Solutions to Exercises

In the book of life, the answers aren't in the back

- Charlie Brown.

Chapter 1

Exercise 1.1 (page 20)

1, 2, 4, 6, 7 and 8 are statements, while 3 and 5 are not.

Note that 7 refers to some unspecified utterance by Felix, upon which the truth of this statement depends. Statement 8 however is more complicated: if the sentence it refers to is itself, then there is no consistent way to determine its truth value: if what it says is true, then it must be false; and if what it says is false, then it must be true.

Exercise 1.2 (page 20)

1. This is *not* a valid deduction. There may be some other reason that everyone is leaving the building, e.g., it may be closing for the night.
2. Ideally this would be true, but it is not a valid deduction. It would be valid to deduce that everyone *must* leave the building; however, saying someone (or something) *must* behave in a particular fashion does not make it so; for example, some people may ignore fire alarms, considering fire alarm testing to be a nuisance.
3. This is *not* a valid deduction. The conclusion is no doubt true, as there is surely a rule that states that a train must wait at a red signal; but this rule is not provided in the argument. It might be that the rules for the railway in question do not state that trains must wait at a red light.
4. This is *not* a valid deduction. The conclusion is true, but not for the reasons provided in the two premises.
5. This is *not* a valid deduction. The rook that has already moved might not be the one involved in the castling.

F. Moller, G. Struth, *Modelling Computing Systems*,
Undergraduate Topics in Computer Science,
DOI 10.1007/978-1-84800-322-4,

6. A judgement as to the validity of this deduction cannot be made on purely logical grounds, due to the ambiguity of the language of the city by-law. Specifically, what is the status of the conjunction *"and"* in the by-law? As Charles does not keep any cats, and certainly no more than three, it could be argued that it is within his rights to keep five (or even fifty) dogs on his property. Even worse, the "more than" in "more than three dogs and three cats" might only apply to dogs and not cats, thereby making the keeping of, say, five dogs and any number of cats allowed except when there are exactly three cats.

Exercise 1.3 (page 21)

1. This is a valid deduction.
2. This is a valid deduction. The conclusion that Epimenides is a liar follows from the premises, as a truth-telling Cretan cannot say that all Cretans (including himself) are liars.
3. This is *not* a valid deduction. It *may* be that all Cretans are liars; or it may be that Epimenides is the only liar. Also, from the previous deduction we already know that Epimenides is a liar based on the given premises, so the conclusion – being precisely what Epimenides claims, must be false.
4. This is a valid deduction. We know that the premises imply that Epimenides is a liar, so his claim that all Cretans are liars must be false.
5. This is *not* a valid deduction. Aristotle may be a liar.

Exercise 1.4 (page 23)

1. "The earth does not revolve around the sun."
2. "I have at least one daughter."
3. $2 + 2 > 4$.

Exercise 1.5 (page 24)

1. This is true, as the second disjunct is true (although the first disjunct is false).
2. This is false, as neither disjunct is true.
3. This is true, as both disjuncts are true.

Exercise 1.6 (page 24)

1. Inclusive. This statement implies that Joel could *not* have come in last place if he beat both Felix and Oskar, so he must have lost to one

of them; but he may well have lost to both of them.

2. Exclusive. It is impossible for a light to be both on and off at the same time.
3. Exclusive. The server no doubt intends to offer the guest only one of the beverages. However, if the guest is so odd as to ask for a cup of both (either one cup with a mix of coffee and tea; or two cups, one with coffee and the other with tea), the server will no doubt reluctantly oblige.

Exercise 1.7 (page 25)

1. This is false, as only the second conjunct is true (the first conjunct is false).
2. This is false, as neither conjunct is true.
3. This is true, as both conjuncts are true.

Exercise 1.8 (page 26)

1. AmandaHappy $\Rightarrow$ JoelHappy.
2. JoelHappy $\Rightarrow$ AmandaHappy.
3. AmandaHappy $\Rightarrow$ JoelHappy.

Exercise 1.9 (page 26)

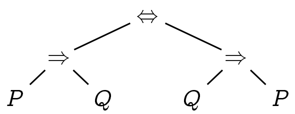
It may well be true that barking dogs don't bite (i.e., Bark $\Rightarrow \neg$Bite), but this says nothing about the habits of dogs that *don't* bark; they may bite, or they might not.

Exercise 1.10 (page 29)

1. $p \mid q \;=\; \neg(p \wedge q)$.
2. $p \downarrow q \;=\; \neg(p \vee q)$.
3. $q \lhd p \rhd r \;=\; (p \wedge q) \;\vee\; (\neg p \wedge r)$.

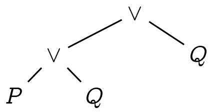
Exercise 1.12 (page 31)

1. $P \Rightarrow Q \;\Leftrightarrow\; Q \Rightarrow P$ has the following syntax tree:

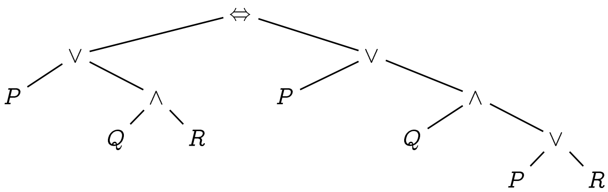


It would be sensible in this example to include redundant parentheses for readability, and to write the formula as $(P \Rightarrow Q) \;\Leftrightarrow\; (Q \Rightarrow P)$

2. This is not a well-formed formula.
3. $(P \vee Q)\ \wedge\ P$ has the following syntax tree:



   Due to the precedence rules, the parentheses are not redundant; $P \vee Q \wedge P$ would be interpreted as $P \vee (Q \wedge P)$.
4. This is not a well-formed formula.
5. $P \vee Q \wedge R\ \Leftrightarrow\ P \vee Q \wedge (P \vee R)$ has the following syntax tree:



   In this case, only one pair of parentheses is redundant; however, it would be sensible to avoid confusion by including all of the redundant parentheses.

Exercise 1.14 (page 33)

This example hints at the many complicated ways that English (or any natural language) can be used to express simple facts. We can draw the conclusion that Lewis Carroll is after by making clear what each of the above assumptions is saying.

Firstly, we introduce propositional variables to represent the different atomic propositions that appear in the argument.

Love:	"Amos Judd loves cold mutton."
Police:	"Amos Judd is a policeman on this beat."
Sup:	"Amos Judd sups with our cook."
Long:	"Amos Judd has long hair."
Poet:	"Amos Judd is a poet."
Prison:	"Amos Judd has been to prison."
Cousin:	"Amos Judd is our cook's cousin."

We wish to deduce, formally and logically, the truth of the atomic proposition Love, which asserts that "Amos Judd loves cold mutton." Notice that we modelled the problem by instantiating the properties of all men to apply only to Amos Judd, as he is the only man in whom we have any interest.

The seven assumptions above then translate into the following propositional formulæ:

1. Police $\Rightarrow$ Sup.
2. Long $\Rightarrow$ Poet.
3. $\neg$Prison.
4. Cousin $\Rightarrow$ Love.
5. Poet $\Rightarrow$ Police.
6. Sup $\Rightarrow$ Cousin.
7. $\neg$Prison $\Rightarrow$ Long.

You should think carefully about each of these translations, and make sure that you understand why they are correct. Assumptions 5 and 6 are particularly tricky. For example, when 5 says that "None but policemen on this beat are poets," it is asserting that in order to be a poet you must be a policeman on this beat. Thus, if Amos Judd is a poet (Poet), then Amos Judd must be a policeman on this beat (Police): Poet $\Rightarrow$ Police. Also, when 7 says that "Men with short hair have all been in prison," it is asserting that anyone who has *not* been to prison must have long hair; thus if Amos Judd has not been to prison ($\neg$Prison), then Amos Judd must have long hair (Long): $\neg$Prison $\Rightarrow$ Long.

We can finally work out the logic, step-by-step, behind the claim that "Amos Judd loves cold mutton" (Love):

	$\neg$Prison	(by 3).
Thus	Long	(by 7, $\neg$Prison $\Rightarrow$ Long).
Thus	Poet	(by 2, Long $\Rightarrow$ Poet).
Thus	Police	(by 5, Poet $\Rightarrow$ Police).
Thus	Sup	(by 1, Police $\Rightarrow$ Sup).
Thus	Cousin	(by 6, Sup $\Rightarrow$ Cousin).
Thus	Love	(by 4, Cousin $\Rightarrow$ Love).

The last line is the conclusion that we sought. (Along the way, we also deduced that Amos Judd has long hair; he is a poet; he is a policeman on this beat; he sups with our cook; and he is a cousin of the cook.)

