time after k steps’ and
- $E_{jj(n-k)}$ =‘the system then goes E_j to E_j in $n-k$ steps’.

We have $p^{(n)}_{ij} = P(E_{ijn}) = \sum_{k=1}^n P(E^k_{ijn})$ with

$$P(E^k_{ijn}) = P(A^k_{ij} \cap E_{jj(n-k)}) = P(E_{jj(n-k)} \,/\, A^k_{ij})P(A^k_{ij})\,,$$

and by the Markov chain property, $P(E^k_{ijn}) = p^{(n-k)}_{jj} f^{(k)}_{ij}$.

13.9. Straightforward by noting that $P(X_0 = X_1 = \cdots = X_n = E_i \,/\, X_0 = E_i) = p^n_{ii}$.

13.10. If E_i is absorbing, then $p_{ii} = f^{(1)}_{ii} = f_{ii} = 1$, and thus E_i is persistent.

13.11. 1.

$$\begin{aligned}
E(N_j \,/\, X_0 = i) &= E\left(\sum_{n=0}^{\infty} \delta_{nj} \,/\, X_0 = i\right) \\
&= \sum_{n=0}^{\infty} E(\delta_{nj} \,/\, X_0 = i) \\
&= \sum_{n=0}^{\infty} \big(0 \times P(\delta_{nj} = 0 \,/\, X_0 = i) + 1 \times P(\delta_{nj} = 1 \,/\, X_0 = i)\big) \\
&= \sum_{n=0}^{\infty} \big(0 \times (1 - p^{(n)}_{ij}) + 1 \times p^{(n)}_{ij}\big) \\
&= \sum_{n=0}^{\infty} p^{(n)}_{ij} \\
&= u_{ij}
\end{aligned}$$

2.

$$\begin{aligned}
u_{ij} &= E(N_j \,/\, X_0 = i) \\
&= \sum_{k=0}^{\infty} P(N_j = k \,/\, X_0 = i) \\
&= \sum_{k=0}^{\infty} f_{ij} P(N_j = k \,/\, X_0 = j) \qquad (15.2) \\
&= f_{ij} \sum_{k=0}^{\infty} P(N_j = k \,/\, X_0 = j) \\
&= f_{ij} E(N_j \,/\, X_0 = j) = f_{ij} u_{jj} \ ,
\end{aligned}$$

where (15.2) follows from (13.6). A direct computation using the distribution of N_j given that $X_0 = j$ yields $E(N_j \,/\, X_0 = j) = \sum_{k=0}^{\infty} k(1 - f_{jj}) f_{jj}^{k-1} = \dfrac{1}{1 - f_{jj}} = u_{jj}$.

13.12. 1. X_n ranges over the values 0, 1, and 2.
Let B_1^l (resp. B_2^l) be the event : 'draw a black ball from U_1 (resp. U_2) given that U_1 (resp. U_2) contains l black balls'. Let $\overline{B}_1^{\,l}$ (resp. $\overline{B}_2^{\,l}$) be the complementary event, i.e. 'draw a non-black ball from U_1 (resp. U_2) given that U_1 (resp. U_2) contains l black balls'. We have, for $k, l \in \{0, 1, 2\}$:

$$\begin{aligned}
P(X_n = k \,/\, X_{n-1} = l) &= 0 \quad \text{if } |k - l| \geq 2 \ , \\
P(X_n = l + 1 \,/\, X_{n-1} = l) &= P(\overline{B}_1^{\,l}) \times P(B_2^{2-l}) = \frac{5 - l}{5} \times \frac{2 - l}{5} \ , \\
P(X_n = l \,/\, X_{n-1} = l) &= P(B_1^l) \times P(B_2^{2-l}) + P(\overline{B}_1^{\,l}) \times P(\overline{B}_2^{\,2-l}) \\
&= \frac{l}{5} \times \frac{2 - l}{5} + \frac{5 - l}{5} \times \frac{5 - (2 - l)}{5} \ , \\
P(X_n = l - 1 \,/\, X_{n-1} = l) &= P(B_1^l) \times P(\overline{B}_2^{\,2-l}) = \frac{l}{5} \times \frac{5 - (2 - l)}{5} \ .
\end{aligned}$$