Exercise 1.15 (page 34)

The first clause states that the right to castle with a particular rook (either the left rook or the right rook) has been lost if either the king or the rook in question has already moved:

$$\begin{aligned}&\mathsf{KingMoved} \;\vee\; \mathsf{LeftRookMoved}\\ &\qquad\Rightarrow\; \neg\mathsf{RightToCastleLeft}.\end{aligned}$$

$$\begin{aligned}&\mathsf{KingMoved} \;\vee\; \mathsf{RightRookMoved}\\ &\qquad\Rightarrow\; \neg\mathsf{RightToCastleRight}.\end{aligned}$$

The second clause states that the player may not castle with a particular rook if the right to do so has been lost, or if there is a piece between the king and the rook in question, or if the square on which the king stands, or the square which it must cross, or the square which it is to occupy is under attack:

$$\begin{array}{l|l} \quad\neg\mathsf{RightToCastleLeft} & \quad\neg\mathsf{RightToCastleRight}\\ \vee\;\; \mathsf{PieceBetweenLeft} & \vee\;\; \mathsf{PieceBetweenRight}\\ \vee\;\; \mathsf{KingAttack} & \vee\;\; \mathsf{KingAttack}\\ \vee\;\; \mathsf{LeftSquareAttack} & \vee\;\; \mathsf{RightSquareAttack}\\ \vee\;\; \mathsf{KingMoveLeftAttack} & \vee\;\; \mathsf{KingMoveRightAttack}\\ \qquad\Rightarrow\; \neg\mathsf{MayCastleLeft} & \qquad\Rightarrow\; \neg\mathsf{MayCastleRight} \end{array}$$

Exercise 1.16 (page 35)

1. We need to express the property that the piece of paper held by each boy has exactly one of the other's names on it, *and* that each name is written on a piece of paper held by exactly one other boy.

   The following proposition p expresses that the piece of paper held by each boy has exactly one of the other's names on it:

   $$\begin{aligned} p \;=\;& (\mathsf{FonJ} \vee \mathsf{OonJ}) \wedge (\neg\mathsf{FonJ} \vee \neg\mathsf{OonJ})\\ \wedge\;& (\mathsf{JonF} \vee \mathsf{OonF}) \wedge (\neg\mathsf{JonF} \vee \neg\mathsf{OonF})\\ \wedge\;& (\mathsf{JonO} \vee \mathsf{FonO}) \wedge (\neg\mathsf{JonO} \vee \neg\mathsf{FonO}). \end{aligned}$$

   For succinctness, we could have used the exclusive-or connective:

   $$p \;=\; (\mathsf{FonJ} \oplus \mathsf{OonJ}) \;\wedge\; (\mathsf{JonF} \oplus \mathsf{OonF}) \;\wedge\; (\mathsf{JonO} \oplus \mathsf{FonO}).$$

   The following proposition q expresses that each name is written on a piece of paper held by exactly one other boy:

$$\begin{aligned} q = \; & (\mathsf{JonF} \lor \mathsf{JonO}) \land (\neg\mathsf{JonF} \lor \neg\mathsf{JonO}) \\ \land \; & (\mathsf{FonJ} \lor \mathsf{FonO}) \land (\neg\mathsf{FonJ} \lor \neg\mathsf{FonO}) \\ \land \; & (\mathsf{OonJ} \lor \mathsf{OonF}) \land (\neg\mathsf{OonJ} \lor \neg\mathsf{OonF}). \end{aligned}$$

Again this could be expressed more succinctly:

$$p = (\mathsf{JonF} \oplus \mathsf{JonO}) \land (\mathsf{FonJ} \oplus \mathsf{FonO}) \land (\mathsf{OonJ} \oplus \mathsf{OonF}).$$

The formula we seek is then $p \land q$.

2. From OonJ we can deduce ¬FonJ from p, from which we can deduce FonO from q, from which we can deduce ¬JonO from p, from which we can deduce JonF from q.

   In summary, we have “Oskar” on Joel’s piece of paper, “Joel” on Felix’s piece of paper, and “Felix” on Oskar’s piece of paper.

Exercise 1.19 (page 40)

If you answer this question quickly, you might conclude that I would reject the white circle. However, this would be wrong if, for example, I had the white square in mind.

In fact, you cannot conclude that I will reject any particular symbol (though you can conclude that I will reject one of them, you just cannot determine which).

Exercise 1.20 (page 40)

Nine.

The point of this old joke is that four and five are nine ***irrespective of the premise of the conditional statement***.

Exercise 1.21 (page 42)

Define the following atomic propositions.

U = **You understand implication.**
P = **You pass the exam.**

The statement translates to $U \Rightarrow P$ which has the following truth table:

U	P	$U \Rightarrow P$
F	**F**	**T**
F	**T**	**T**
T	**F**	**F**
T	**T**	**T**

The *only* scenario in which the above statement can be considered false is if U is true and P is false – that is, if you do not pass the exam despite understanding induction.

Exercise 1.22 (page 44)

Each new variable *doubles* the number of combinations of truth values. Thus, a truth table involving four propositional variables will have 16 rows, and one involving five variables will have 32 rows. In general, a truth table involving n propositional variables will have 2^n rows.

Truth tables grow very quickly with the number of propositional variables. Building truth tables for propositions with many variables, such as in the Amos Judd example (Exercise 1.14), can therefore be frustrating or even infeasible.

Exercise 1.23 (page 44)

1.

P	Q	$\neg$	$(P$	$\Leftrightarrow$	$\neg$	$Q)$
F	F	**T**	F	F	T	F
F	T	**F**	F	T	F	T
T	F	**F**	T	T	T	F
T	T	**T**	T	F	F	T

2.

P	Q	$(P$	$\wedge$	$Q)$	$\vee$	$(\neg$	P	$\wedge$	$\neg$	$Q)$
F	F	F	F	F	**T**	T	F	T	T	F
F	T	F	F	T	**F**	T	F	F	F	T
T	F	T	F	F	**F**	F	T	F	T	F
T	T	T	T	T	**T**	F	T	F	F	T

3.

P	Q	R	S	$(P$	$\wedge$	$Q)$	$\Rightarrow$	$(\neg$	R	$\vee$	$S)$
F	F	F	F	F	F	F	**T**	T	F	T	F
F	F	F	T	F	F	F	**T**	T	F	T	T
F	F	T	F	F	F	F	**T**	F	T	F	F
F	F	T	T	F	F	F	**T**	F	T	T	T
F	T	F	F	F	F	T	**T**	T	F	T	F
F	T	F	T	F	F	T	**T**	T	F	T	T
F	T	T	F	F	F	T	**T**	F	T	F	F
F	T	T	T	F	F	T	**T**	F	T	T	T
T	F	F	F	T	F	F	**T**	T	F	T	F
T	F	F	T	T	F	F	**T**	T	F	T	T
T	F	T	F	T	F	F	**T**	F	T	F	F
T	F	T	T	T	F	F	**T**	F	T	T	T
T	T	F	F	T	T	T	**T**	T	F	T	F
T	T	F	T	T	T	T	**T**	T	F	T	T
T	T	T	F	T	T	T	**F**	F	T	F	F
T	T	T	T	T	T	T	**T**	F	T	T	T

Exercise 1.24 (page 44)

p	q	p	$\Leftrightarrow$	$\neg$	q
F	F	F	**F**	T	F
F	T	F	**T**	F	T
T	F	T	**T**	T	F
T	T	T	**F**	F	T

Exercise 1.25 (page 46)

1. $p \vee (\neg p \wedge q)$ is neither a tautology nor a contradiction:

p	q	p	$\vee$	$(\neg$	p	$\wedge$	$q)$
F	F	F	**F**	T	F	F	F
F	T	F	**T**	T	F	T	T
T	F	T	**T**	F	T	F	F
T	T	T	**T**	F	T	F	T

2. $(p \wedge q) \wedge \neg(p \vee q)$ is a contradiction:

p	q	$(p$	$\wedge$	$q)$	$\wedge$	$\neg$	$(p$	$\vee$	q	$)$
F	F	F	F	F	**F**	T	F	F	F	
F	T	F	F	T	**F**	F	F	T	T	
T	F	T	F	F	**F**	F	T	T	F	
T	T	T	T	T	**F**	F	T	T	T	

3. $(p \Rightarrow \neg p) \Leftrightarrow \neg p$ is a tautology:

p	$(p$	$\Rightarrow$	$\neg$	$p)$	$\Leftrightarrow$	$\neg$	p
F	F	T	T	F	**T**	T	F
T	T	F	F	T	**T**	F	T

4. $(p \Rightarrow q) \Rightarrow p$ is neither a tautology nor a contradiction:

p	q	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	p
F	F	F	T	F	**F**	F
F	T	F	T	T	**F**	F
T	F	T	F	F	**T**	T
T	T	T	T	T	**T**	T

5. $p \Rightarrow (q \Rightarrow p)$ is a tautology:

p	q	p	$\Rightarrow$	$(q$	$\Rightarrow$	$p)$
F	F	F	**T**	F	T	F
F	T	F	**T**	T	F	F
T	F	T	**T**	F	T	T
T	T	T	**T**	T	T	T

Exercise 1.26 (page 47)

The following is a truth table for these three propositions:

Pressure	Height	Land	p	q	r
F	F	F	T	T	T
F	F	T	T	T	T
F	T	F	F	*T*	F
F	T	T	T	T	T
T	F	F	F	*T*	F
T	F	T	T	T	T
T	T	F	F	F	F
T	T	T	T	T	T

The formula p representing the original program code is not equivalent to the formula q representing the first optimisation, as there are interpretations of the atomic propositions which give rise to different truth values for p and q, highlighted in the third and fifth rows of the above truth table.

However, the formulæ p and q are equivalent, as the truth values of these formulæ are the same under all interpretations, and hence the second optimisation is valid.

Exercise 1.27 (page 50)

1. $p \wedge (\neg p \vee q)$

$\Leftrightarrow (p \wedge \neg p) \vee (p \wedge q)$ *(Distributivity)*

$\Leftrightarrow \mathsf{false} \vee (p \wedge q)$ *(Excluded Middle)*

$\Leftrightarrow (p \wedge q) \wedge \mathsf{false}$ *(Commutativity)*

$\Leftrightarrow p \wedge q$ *(Tautology)*

2. $\neg(p \Rightarrow q)$

$\Leftrightarrow \neg(\neg p \vee q)$ *(Implication)*

$\Leftrightarrow \neg\neg p \wedge \neg q$ *(De Morgan)*

$\Leftrightarrow p \wedge \neg q$ *(Double Negation)*

3. $p \Rightarrow (q \vee r)$

$\Leftrightarrow \neg p \vee (q \vee r)$ *(Implication)*

$\Leftrightarrow (\neg p \vee \neg p) \vee (q \vee r)$ *(Idempotence)*

$\Leftrightarrow (\neg p \vee q) \vee (\neg p \vee r)$ *(Associativity, Commutativity)*

$\Leftrightarrow (p \Rightarrow q) \vee (p \Rightarrow r)$ *(Implication)*

4. $p \Rightarrow (q \wedge r)$

$\Leftrightarrow \neg p \vee (q \wedge r)$ *(Implication)*

$\Leftrightarrow (\neg p \vee q) \wedge (\neg p \vee r)$ *(Distributivity)*

$\Leftrightarrow (p \Rightarrow q) \wedge (p \Rightarrow r)$ *(Implication)*

5. $(p \wedge q) \Rightarrow r$

$\Leftrightarrow \neg(p \wedge q) \vee r$ *(Implication)*

$\Leftrightarrow (\neg p \vee \neg q) \vee r$ *(De Morgan)*

$\Leftrightarrow (\neg p \vee \neg q) \vee (r \vee r)$ *(Idempotence)*

$\Leftrightarrow (\neg p \vee r) \vee (\neg q \vee r)$ *(Associativity, Commutativity)*

$\Leftrightarrow (p \Rightarrow r) \vee (q \Rightarrow r)$ *(Implication)*

6. $(p \vee q) \Rightarrow r$

$\Leftrightarrow \neg(p \vee q) \vee r$ *(Implication)*

$\Leftrightarrow (\neg p \wedge \neg q) \vee r$ *(De Morgan)*

$\Leftrightarrow (\neg p \vee r) \wedge (\neg p \vee r)$ *(Distributivity)*

$\Leftrightarrow (p \Rightarrow r) \wedge (q \Rightarrow r)$ *(Implication)*

Chapter 2

Exercise 2.1 (page 59)

1. $\{1, 3, 5, 7\}$.
2. { Tuesday, Thursday, Friday, Saturday }.
3. { Catherine of Aragon, Anne Boleyn, Jane Seymour, Anne of Cleves, Catherine Howard, Catherine Parr }.
4. { Sean Connery, George Lazenby, Roger Moore, Timothy Dalton, Pierce Brosnan, Daniel Craig }.

Exercise 2.2 (page 60)

1. $\{2, 4, 6, 8, 10\}$.
2. $\{1, 2\}$.

Exercise 2.3 (page 60)

1, 3 and 5 are true, while 2 and 4 are false.

Exercise 2.4 (page 60)

$A = E$ and $C = D$.

Exercise 2.5 (page 62)

1 is true, while 2 and 3 are false.

Exercise 2.7 (page 65)

If $R \in R$, then by definition of R we would have $R \notin R$, which cannot be true. Therefore we must have that $R \notin R$.

This is no longer a problem, as $R \notin R$ now means that either $R \notin A$ or $R \in R$; since we know that $R \notin R$, this simply means that $R \notin A$.

Exercise 2.15 (page 69)

The Venn diagram is depicted in Figure 15.2

1. $A \cap C = \{5, 7, 9\}$.
2. $(A \cap B) \cup C = \{3, 5, 6, 7, 8, 9\}$.
3. $A \cap (B \cup C) = \{3, 5, 7, 9\}$.
4. $(A \cup B) \setminus C = \{1, 3, 4\}$.
5. $\overline{(A \cup B)} \cap C = \{6, 8\}$.

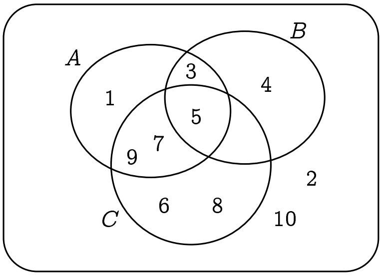


Figure 15.2: Venn diagram for Exercise 2.15.

Exercise 2.16 (page 69)

You can use Venn diagrams to verify these properties.

1. If $A \subseteq B$, then $A \cup B = B$ and $A \cap B = A$.
2. If $A \subseteq B$, then $\overline{B} \subseteq \overline{A}$.
3. $\overline{\overline{A}} = A$.
4. If $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cap B$.
5. If $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

Exercise 2.17 (page 71)

Letting D = Daniel, E = Ella, M = Mia, R = Rhodri and Z = Zoe, we get

$$\begin{aligned}
&\mathcal{P}(\{D, E, M, R, Z\}) \\
&\quad = \{\emptyset, \\
&\qquad \{D\}, \{E\}, \{M\}, \{R\}, \{Z\}, \\
&\qquad \{D, E\}, \{D, M\}, \{D, R\}, \{D, Z\}, \\
&\qquad \{E, M\}, \{E, R\}, \{E, Z\}, \\
&\qquad \{M, R\}, \{M, Z\}, \{R, Z\}, \\
&\qquad \{D, E, M\}, \{D, E, R\}, \{D, E, Z\}, \\
&\qquad \{D, M, R\}, \{D, M, Z\}, \{D, R, Z\}, \\
&\qquad \{E, M, R\}, \{E, M, Z\}, \{E, R, Z\}, \{M, R, Z\}, \\
&\qquad \{D, E, M, R\}, \{D, E, M, Z\}, \{D, E, R, Z\}, \\
&\qquad \{D, M, R, Z\}, \{E, M, R, Z\}, \\
&\qquad \{D, E, M, R, Z\}\}.
\end{aligned}$$

More specifically, there are the following subsets:

- one subset with no elements (the empty set);
- five singleton subsets (one for each element in the set);
- ten subsets with two elements (one for each pair);
- ten subsets with three elements (one for each pair left out);
- five subsets with four elements (one for each element left out); and
- one subset with five elements (the whole set itself).

Exercise 2.18 (page 71)

1. $A = \mathcal{P}(\emptyset) = \{\emptyset\}$ contains 1 element.
2. $B = \mathcal{P}(A) = \{\emptyset, \{\emptyset\}\}$ contains 2 elements.
3. $C = \mathcal{P}(B) = \left\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\right\}$ contains 4 elements.

Exercise 2.19 (page 71)

$\mathcal{P}(A) \cap \emptyset \ = \ \emptyset$ and $\mathcal{P}(A) \cap \{\emptyset\} \ = \ \{\emptyset\}$.

Exercise 2.20 (page 73)

$\bigcap \mathcal{P}_{\text{fin}}(A) \ = \ \emptyset$ and $\bigcup \mathcal{P}_{\text{fin}}(A) \ = \ A$.

Note that the union of infinitely-many finite sets may well be infinite, although the union of finitely-many finite sets will of course be finite.

Exercise 2.23 (page 75)

$(p, q) + (r, s) \ = \ (ps + qr, qs)$ and $(p, q) \times (r, s) \ = \ (pr, qs)$.