The X_ns form a Markov chain because the above probabilities are independent of n.
2. We obtain the matrix

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \!\!\begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} 15/25 & 10/25 & 0 \\ 4/25 & 17/25 & 4/25 \\ 0 & 10/25 & 15/25 \end{pmatrix} \end{array}$$

and the graph (figure 15.12)

Figure 15.12

The chain is thus irreducible and all its states are persistent.
3. Returning to the result of Exercise 13.5, we deduce that all the X_ns have the same probability distribution if the vector

$$L_0 = \begin{pmatrix} P(X_0 = 0) \\ P(X_0 = 1) \\ P(X_0 = 2) \end{pmatrix}$$

is an eigenvector of the matrix P^t associated with the eigenvalue 1, i.e. if

$$P(X_0 = 0) = 2/9 \ , \ P(X_0 = 1) = 5/9 \ \text{ and } P(X_0 = 2) = 2/9 \ .$$

13.13. 1. Each urn contains a fixed number (nine) of balls. The total number of black (resp. red) balls is also invariant. Assume that at step n urn U_1 contains k $(0 \leq k \leq 4)$ black balls. Then at step n, U_2 will contain $l = 4 - k$ black balls and for all $n \geq 0$, we will have

$$P(X_{n+1} = j \,/\, X_n = k) = \begin{cases} \dfrac{9-k}{9} \times \dfrac{4-k}{9} & \text{if } j = k+1, \\ \dfrac{k}{9} \times \dfrac{4-k}{9} + \dfrac{9-k}{9} \times \dfrac{5+k}{9} & \text{if } j = k, \\ \dfrac{k}{9} \times \dfrac{5+k}{9} & \text{if } j = k-1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus the X_ns indeed form a Markov chain because the same values will be obtained when computing $P(X_{n+1} = j \,/\, X_n = k, X_{n-1} = l_{n-1}, \ldots, X_0 = l_0)$.

The states of the chain are $\{0, 1, 2, 3, 4\}$ and the initial state satisfies

$$q_i = P(X_0 = i) = \begin{cases} 1 & \text{if } i = 2, \\ 0 & \text{if } i \neq 2. \end{cases}$$

2.

$$P = \frac{1}{81} \begin{pmatrix} 45 & 36 & 0 & 0 & 0 \\ 6 & 51 & 24 & 0 & 0 \\ 0 & 14 & 53 & 14 & 0 \\ 0 & 0 & 24 & 51 & 6 \\ 0 & 0 & 0 & 36 & 45 \end{pmatrix}$$

3. The graph is shown in figure 15.13.

Figure 15.13

The chain is irreducible.

4.

- $L(0) = (0, 0, 1, 0, 0)$.
- $L(1) = \dfrac{1}{81}(0, 14, 53, 14, 0)$.
- $L(2) = \dfrac{1}{(81)^2}(6 \times 14, 14(51 + 53), 2 \times 24 \times 14 + 53^2, 14(53 + 51), 6 \times 14)$.

13.14. The graph is shown in figure 15.14.

Figure 15.14

The chain is irreducible and all its states are persistent ; hence there can be no transient or absorbing states.

13.15. Let $T = \{E_1, \ldots, E_k\}$ be the set of transient states, and let $C_1 = \{E_{k+1}, \ldots, E_r\}$ be the irreducible closed set of persistent states. We note that the transition matrix P can be written as

$$P = \begin{pmatrix} M & P_1 \\ 0 & V_1 \end{pmatrix} ,$$

where M is a square $k \times k$ matrix representing the transition probabilities restricted to T, and P_1 is the matrix with k rows and $r - k$ columns defined by

$$M = \begin{pmatrix} p_{1,k+1} & p_{1,k+2} & \cdots & p_{1,k+r} \\ p_{2,k+1} & p_{2,k+2} & \cdots & p_{2,k+r} \\ \vdots & \vdots & \ddots & \vdots \\ p_{k,k+1} & p_{k,k+2} & \cdots & p_{k,k+r} \end{pmatrix} .$$

Note that the matrix M is not stochastic, but verifies

$$\forall i, j, \quad p_{ij} \geq 0 \quad \text{and} \quad \forall i, \quad \sum_{j=1}^{k} p_{ij} \leq 1. \tag{15.3}$$