Exercise 2.24 (page 76)

Consider the following sets of people:

$$
\begin{aligned}
\mathsf{Love} &= \text{the set of people who love cold mutton.}\\
\mathsf{Police} &= \text{the set of policemen on this beat.}\\
\mathsf{Sup} &= \text{the set of people who sup with our cook.}\\
\mathsf{Long} &= \text{the set of long-haired people.}\\
\mathsf{Poet} &= \text{the set of poets.}\\
\mathsf{NoPrison} &= \text{the set of people who have never been to prison.}\\
\mathsf{Cousin} &= \text{the set of cousins of our cook.}
\end{aligned}
$$

The above seven assumptions then translate to the following set inclusions:

1. $\mathsf{Police} \subseteq \mathsf{Sup}$.

2. Long $\subseteq$ Poet.
3. Amos $\in$ NoPrison.
4. Cousin $\subseteq$ Love.
5. Poet $\subseteq$ Police.
6. Sup $\subseteq$ Cousin.
7. NoPrison $\subseteq$ Long.

We can then conclude that Amos $\in$ LOVE, that is, that Amos Judd loves cold mutton, as follows:

	Amos $\in$ NoPrison	(by 3).
Thus	Amos $\in$ Long	(by 7, NoPrison $\subseteq$ Long).
Thus	Amos $\in$ Poet	(by 2, Long $\subseteq$ Poet).
Thus	Amos $\in$ Police	(by 5, Poet $\subseteq$ Police).
Thus	Amos $\in$ Sup	(by 1, Police $\subseteq$ Sup).
Thus	Amos $\in$ Cousin	(by 6, Sup $\subseteq$ Cousin).
Thus	Amos $\in$ Love	(by 4, Cousin $\subseteq$ Love).

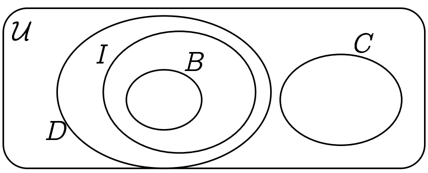
The last line is the conclusion that we sought. (Again, along the way, we also deduced that Amos Judd has long hair; he is a poet; he is a policeman on this beat; he sups with our cook; and he is a cousin of the cook.)

Exercise 2.25 (page 77)

Let B stand for the set of all babies, I for the set of all illogical persons, D for the set of despised persons and C for the set of those persons who can manage a crocodile. Then the premises become :

$$B \subseteq I,\ C \cap D = \emptyset,\ \text{and}\ I \subseteq D$$

which are reflected in the following Venn diagram:



It is clear from this that no baby can manage a crocodile, as a baby would be illogical ($B \subseteq I$) and hence despised ($I \subseteq D$); and no despised person, such as this baby, could manage a crocodile.

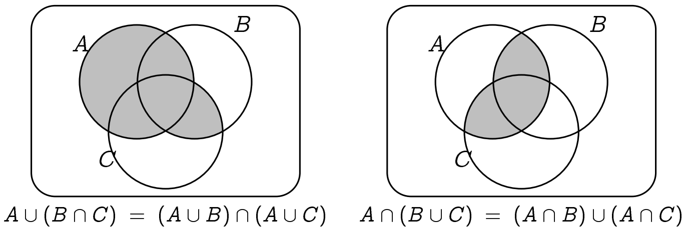
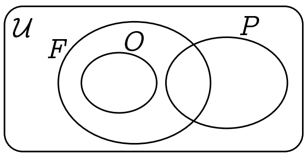


Figure 15.3: Venn diagram for Exercise 2.27.

Exercise 2.26 (page 77)

Consider the following Venn diagram:



F = things full of water

O = oceans

P = ponds

The first premise in the argument says that $O \subseteq F$; and the second premise in the argument says that $P \cap O = \emptyset$. These premises are satisfied by the above Venn diagram. However, the conclusion of the argument says that $P \cap F = \emptyset$, which is not (necessarily) satisfied by the above Venn diagram.

The argument is thus not valid, as the above Venn diagram suggests a counter-example to the argument: there may well be ponds which are not oceans yet are nonetheless full of water.

Exercise 2.27 (page 80)

The two Venn diagrams are depicted in Figure 15.3.

Exercise 2.28 (page 80)

$$
\begin{aligned}
A \cap (\overline{A} \cup B) &= (A \cap \overline{A}) \cup (A \cap B) && \textit{(Distributive Law)} \\
&= \emptyset \cup (A \cap B) && \textit{(Complement Law)} \\
&= (A \cap B) \cap \emptyset && \textit{(Commutative Law)} \\
&= A \cap B && \textit{(Empty Set Law)}
\end{aligned}
$$

Exercise 2.29 (page 81)

- By Associativity, Commutativity and Idempotence, $(A \cap B) \cap A = A \cap B$.
- Letting $X = A \cap B$ and $Y = A$, this says that $X \cap Y = X$.
- This means that $X \subseteq Y$; that is, that $A \cap B \subseteq A$.

Exercise 2.30 (page 83)

1. $A \subseteq B$ if, and only if, $\overline{B} \subseteq \overline{A}$.
2. $A = B$ if, and only if, $(A \subseteq B) \wedge (B \subseteq A)$.

Exercise 2.31 (page 83)

We might naïvely translate the law

$$\neg(P \Rightarrow Q) \quad \Leftrightarrow \quad P \wedge \neg Q$$

into $A \not\subseteq B$ if, and only if, $A \cap \overline{B} = \mathcal{U}$. This law for sets is blatantly false: $A \cap \overline{B} = \mathcal{U}$ can only be true if $A = \mathcal{U}$ and $B = \emptyset$; and this is certainly not the only situation in which we can have $A \not\subseteq B$.

The problem arises from attempting to translate the negation of an implication. To get a correct law for sets corresponding to the given law for propositions, we first simplify the law by negating both sides:

$$P \Rightarrow Q \quad \Leftrightarrow \quad \neg(P \wedge \neg Q)$$

Translating $P \Rightarrow Q$ into $A \subseteq B$, and expressing $\neg(P \wedge \neg Q)$ as $P \wedge \neg Q \Leftrightarrow \mathbf{F}$ gives rise to the following valid law for sets:

$$A \subseteq B \text{ if, and only if, } A \cap \overline{B} = \emptyset.$$

Chapter 3

Exercise 3.3 (page 89)

It is straightforward, if a bit tedious, verifying that each of these laws holds for every combination of values of x, y and z. For example, to verify that the first Distributivity Law

$$x + (y \times z) \quad = \quad (x+y) \times (x+z)$$

is true, we need only use the tables defining $+$ and $\times$ to check the following eight equations are true (one for each of the eight combinations of values for x, y and z):

$$
\begin{aligned}
0 + (0{\times}0) &= (0{+}0) \times (0{+}0) & \qquad 1 + (0{\times}0) &= (1{+}0) \times (1{+}0) \\
0 + (0{\times}1) &= (0{+}0) \times (0{+}1) & \qquad 1 + (0{\times}1) &= (1{+}0) \times (1{+}1) \\
0 + (1{\times}0) &= (0{+}1) \times (0{+}0) & \qquad 1 + (1{\times}0) &= (1{+}1) \times (1{+}0) \\
0 + (1{\times}1) &= (0{+}1) \times (0{+}1) & \qquad 1 + (1{\times}1) &= (1{+}1) \times (1{+}1)
\end{aligned}
$$

The details are omitted.

Exercise 3.9 (page 92)

Since $0{+}1 = 1$ (by Ident1) and $0{\times}1 = 0$ (by Ident2), the Uniqueness of Complement Theorem 3.8 says that $0' = 1$.

But then $1' = (0')' = 0$ by the Involution Law (Theorem 3.9).

An alternative proof which avoid the use of the Uniqueness of Complement Theorem is as follows:

$$
\begin{aligned}
0' &= 0' + 0 && \textit{(Ident1)} & \qquad 1' &= 1' \cdot 1 && \textit{(Ident2)} \\
&= 0 + 0' && \textit{(Comm1)} & &= 1 \cdot 1' && \textit{(Comm2)} \\
&= 1 && \textit{(Compl1)} & &= 0 && \textit{(Compl2)}
\end{aligned}
$$

Exercise 3.10 (page 93)

1. $$
\begin{aligned}
(xy + x'y')' &= (x' + y')(x + y) && \textit{(De Morgan, Involution)} \\
&= xx' + xy' + x'y + yy' && \textit{(Distr, Comm, Assoc)} \\
&= xy' + x'y && \textit{(Compl, Ident, Comm, Assoc)}
\end{aligned}
$$

2. Assume that $x + y = x + z$ and $x' + y = x' + z$. Then

$$
\begin{aligned}
xy &= xx' + xy && \textit{(Compl2, Ident1, Comm1)} \\
&= x(x' + y) && \textit{(Distr2)} \\
&= x(x' + z) && \textit{(Assumption 2)} \\
&= xx' + xz && \textit{(Distr2)} \\
&= xz && \textit{(Compl2, Ident1, Comm1)}
\end{aligned}
$$

   Thus, with Assumption 1, we have from Theorem 3.7 that $y = z$.

3. If $x + y = 0$ then $x' = x + y + x' = (x{+}x') + y = 1 + y = 1$, so $x = 0$.

   By similar reasoning, if $x + y = 0$ then $y = 0$.

4. If $x = 0$ then $x' = 1$ and thus $y = 0y' + 1y = xy' + x'y$.

   Conversely, if $y = xy' + x'y$ for all y, then taking $y = 0$, and thus $y' = 1$, we get that $0 = xy' + x'y = x1 + x'0 = x$.

Exercise 3.11 (page 94)

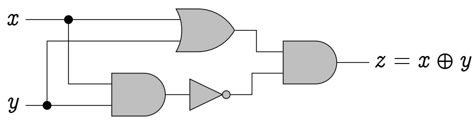
1. $\big((x{+}y)(x'{+}y')\big)' = (x{+}y')(x'{+}y)$.
2. If $xy = xz$ and $x'y = x'z$ then $y = z$.
3. If $xy = 1$ then $x = y = 1$.
4. $x = 1$ if, and only if, $y = (x{+}y')(x'{+}y)$ for all y.

Exercise 3.14 (page 99)

We start by expressing $x \oplus y$ in terms of the three basic operations:

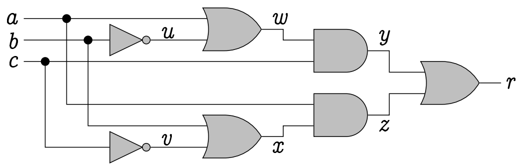
$$x \oplus y \quad = \quad (x + y)(xy)'$$

The circuit for this is then as follows:



Exercise 3.15 (page 99)

We start by annotating the diagram with variables for all of the intermediate values which are computed:



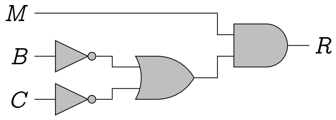
We can then calculate the intermediate and final values by considering their Boolean expressions:

$$\begin{aligned} u &= b' \\ v &= c' \\ w &= a + u \\ x &= b + v \\ y &= wc \\ z &= ax \\ r &= y + z \end{aligned}$$

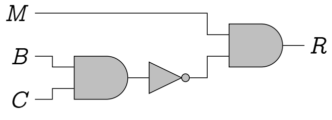
a	b	c	u	v	w	x	y	z	r
0	0	0	1	1	1	1	0	0	0
0	0	1	1	0	1	0	1	0	1
0	1	0	0	1	0	1	0	0	0
0	1	1	0	0	0	1	0	0	0
1	0	0	1	1	1	1	0	1	1
1	0	1	1	0	1	0	1	0	1
1	1	0	0	1	1	1	0	1	1
1	1	1	0	0	1	1	1	1	1

Exercise 3.16 (page 99)

The output R to be computed is given by the formula $R = M(B' + C')$, which by De Morgan's Law can be rewritten as $R = M(BC)'$. Thus either of the following two Boolean circuits will give a valid implementation.



$R = M(B' + C')$



$R = M(BC)'$

Exercise 3.17 (page 102)

29 + 22 = 51.

Chapter 4

Exercise 4.2 (page 111)

1. $\{x : \mathit{Even}(x)\} = \{x \in \mathbb{Z} : x \text{ is even}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.$
2. $\{x : \mathit{EvenPrime}(x)\} = \{2\}.$
3. $\{x : \mathit{DeadlySin}(x)\} = \{\mathit{lust}, \mathit{gluttony}, \mathit{greed}, \mathit{sloth}, \mathit{wrath}, \mathit{envy}, \mathit{pride}\}.$
4. $\{x : \mathit{Sum}(x, y, z)\} = \{(x, y, z) \in \mathbb{Z}^3 : x + y = z\}$
5. $\{x : \mathit{Sum}(u, 5, v)\} = \{(u, v) \in \mathbb{Z}^2 : u + 5 = v\} = \{\ldots, (-3, 2), (-2, 3), (-1, 4), (0, 5), (1, 6), (2, 7), (3, 8), \ldots\}.$

Exercise 4.5 (page 115)

1. $\forall x \, \forall y \, \big(B(x) \wedge F(y) \Rightarrow L(x, y) \big).$
2. $\forall x \, \forall y \, \big(B(x) \wedge L(x, y) \Rightarrow F(y) \big).$
3. $\forall x \, \forall y \, \big(F(y) \wedge L(x, y) \Rightarrow B(x) \big).$

Exercise 4.7 (page 117)

1. $\forall x \, \big(\mathit{Male}(x) \oplus \mathit{Female}(x) \big).$
2. $\forall x \, \big(\exists y \, \mathit{Mother}(x, y) \Rightarrow \mathit{Parent}(x, y) \wedge \mathit{Female}(x) \big).$

3. $\forall x\,\exists m\,\exists f\,\forall y\,\big((Mother(y,x)\ \Leftrightarrow\ y{=}m)\ \wedge\ (Father(y,x)\ \Leftrightarrow\ y{=}f)\big)$.
4. $\forall x\,\forall y\,\big(\,Sibling(x,y)\ \Rightarrow\ \forall z\,(\,Parent(z,x)\ \Leftrightarrow\ Parent(z,y)\,)\,\big)$.
5. $\forall x\,\forall y\,\big(\,Cousin(x,y)\ \Rightarrow$
   $\exists u\,\exists v\,(\,Parent(u,x)\ \wedge\ Parent(v,y)\ \wedge\ Sibling(u,v)\,)\,\big)$.

Exercise 4.8 (page 117)

The premise of the argument translates into

$$\forall h\big(\,Horse(h) \Rightarrow Animal(h)\,\big)$$

which says that any thing h which is a horse is an animal.

The conclusion of the argument translates into

$$\forall x\big(\,\exists h(Horse(h) \wedge Head(x,h))\ \Rightarrow\ \exists a(Animal(a) \wedge Head(x,a))\,\big)$$

which says that any thing x which is the head of some horse h is the head of some animal a.

This argument is valid: for suppose x is the head of some horse h (Black Beauty, say). Since the premise says that all horses are animals, this particular horse h (Black Beauty) is an animal; and hence this thing x is the head of some animal a, namely h (Black Beauty).

Exercise 4.9 (page 120)

1. $\exists! c\,(\,T(Alice,c)\ \wedge\ T(Bob,c)\,)$
2. $\exists c_1\,\big(\,T(Alice,c_1)\ \wedge\ T(Bob,c_1)$
   $\wedge\ \exists! c_2\,(\,T(Alice,c_2)\ \wedge\ T(Bob,c_2)\ \wedge\ c_1 \neq c_2\,)\,\big)$

Exercise 4.10 (page 121)

1. $\exists x\, LikesMaths(x)$, where $LikesMaths(x)$ = "x likes maths".

   Its negation is (b).

   (a) $\exists x\,\neg LikesMaths(x)$.
   (b) $\forall x\,\neg LikesMaths(x)$.
   (c) $\forall x\, LikesMaths(x)$.

2. $\forall x\,(\,Fur(x)\ \wedge\ Tail(x)\,)$, where $Fur(x)$ = "x has fur" and $Tail(x)$ = "x has a tail".

   Its negation is (c).

   (a) $\neg\exists x\,(\,Fur(x)\ \wedge\ Tail(x)\,)$.

(b) $\exists x\,(\neg Fur(x) \;\wedge\; \neg Tail(x))$.
(c) $\exists x\,(\neg Fur(x) \;\vee\; \neg Tail(x))$.

3. $\forall x\,(\neg Vaccinated(x) \;\Rightarrow\; Sick(x))$, where $Vaccinated(x) =$ "x has been vaccinated" and $Sick(x) =$ "x got Sick".

   Its negation is (c).

   (a) $\forall x\,(Vaccinated(x) \;\Rightarrow\; \neg Sick(x))$.
   (b) $\exists x\,(Vaccinated(x) \;\wedge\; Sick(x))$.
   (c) $\exists x\,(\neg Vaccinated(x) \;\wedge\; \neg Sick(x))$.

Exercise 4.12 (page 125)

Let $Loves(x, y) =$ "x loves y", where the universe of discourse is the set of people.

1. *Everybody loves somebody*: $\forall x\, \exists y\, Loves(x, y)$.
   Somebody is loved by everybody: $\exists x\, \forall y\, Loves(y, x)$.