We say that M is substochastic.
The equation system (13.7) is equivalent to

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_k \end{pmatrix} = M \times \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_k \end{pmatrix} + \begin{pmatrix} p_{1,k+1} + p_{1,k+2} + \cdots + p_{1,k+r} \\ p_{2,k+1} + p_{2,k+2} + \cdots + p_{2,k+r} \\ \vdots \\ p_{k,k+1} + p_{k,k+2} + \cdots + p_{k,k+r} \end{pmatrix} = M \times \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_k \end{pmatrix} + P_1 \times \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}. \tag{15.4}$$

Equations (13.1) tell us that

$$M \times \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + P_1 \times \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} M & P_1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

and hence that $\lambda_1 = \lambda_2 = \cdots = \lambda_k = 1$ is a solution of (15.4).

13.16. 1.

$$P = \begin{array}{c} \\ 1 \\ 2 \\ a \\ s \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & a & s \end{array} \\ \begin{pmatrix} q & p & r & 0 \\ 0 & q & r & p \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

The graph is shown in figure 15.15 below.

Figure 15.15

2. The chain is not irreducible ; the transient states are 1 and 2 and the persistent states are a and s. The persistent states are also absorbing.
3. $\lambda_{i,t}^{n+1} = \sum_{j=1,2} p_{ij} \lambda_{j,t}^{n}$, and hence :

$$\begin{aligned} \lambda_{1,a}^{n+1} &= q\lambda_{1,a}^{n} + p\lambda_{2,a}^{n} \ , \\ \lambda_{2,a}^{n+1} &= q\lambda_{2,a}^{n} \ . \end{aligned}$$

Similarly :

$$\begin{aligned} \lambda_{1,s}^{n+1} &= q\lambda_{1,s}^{n} + p\lambda_{2,s}^{n} \ , \\ \lambda_{2,s}^{n+1} &= q\lambda_{2,s}^{n} \ . \end{aligned}$$

4. $\lambda_{i,t} = \sum_{n \in \mathbb{N}} \lambda_{i,t}^{n}$, and hence, summing the above equalities, $\lambda_{i,t} - \lambda_{i,t}^{1} = \sum_{j=1,2} p_{ij} \lambda_{j,t}$, or, noting that $\lambda_{i,t}^{1} = p_{it}$,

$$\begin{pmatrix} \lambda_{1,a} \\ \lambda_{2,a} \end{pmatrix} = \begin{pmatrix} q & p \\ 0 & q \end{pmatrix} \times \begin{pmatrix} \lambda_{1,a} \\ \lambda_{2,a} \end{pmatrix} + \begin{pmatrix} r \\ r \end{pmatrix}$$

and

$$\begin{pmatrix} \lambda_{1,s} \\ \lambda_{2,s} \end{pmatrix} = \begin{pmatrix} q & p \\ 0 & q \end{pmatrix} \times \begin{pmatrix} \lambda_{1,s} \\ \lambda_{2,s} \end{pmatrix} + \begin{pmatrix} 0 \\ p \end{pmatrix},$$

and hence

$$\begin{pmatrix} 1-q & -p \\ 0 & 1-q \end{pmatrix} \times \begin{pmatrix} \lambda_{1,a} \\ \lambda_{2,a} \end{pmatrix} = \begin{pmatrix} r \\ r \end{pmatrix} \qquad \begin{pmatrix} 1-q & -p \\ 0 & 1-q \end{pmatrix} \times \begin{pmatrix} \lambda_{1,s} \\ \lambda_{2,s} \end{pmatrix} = \begin{pmatrix} 0 \\ p \end{pmatrix} ,$$

thus

$$\begin{pmatrix} \lambda_{1,a} \\ \lambda_{2,a} \end{pmatrix} = \begin{pmatrix} 1-q & -p \\ 0 & 1-q \end{pmatrix}^{-1} \times \begin{pmatrix} r \\ r \end{pmatrix} \qquad \begin{pmatrix} \lambda_{1,s} \\ \lambda_{2,s} \end{pmatrix} = \begin{pmatrix} 1-q & -p \\ 0 & 1-q \end{pmatrix}^{-1} \times \begin{pmatrix} 0 \\ p \end{pmatrix}$$