   These English statements are ambiguous, as each may be interpreted as saying precisely what the other is saying. However, the likely interpretation for each is as formalised in predicate logic above.

   This argument is *not* valid. For example, perhaps Alice only loves herself, but everyone else loves Bob (including Bob himself); in this scenario, the premise is true, but the conclusion is false.

2. *Somebody loves everybody*: $\exists x\, \forall y\, Loves(x, y)$.
   Everybody is loved by somebody: $\forall x\, \exists y\, Loves(y, x)$.

   This argument is valid. The premise of the argument says that there is some person – Theresa say – who loves everybody. This means that the conclusion of the argument must be true as well: everybody *is* loved by someone, in particular by Theresa.

Exercise 4.13 (page 127)

2	9	8	1	3	5	4	6	7
4	1	7	8	9	6	2	3	5
3	6	5	2	7	4	9	8	1
7	4	9	5	2	3	6	1	8
8	2	3	9	6	1	7	5	4
6	5	1	7	4	8	3	9	2
1	3	4	6	8	7	5	2	9
5	7	2	3	1	9	8	4	6
9	8	6	4	5	2	1	7	3

Chapter 5

Exercise 5.2 (page 134)

Fact 15.14

$A \cup B \subseteq C \;\Rightarrow\; A \subseteq C \;\wedge\; B \subseteq C.$

Proof: Assume that $A \cup B \subseteq C$; we must show that $A \subseteq C \;\wedge\; B \subseteq C$. This means that we must show both $A \subseteq C$ and $B \subseteq C$.

We consider $A \subseteq C$ first. By the definition of the set inclusion $A \subseteq C$, we choose an arbitrary element $x \in A$ and we show that $x \in C$. Since $x \in A$, it is thus also the case that $x \in A \cup B$. Hence, by our assumption, $x \in C$. We have thus shown that $A \subseteq C$.

The proof that $B \subseteq C$ is very similar. □

Exercise 5.3 (page 136)

Fact: If a and b are both odd integers, then ab is an odd integer.

Proof: Assume that a and b are odd integers.

An odd integer is one more than twice an integer.

Thus $a = 2p+1$ and $b = 2q+1$ for some integers p and q.

$$\begin{aligned} \text{Hence } ab &= (2p+1)(2q+1) = 4pq + 2p + 2q + 1 \\ &= 2(2pq + p + q) + 1 \\ &= 2k+1 \text{ for the integer } k = 2pq + p + q. \end{aligned}$$

Therefore, ab is an odd integer. □

Exercise 5.5 (page 138)

If the sum of the digits of a number is divisible by 3, then that number itself is divisible by 3.

- The sum of the digits of 45 is $4+5 = 9$, which is divisible by 3; so by modus ponens, 45 itself is divisible by 3.
- The sum of the digits of 9 839 853 is $9+8+3+9+8+5+3 = 45$, which is divisible by 3; so by modus ponens, 9 839 853 itself is divisible by 3.

Exercise 5.9 (page 141)

Fact: There is no smallest positive rational number.

Proof: Assume to the contrary that $a > 0$ is the smallest rational number.

> Then $b = a/2$ is a positive rational number which is smaller than a, contradicting our assumption that a is the smallest such number.

Hence there cannot be a smallest positive rational number. □

Exercise 5.10 (page 142)

Fact: Every integer greater than 1 can be written as a product of prime numbers.

Proof: Assume to the contrary that not all integers greater than 1 can be written as a product of prime numbers,

> Let n be the smallest such integer; thus, every smaller integer greater than 1 can be written as a product of primes.
>
> By assumption, n cannot be prime, so $n = pq$ where p and q are two smaller integers greater than 1.
>
> Since p and q are smaller than n, they must themselves each be a product of primes.
>
> But then n must be a product of primes as well. namely the product of those primes making up p and q, contradicting the definition of n.

Hence every integer greater than 1 can be written as a product of prime numbers. □

Exercise 5.13 (page 145)

Fact: If a and b are integers and ab is even, then either a is even or b is even.

Proof: Assume that a and b are integers and that ab is even. That is, $ab = 2p$ for some integer p.

Suppose that a is odd; that is, suppose that $a = 2q+1$ for some integer q.

> Then $ab = (2q+1)b = 2qb + b$; and since $ab = 2p$, this means that $2p = 2qb + b$, and thus that $b = 2p - 2qb = 2(p - qb)$.
>
> Since $p - qb$ is an integer, this means that b must be even.

Thus, if a is *not* even, then b must be even; that is, either a or b is even.

Exercise 5.14 (page 146)

Fact: If $A \subseteq B$ then either $x \notin A$ or $x \in B$.

Proof: Assume that $A \subseteq B$.

Suppose that $x \in A$; that is, that it is *not* the case that $x \notin A$.

Then since $A \subseteq B$, we must have that $x \in B$.

Thus, either $x \notin A$, or $x \in B$.

Exercise 5.15 (page 147)

Fact: For real numbers a and b, $|a+b| \leq |a|+|b|$.

Proof: Since $|a+b| = |b+a|$, we can assume without any loss of generality that $|a| \geq |b|$.

- Either a and b have the same sign – that is, they are both nonnegative (i.e., greater than or equal to 0) or they are both negative;
- or a and b have opposite signs – that is, one is nonnegative and the other is negative.

We shall consider these two cases in turn.

- If a and b have the same sign, then $|a+b| = |a|+|b| \leq |a|+|b|$.
- If a and b have opposite signs, then $|a+b| = |a|-|b| \leq |a|+|b|$.

In either case, the result is true. □

Exercise 5.16 (page 147)

Fact: If n is an integer, then the final digit of n^2 is 0, 1, 4, 5, 6 or 9.

Proof: We can prove this by breaking down the problem into cases depending on the final digit of n:

- If the final digit of n is 0, then the final digit of n^2 will be 0.
- If the final digit of n is 1 or 9, then the final digit of n^2 will be 1.
- If the final digit of n is 2 or 8, then the final digit of n^2 will be 4.
- If the final digit of n is 3 or 7, then the final digit of n^2 will be 9.
- If the final digit of n is 4 or 6, then the final digit of n^2 will be 6.
- If the final digit of n is 5, then the final digit of n^2 will be 5.

This exhausts all possibilities for the final digit of n, and hence the result must be true. □

Exercise 5.17 (page 147)

Saying that it is *not* the case that $x \neq 7$ and $y \neq 8$ means that either $x = 7$ or $y = 8$, *not* that both of these equalities holds.

Exercise 5.18 (page 149)

Fact: If A and $B \setminus C$ are disjoint then $A \cap B \subseteq C$.

Proof: Assume that A and $B \setminus C$ are disjoint. From this assumption, we need to prove that $A \cap B \subseteq C$; that is, that for any x, if $x \in A \cap B$ then $x \in C$:

$$\forall x\,(x \in A \cap B \;\Rightarrow\; x \in C).$$

To this end, let a be an arbitrary value.

> To show that $a \in A \cap B \Rightarrow a \in C$, we assume that $a \in A \cap B$ and prove from this assumption that $a \in C$.
>
> Assume then that $a \in A \cap B$; that is, that $a \in A$ and $a \in B$.
>
> Since A and $B \setminus C$ are disjoint (from a premise of the proposition) and $a \in A$, we must have that $a \notin B \setminus C$.
>
> But since $a \in B$, $a \notin B \setminus C$ means we must have that $a \in C$. □

Exercise 5.19 (page 151)

Fact: $\forall\, x{>}0\, \exists\, y\, (\, y(y{+}1) = x\,)$.

Proof: Let $x > 0$ be arbitrary, and let $y \;=\; \frac{1}{2}\Big(-1 + \sqrt{1{+}4x}\,\Big)$.

$$\begin{aligned} \text{Then}\; y(y{+}1) \;&=\; \tfrac{1}{2}\Big(-1 + \sqrt{1{+}4x}\,\Big)\,\Big(\tfrac{1}{2}\Big(-1 + \sqrt{1{+}4x}\,\Big) + 1\Big) \\ &=\; \tfrac{1}{4}\Big(\sqrt{1{+}4x} - 1\Big)\Big(\sqrt{1{+}4x} + 1\Big) \\ &=\; \tfrac{1}{4}\Big((1{+}4x) - 1\Big) \;=\; \tfrac{1}{4}(4x) \;=\; x \end{aligned}$$

□

Where did this value of y come from? Given $x{>}0$, we want a value y satisfying $y(y{+}1) = x$, or in other words, by expanding and rewriting this equation, a solution y to the quadratic equation

$$y^2 + y - x \;=\; 0.$$

The quadratic formula tells us that the two values for y which solve this equation are

$$y \;=\; \frac{-1 \;\pm\; \sqrt{1+4x}}{2}.$$

Only one of these two solutions is positive as required, namely

$$y = \tfrac{1}{2}\big(-1 + \sqrt{1+4x}\,\big).$$

Exercise 5.20 (page 152)

Fact: $\exists x\,\big(P(x) \vee Q(x)\big) \;\Leftrightarrow\; \exists x\,P(x) \;\vee\; \exists x\,Q(x)$.