and, finally,

$$\begin{pmatrix} \lambda_{1,a} \\ \lambda_{2,a} \end{pmatrix} = \begin{pmatrix} \dfrac{1}{1-q} & \dfrac{p}{(1-q)^2} \\ 0 & \dfrac{1}{1-q} \end{pmatrix} \times \begin{pmatrix} r \\ r \end{pmatrix} \qquad \begin{pmatrix} \lambda_{1,s} \\ \lambda_{2,s} \end{pmatrix} = \begin{pmatrix} \dfrac{1}{1-q} & \dfrac{p}{(1-q)^2} \\ 0 & \dfrac{1}{1-q} \end{pmatrix} \times \begin{pmatrix} 0 \\ p \end{pmatrix} .$$

We can check that $\lambda_{1,a} + \lambda_{1,s} = 1$, and similarly that $\lambda_{2,a} + \lambda_{2,s} = 1$.
For $p = 0.6$, $q = 0.3$ and $r = 0.1$, we obtain $\lambda_{1,a} = 0.27$, $\lambda_{1,s} = 0.73$, $\lambda_{2,a} = 0.14$ and $\lambda_{2,s} = 0.86$.
5. The result is clear for $n = 0$; we can easily check the inductive step. We note that

$$\begin{pmatrix} \lambda_{1,t}^{n+1} \\ \lambda_{2,t}^{n+1} \end{pmatrix} = \begin{pmatrix} q & p \\ 0 & q \end{pmatrix} \times \begin{pmatrix} \lambda_{1,t}^{n} \\ \lambda_{2,t}^{n} \end{pmatrix} = M \times \begin{pmatrix} \lambda_{1,t}^{n} \\ \lambda_{2,t}^{n} \end{pmatrix} = M^n \times \begin{pmatrix} \lambda_{1,t}^{1} \\ \lambda_{2,t}^{1} \end{pmatrix} ,$$

or, for $n \geq 1$,

$$\begin{aligned} \lambda_{2,a}^n &= rq^{n-1} , \\ \lambda_{2,s}^n &= pq^{n-1} , \\ \lambda_{1,a}^1 &= r , \end{aligned}$$

and, for $n \geq 2$,

$$\begin{aligned} \lambda_{1,a}^n &= r(q^{n-1} + (n-1)pq^{n-2}) , \\ \lambda_{1,s}^n &= p^2(n-1)q^{n-2} . \end{aligned}$$

6. We have $P(N_i = n) = \lambda_{i,s}^n + \lambda_{i,a}^n$, thus

$$G_i(Z) = \sum_{n\geq 1} (\lambda_{i,s}^n + \lambda_{i,a}^n) Z^n,$$

$$G_2(Z) = \sum_{n\geq 1} (p+r)q^{n-1}Z^n = \frac{(p+r)Z}{1-qZ} ,$$

$$G_1(Z) = \sum_{n\geq 1} rq^{n-1}Z^n + \sum_{n\geq 2} p(p+r)(n-1)q^{n-2}Z^n = \frac{rZ}{1-qZ} + \frac{p(p+r)Z^2}{(1-qZ)^2} .$$

N_i represents the waiting time of the chain in the transient states, given that it started from the initial state i. We verify that

$$\begin{aligned} P(N_i < \infty) &= \sum_{n\in\mathbb{N}} P(N_i = n) = \sum_{n\geq 1} (\lambda_{i,s}^n + \lambda_{i,a}^n) \\ &= G_i(1) = 1 . \end{aligned}$$

We have $G_2(1) = \dfrac{p+r}{1-q} = 1$ and $G_1(1) = \dfrac{(1-q)(p+r)}{(1-q)^2} = 1$.

Lastly, we have $m_i = E(N_i) = (G_i(Z))'(1)$, or by a direct computation,

$$m_2 = E(N_2) = \sum_{n\geq 1} n(p+r)q^{n-1} = \frac{(p+r)}{(1-q)^2} = \frac{1}{1-q} ,$$

$$m_1 = E(N_1) = \sum_{n\geq 1} nrq^{n-1} + \sum_{n\geq 2} n(n-1)p(p+r)q^{n-2} = \frac{r}{(1-q)^2} + \frac{2p(p+r)}{(1-q)^3} = \frac{r+2p}{(1-q)^2} .$$

m_i represents the average waiting time of the chain in the transient states before ultimate absorption at a or s, given that it started from initial state i.