Proof: $(\Rightarrow)$ Suppose $\exists x\,\big(P(x) \vee Q(x)\big)$.

Then $P(a) \vee Q(a)$ holds for some a.

For this value a, either $P(a)$ holds or $Q(a)$ holds.

- If $P(a)$ holds, then $\exists x\,P(x)$, and thus $\exists x\,P(x) \;\vee\; \exists x\,Q(x)$.
- If $Q(a)$ holds, then $\exists x\,Q(x)$, and thus $\exists x\,P(x) \;\vee\; \exists x\,Q(x)$.

In either case, $\exists x\,P(x) \;\vee\; \exists x\,Q(x)$.

$(\Leftarrow)$ Suppose $\exists x\,P(x) \;\vee\; \exists x\,Q(x)$.

Then either $\exists x\,P(x)$ holds, or $\exists x\,Q(x)$ holds.

- If $\exists x\,P(x)$ holds, then $P(a)$ holds for some value a.
  For this a, $P(a) \vee Q(a)$ holds, and so $\exists x\,\big(P(x) \vee Q(x)\big)$.
- If $\exists x\,Q(x)$ holds, then $Q(a)$ holds for some value a.
  For this a, $P(a) \vee Q(a)$ holds, and so $\exists x\,\big(P(x) \vee Q(x)\big)$.

Thus, in either case, $\exists x\,\big(P(x) \vee Q(x)\big)$. □

Exercise 5.22 (page 153)

Fact: There is a unique set A such that, for every set B, $A \cup B = B$.

Proof: To show existence of such a set, we simply note that the empty set $\emptyset$ clearly has the desired property, as $\emptyset \cup B = B$ for every set B.

To show that $\emptyset$ is the only set with this property, assume that some set A satisfies this property; in particular, taking $B = \emptyset$, this means that $A \cup \emptyset = \emptyset$. But then $A = A \cup \emptyset = \emptyset$. □

Chapter 6

Exercise 6.2 (page 158)

1. $\mathsf{range}(\mathsf{score}) = \{46, 54, 59, 64, 68, 75, 78, 88, 92, 100\}$.
2. $\mathsf{score}^{-1}(\{n \in \mathbb{N} : n \geq 70\})$.

Exercise 6.3 (page 158)

1. *Mother* is a function as every person has one and exactly one (biological) mother.
2. *Parent* is not a function as people have two parents not one.
3. *Child* is not a function as a person may have any number of children.
4. *FirstBornChild* is not a function as a person may have no children.

Exercise 6.4 (page 160)

$$\mathsf{graph}(f) = \{ (1, c), (2, a), (3, c) \}.$$

Exercise 6.5 (page 161)

1. The function score is *not* one-to-one as, for example, score(Collins) = score(Parker). Also, score(Evans) = score(Williams).
2. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is *not* one-to-one as, for example, $f(-1) = f(1)$. (In fact, $f(x) = f(-x)$ for any value $x \in \mathbb{R}$.)
3. The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$ *is* one-to-one.

Exercise 6.6 (page 161)

1. The function score is *not* onto as, for example, no one has scored 0.
2. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is *not* onto as $f(x) \geq 0$ for all $x \in \mathbb{R}$ so, for example, for no $x \in \mathbb{R}$ do we have $x^2 = -1$.
3. The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$ is *not* onto as, for example, for no $x \in \mathbb{N}$ do we have $x^2 = 3$.

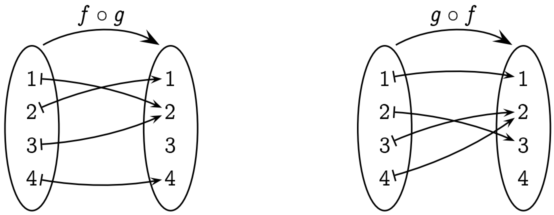
Exercise 6.7 (page 161)

- f_1 is one-to-one but not onto, as there is an element of the codomain (the third element from the top) which is not in the range of the function.
- f_2 is onto but not one-to-one, as f_2 maps two elements of the domain (the top and bottom elements) to the same element of the codomain (the middle of the three elements).
- f_3 is not one-to-one, as it maps two elements of the domain (the first two elements) to the same element of the codomain (the third element from the top); nor is f_3 onto, as there is an element of the codomain (the second element from the top) which is not in the range of the function.
- f_4 is both one-to-one and onto,

Exercise 6.8 (page 163)

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
x	i	e	p	d	t	o	v	z	s	b	m	j
n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
w	r	q	n	u	f	c	h	l	g	y	a	k

Exercise 6.9 (page 164)



Exercise 6.10 (page 165)

If $f : A \to B$ and $g : B \to C$ are both bijections, then they are both one-to-one and onto. Therefore, $g \circ f : A \to C$ is both one-to-one (by Theorem 6.9) and onto (by Theorem 6.10), and thus it is a bijection.

Exercise 6.11 (page 165)

Let $a \in A$ be arbitrary. By the definition of the inverse of a bijection, Definition 6.7 (page 162), if $f^{-1}(f(a)) = x$ then $f(x) = f(a)$. Since f is one-to-one, this means that $x = a$. Hence $f^{-1}(f(a)) = a$ for any $a \in A$; that is, $f^{-1} \circ f = \mathrm{id}_A$.

Let $b \in B$ be arbitrary. Again by Definition 6.7, if $f(f^{-1}(b)) = y$ then $y = b$. Hence $f(f^{-1}(b)) = b$ for any $b \in B$; that is, $f \circ f^{-1} = \mathrm{id}_B$.

Exercise 6.12 (page 166)

$$\begin{aligned}\Big(h \circ (g \circ f)\Big)(x) = h\Big((g \circ f)(x)\Big) &= h\Big(g(f(x))\Big) \\ = (h \circ g)(f(x)) &= \Big((h \circ g) \circ f\Big)(x).\end{aligned}$$

Exercise 6.14 (page 170)

$$f^{-1}(n) = \begin{cases} 2n-1, & \text{if } n > 0; \\ -2n, & \text{if } n \leq 0 \end{cases}$$

Exercise 6.15 (page 170)

Take $h = g \circ f^{-1}$ which, by Exercise 6.10, is guaranteed to be a bijection.

Exercise 6.16 (page 172)

Given the bijection $f : \mathbb{N} \to \mathbb{Q}^+$ from Example 6.15, the function $g : \mathbb{N} \to \mathbb{Q}$ defined by

$$g(n) = \begin{cases} 0, & \text{if } n = 0, \\ f\left(\frac{n-1}{2}\right), & \text{if } n > 0 \text{ is odd}, \\ -f\left(\frac{n}{2}\right), & \text{if } n > 0 \text{ is even}, \end{cases}$$

is a bijection.

Exercise 6.17 (page 173)

Consider any element $a \in A$.

- If $a \in B$ then by definition of B, $a \notin f(a)$, so $B \neq f(a)$.
- If $a \notin B$ then by definition of B, $a \in f(a)$, so again $B \neq f(a)$.

We thus have that $B \neq f(a)$ for every $a \in A$, that is, f cannot be onto.

Exercise 6.18 (page 174)

Let $S = \{1, 2\}$, and let $f : \mathcal{P}(S) \to \mathcal{P}(S)$ be defined by:

$$f(\emptyset) = f(\{1\}) = \{1\} \quad \text{and} \quad f(\{2\}) = f(S) = \{2\}.$$

The subsets $\{1\}$ and $\{2\}$ are clearly fixed points of f, and are the only fixed points of f. As $\{1\} \not\subseteq \{2\}$ and $\{2\} \not\subseteq \{1\}$, these are neither greatest nor least fixed points.