For $p = 0.6$, $q = 0.3$ and $r = 0.1$, we obtain : $m_1 = 2.65$ and $m_2 = 1.43$.

7. The average number of years of study, m_i^s, represents the mean of the r.v. N_i when final success is assumed. Defining event S by : 'the chain, given that it started from the initial state i, eventually reaches state s', we have $m_i^s = E(N_i/S)$, i.e. m_i^s is the mean of the r.v. N_i conditioned by S, or the mean of the r.v. N_i conditioned by final success.

We thus obtain

$$\begin{aligned} m_i^s = E(N_i/S) &= \sum_{n\geq 1} nP(N_i = n/S) = \sum_{n\geq 1} \frac{nP(N_i = n \text{ and } S)}{P(S)} \\ &= \sum_{n\geq 1} \frac{nP(N_i = n \text{ and } X_n = s)}{P(S)} = \sum_{n\geq 1} \frac{n\lambda_{i,s}^n}{\lambda_{i,s}} . \end{aligned}$$

Similarly, defining event A by : 'the chain, given that it started from the initial state i, ends up in state a', we have

$$m_i^a = E(N_i/A) = \sum_{n\geq 1} \frac{n\lambda_{i,a}^n}{\lambda_{i,a}} .$$

m_i^t represents the average waiting time of the chain in the transient states before ultimate absorption at state t, with $t \in \{a, s\}$, given that it started from initial state i.

$$m_2^s = E(N_2/S) = \sum_{n\geq 1} npq^{n-1}/\lambda_{2,s} = \frac{p/(1-q)^2}{p/(1-q)} = \frac{1}{1-q} ,$$

$$m_1^s = E(N_1/S) = \sum_{n\geq 2} n(n-1)p^2q^{n-2}/\lambda_{1,s} = \frac{2p^2/(1-q)^3}{p^2/(1-q)^2} = \frac{2}{1-q} ,$$

and, similarly,

$$m_2^a = E(N_2/A) = \sum_{n\geq 1} nrq^{n-1}/\lambda_{2,a} = \frac{r/(1-q)^2}{r/(1-q)} = \frac{1}{1-q}$$

and

$$\begin{aligned} m_1^a = E(N_1/A) &= \sum_{n\geq 1} nr(q^{n-1} + (n-1)pq^{n-2})/\lambda_{1,a} \\ &= \frac{r(1-q+2p)/(1-q)^3}{r(1-q+p)/(1-q)^2} = \frac{1-q+2p}{(1-q)(1-q+p)} . \end{aligned}$$

for $p = 0.6$, $q = 0.3$ and $r = 0.1$, we obtain : $m_1^s = 2.86$, $m_1^a = 2.09$ and $m_2^s = m_2^a = 1.43$.

8. The Markov chain hypothesis means that the probability of success or failure neither improves nor worsens as years go by ; thus the generic student remains equable whatever the circumstances.

Chapter 14

14.1. We will give only one case of 'optimistic' or minimalist termination (after $n-1$ comparisons) and a case of 'pessimistic' or maximalist termination (after $n+1$ comparisons), but we strongly advise the reader to study other possible cases.

Case 1 ('optimistic' ending, after $n-1$ comparisons) : assume that, just before the two counters k and l meet, we have the following configuration (Figure 15.16) :

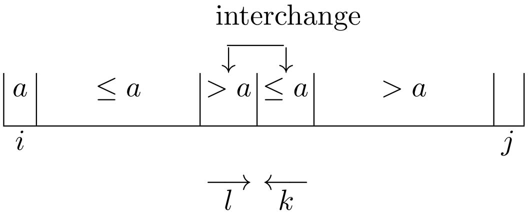

Figure 15.16

in that case the `pivot` procedure will stop after $n-1$ comparisons.

Case 2 ('pessimistic' ending, after $n+1$ comparisons) : Assume that, before counters k and l meet, we have the following configuration (Figure 15.17) :

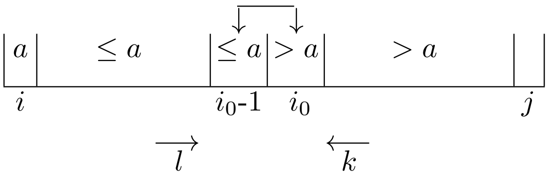

Figure 15.17

in this case the `pivot` procedure will stop after $n+1$ comparisons. Indeed, for $k = i_0$ and $k = i_0 - 1$, $T(k)$ will be compared to the pivot ; then, for $l = i_0 - 1$ and $l = i_0$, $T(l)$ will be compared to the pivot ; each of the elements $T(i_0)$ and $T(i_0 - 1)$ will thus be compared to the pivot **twice** before the procedure `pivot` finally stops.

14.2. 1. First check the case when $T[1,2] = (11,22)$; procedure `Quicksort` will call the `pivot` procedure with $i = 1$, $j = 2$; the `pivot` procedure will set $l := 2$, $k := 2$, $p := 11$; then it will perform the comparisons

- $T(k) > 11$ hence $k := 1$, and
- $T(l) \leq 11$ hence $l := 3$;

and it will stop after these two comparisons, since $l > k$.

Then check the case when $T[1,2] = (22,11)$; the `pivot` procedure will set $l := 2$, $k := 2$, $p := 22$; then it will perform the comparisons

- $T(k) \not> 22$ hence $k := 2$, and
- $T(l) \leq 22$ hence $l := 3$;

as $l < k$, `pivot` will then perform `interchange`$(T(l), T(k))$, and it will stop, since $l > k$; `pivot` also stops here after two comparisons.

2. Similar.

14.3. Writing equations (14.1) for $i = 2, \ldots, n$, and summing these equations, we deduce

$$\forall n \geq 2, \qquad p_n = \frac{(n+1)(n+2)}{2} - 3.$$

14.4. Computations are almost identical (albeit very slightly simpler).

14.5. Similar computations.

14.6. In order to prove termination, we associate with the loop the integral-valued expression v, which strictly decreases each time we execute the body of the `WHILE` loop.

In order to prove that the program computes the greatest common divisor of its arguments, let us introduce the loop invariant $I : \gcd(u, v) = k$, where k is a constant which does not change when we go through the loop. k is thus equal to $gcd(u_0, v_0)$ when the program begins, where u_0 and v_0 are the values read by the program, and k is equal to u_n when exiting the program, where u_n is the value of u when the loop is exited with $v = 0$.

14.7. We have the successive divisions

$$\begin{aligned} 29 &= 3 \times 8 + 5 \\ 8 &= 5 \times 8 + 1 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 1 \times 1 + 1 \end{aligned}$$

hence

$$\frac{8}{29} = \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}$$

$n = 5$.

14.8. We associate with the first loop the value $-n$, which is a strictly positive integer and which strictly decreases at each execution of the `WHILE` loop ; this first loop thus terminates. Similarly, in order to prove that the second `WHILE` loop terminates, we associate with it the value n.

In order to prove that the program indeed computes the power, we associate with it the loop invariant

$$I(a, n, r) \colon r \times a^n = a^k \ ,$$

whose value remains constant at each execution of the `WHILE` loops ; its value when entering the `WHILE` loops is $i = a^k$ and its value when exiting the `WHILE` loops is $i = r$. We thus have that

$r = a^k$. The annotated program is as follows :

```
PROGRAM power
VAR a,k,r : integer
BEGIN
READ a,n                               $integer(a, k)$
n := k
IF n < 0 and a = 0 THEN
   WRITE undefined result
OTHERWISE
   r := 1                               $(n \neq 0) \wedge (r = 1) \wedge (a^n r = a^k)$
   WHILE n < 0 DO
      r := r / a
      n := n+1
   ENDWHILE                            $(n = 0) \wedge (a^n r = a^k)$
   WHILE n > 0 DO
      r := r * a
      n := n-1
   ENDWHILE                            $(n = 0) \wedge (a^n r = a^k)$
   WRITE r                              $(r = a^k)$
ENDIF
END
```

14.9. For proving termination, we use the expression $V = n$. For showing that the program indeed computes the factorial function, we prove the property $p(n) = \big(y = n!\big)$. `Fact` annotated with the final assertions is

```
FUNCTION Fact(n : integer) : y : integer
BEGIN
IF n = 0 THEN y := 1                  $(n = 0) \wedge (y = 1)$
OTHERWISE y := n*Fact(n-1)             $y = n \times (n-1)!$
ENDIF                                 $y = n!$
RETURN(y)                             $y = n!$
END
```

14.10. $V = (n, m)$, and $\mathbb{N}^2$ is endowed with the lexicographic ordering :

- If $n = 0$, the call `Ackermann`(n, m) terminates.
- If $n \neq 0$, `Ackermann`(n, m) calls :
  - `Ackermann`$(n-1, 1)$,
  - `Ackermann`$(n, m-1)$ and
  - `Ackermann`$(n-1,$ `Ackermann`$(n, m-1))$.

We have in the lexicographic ordering,

$$\begin{aligned} & (n-1, 1) < (n, m) \\ & (n, m-1) < (n, m) \\ \text{and} \quad & (n-1, \texttt{Ackermann}(n, m-1)) < (n, m) \end{aligned}$$

14.11. $V = x$.

- If $x = 0$, the first clause of the program terminates with result `Q(x)`$=$*true*.
- Assume that : $\forall y \leq n-1$, `Q(y)` terminates with the result *true*, then for $x = n$, `Q(x)` has for result the result returned by the recursive call of `Q(y)`, with $y = n-1$. Thus `Q(x)` also terminates with the result *true*.

14.12. 1. `pivot` terminates : with the first (resp. second) inner `WHILE` loop we associate the integer k (resp. l), which strictly decreases (resp. strictly increases) at each execution of the loop and is in the well-ordered set $\{i, i+1, \ldots, \sup(i+1, j)\}$, and with the outer `WHILE` loop we associate the integer $k - l$, which strictly decreases at each execution of the loop and is in the well-ordered set $\{-1\} \cup \mathbb{N}$.

`Quicksort` terminates : the length of the list to be sorted strictly decreases at each recursive call.

2. For the partial correctness, we simply give the programs annotated with the final assertions ; each final assertion is written at the right-hand of the instruction after which it is true.

```
PROGRAM pivot
VAR i, j, k, l : integer
VAR T : integer list
BEGIN
READ i,j,T
l := i+1
k := j                                        $integer(i, j, k)$
p := T(i)                                     $q$
WHILE l $\leq$ k DO
   WHILE T(k) $>$ p DO k := k-1 ENDWHILE       $\big(T(k) \leq p\big) \wedge\ q$
   WHILE T(l) $\leq$ p DO l := l+1 ENDWHILE    $\big(T(l) > p\big) \wedge \big(T(k) \leq p\big) \wedge q$
   IF l $<$ k THEN
      interchange (T(l),T(k))
      k := k-1
      l := l+1
   ENDIF                                      $q$
ENDWHILE                                      $(k > l) \wedge q$
interchange (T(i),T(k))
RETURN (k)     $\big((i \leq l' < k) \Longrightarrow \big(T(l') \leq T(k)\big)\big) \wedge \big(k' > k \Longrightarrow \big(T(k') > T(k)\big)\big)$
END
```

where q is the assertion

$$\Big(p = T(i)\Big) \wedge \Big((i \leq l' < l) \Longrightarrow \big(T(l') \leq p\big)\Big) \wedge \Big(k' > k \Longrightarrow \big(T(k') > p\big)\Big)$$

note that q is a loop invariant for the loop `WHILE l` $\leq$ `k ....`

Now let $q(T, i, j)$ be the assertion $i \leq k \leq l \leq j \Longrightarrow \big(T(k) \leq T(l)\big)$, and let q' be the assertion $\big((i \leq l' < k) \Longrightarrow \big(T(l') \leq T(k)\big)\big) \wedge \big(k' > k \Longrightarrow \big(T(k') > T(k)\big)\big)$; the following annotations show the partial correctness of `Quicksort` :

```
PROGRAM Quicksort
VAR i,j,k : integer
VAR T : integer list
BEGIN
READ i,j,T
IF i $<$ j THEN
   pivot(T,i,j ; k)             $q'$
   Quicksort(T, i, k-1)         $q' \wedge q(T, i, k-1)$
   Quicksort(T, k+1, j)         $q' \wedge q(T, i, k-1) \wedge q(T, k+1, j)$
ENDIF                           $q(T, i, j)$
PRINT T
END
```