Exercise 6.20 (page 176)

1. If $S \subseteq T$, then

$$\begin{aligned} f(S) &= \{0\} \cup \{n+2 : n \in S\} \\ &\subseteq \{0\} \cup \{n+2 : n \in T\} = f(T). \end{aligned}$$

2.

$$\begin{aligned} f(\emptyset) &= \{0\} & f(\mathbb{N}) &= \mathbb{N} \setminus \{1\} \\ f^2(\emptyset) &= \{0, 2\} & f^2(\mathbb{N}) &= \mathbb{N} \setminus \{1, 3\} \\ f^3(\emptyset) &= \{0, 2, 4\} & f^3(\mathbb{N}) &= \mathbb{N} \setminus \{1, 3, 5\} \\ &\vdots & &\vdots \\ f^n(\emptyset) &= \{0, 2, \ldots, 2n-2\} & f^n(\mathbb{N}) &= \mathbb{N} \setminus \{1, 3, \ldots, 2n-1\} \end{aligned}$$

3. L = G = {0, 2, 4, 6, ...}.

Chapter 7

Exercise 7.1 (page 180)

1. $Q = \{r \in \mathit{BondFilms} : r \text{ was directed by Lewis Gilbert}\}$
   $= \{r03, r06, r07\}.$
2. $Q = \{r \in \mathit{BondFilms} : r \text{ was released in the 1970s}\}$
   $= \{r05, r06, r07\}.$

Exercise 7.3 (page 183)

StarsIn = { (Sean Connery, Dr. No),
(Sean Connery, Thunderball),
(Sean Connery, You Only Live Twice),
(George Lazenby, On Her Majesty's Secret Service),
(Sean Connery, Diamonds Are Forever),
(Roger Moore, The Spy Who Loved Me),
(Roger Moore, Moonraker),
(Roger Moore, For Your Eyes Only),
(Sean Connery, Never Say Never Again),
(Roger Moore, Octopussy),
(Roger Moore, A View to a Kill),
(Timothy Dalton, The Living Daylights),
(Timothy Dalton, Licence to Kill),
(Pierce Brosnan, Golden Eye),
(Pierce Brosnan, Tomorrow Never Dies),
(Pierce Brosnan, The World Is Not Enough),
(Pierce Brosnan, Die Another Day),
(Daniel Craig, Casino Royale),
(Daniel Craig, Quantum of Solace),
(Daniel Craig, Skyfall) }.

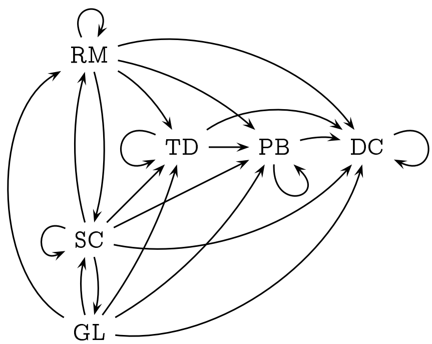
Exercise 7.5 (page 184)

Letting SC, GL, TD, PB, and DC stand for Sean Connery, George Lazenby, Roger Moore, Timothy Dalton, Pierce Brosnan and Daniel Craig, respectively, the binary relation *Before* consists of the following pairs:

Before = { (SC, SC), (SC, GL), (SC, RM), (SC, TD),

$$\begin{array}{llll}
(\mathrm{SC},\mathrm{PB}), & (\mathrm{SC},\mathrm{DC}), & (\mathrm{GL},\mathrm{SC}), & (\mathrm{GL},\mathrm{RM}), \\
(\mathrm{GL},\mathrm{TD}), & (\mathrm{GL},\mathrm{PB}), & (\mathrm{GL},\mathrm{DC}), & (\mathrm{RM},\mathrm{SC}), \\
(\mathrm{RM},\mathrm{RM}), & (\mathrm{RM},\mathrm{TD}), & (\mathrm{RM},\mathrm{PB}), & (\mathrm{RM},\mathrm{DC}), \\
(\mathrm{TD},\mathrm{TD}), & (\mathrm{TD},\mathrm{PB}), & (\mathrm{TD},\mathrm{DC}), & (\mathrm{PB},\mathrm{PB}), \\
 & & (\mathrm{PB},\mathrm{DC}), & (\mathrm{DC},\mathrm{DC}) \ \}.
\end{array}$$

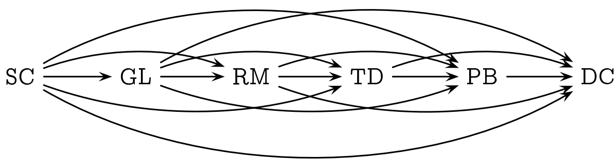
This binary relation can be visualised as follows:



The binary relation *FirstBefore* consists of the following pairs:

$$\begin{array}{rcl}
\mathit{FirstBefore} & = & \{\ (\mathrm{SC},\mathrm{GL}),\ (\mathrm{SC},\mathrm{RM}),\ (\mathrm{SC},\mathrm{TD}), \\
 & & (\mathrm{SC},\mathrm{PB}),\ (\mathrm{SC},\mathrm{DC}),\ (\mathrm{GL},\mathrm{RM}), \\
 & & (\mathrm{GL},\mathrm{TD}),\ (\mathrm{GL},\mathrm{PB}),\ (\mathrm{GL},\mathrm{DC}), \\
 & & (\mathrm{RM},\mathrm{TD}),\ (\mathrm{RM},\mathrm{PB}),\ (\mathrm{RM},\mathrm{DC}), \\
 & & (\mathrm{TD},\mathrm{PB}),\ (\mathrm{TD},\mathrm{DC}),\ (\mathrm{PB},\mathrm{DC})\ \}.
\end{array}$$

This binary relation can be visualised as follows:

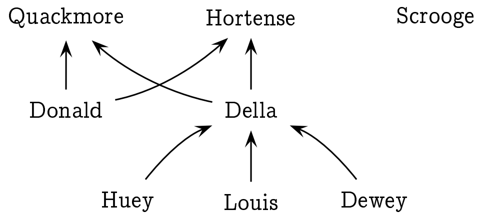


Exercise 7.6 (page 185)

$$\begin{array}{rl}
\mathit{Child} = & \{\,(\text{Donald},\ \text{Quackmore}),\ (\text{Donald},\ \text{Hortense}), \\
 & (\text{Della},\ \text{Quackmore}),\ (\text{Della},\ \text{Hortense}), \\
 & (\text{Huey},\ \text{Della}),\ (\text{Louis},\ \text{Della}),\ (\text{Dewey},\ \text{Della})\,\}.
\end{array}$$

$$\begin{aligned} \mathit{Brother} &= \{ \text{(Scrooge, Hortense), (Donald, Della),} \\ &\quad \text{(Huey, Louis), (Huey, Dewey), (Louis, Huey),} \\ &\quad \text{(Louis, Dewey), (Dewey, Huey), (Dewey, Louis)} \}. \\ \mathit{Sister} &= \{ \text{(Hortense, Scrooge), (Della, Donald)} \}. \\ \mathit{Sibling} &= \{ \text{(Scrooge, Hortense), (Hortense, Scrooge),} \\ &\quad \text{(Donald, Della), (Della, Donald),} \\ &\quad \text{(Huey, Louis), (Louis, Huey),} \\ &\quad \text{(Huey, Dewey), (Dewey, Huey),} \\ &\quad \text{(Louis, Dewey), (Dewey, Louis)} \}. \end{aligned}$$

The *Child* relation can be visualised as follows.



Exercise 7.7 (page 187)

1. $R_1 \cup R_2 = R_3$.
2. $R_3 \cap \overline{R_2} = R_1$.
3. $R_3 \setminus R_1 = R_2$.

Exercise 7.8 (page 188)

$$\mathit{Sibling}^{-1} = \mathit{Sibling}.$$

Exercise 7.9 (page 189)

- $\mathit{Uncle} = \mathit{Parent} \circ \mathit{Brother}$ (an uncle is a brother of a parent).

  In the case of the Duck family, we have:

  $$\begin{aligned} \mathit{Uncle} = \{ & \text{(Scrooge, Donald), (Scrooge, Della),} \\ & \text{(Donald, Huey), (Donald, Louis), (Donald, Dewey)} \}. \end{aligned}$$

  The first two pairs arise from the fact that Scrooge is a brother of Hortense, who is a parent of Donald and Della.

  The final three pairs arise from the fact that Donald is a brother of Della, who is a parent of Huey, Louis and Dewey.

- $Nephew = Sibling \circ Son$ (a nephew is a son of a sibling).

  In the case of the Duck family, we have:

$$Nephew = \{\,(\text{Donald}, \text{Scrooge}),\ (\text{Huey}, \text{Donald}),\\ (\text{Louis}, \text{Donald}),\ (\text{Dewey}, \text{Donald})\,\}.$$

  The first pair arises from the fact that Donald is a son of Hortense, who is a sibling of Scrooge.

  The final three pairs arise from the fact that Huey, Louis and Dewey are sons of Della, who is a sibling of Donald.

Exercise 7.10 (page 190)

This follows easily from property ($\star$) of Theorem 7.6.

Exercise 7.11 (page 191)

The relation *Before* is not reflexive, as George Lazenby is not related to himself by this relation. (Having starred in only one film, he could not have appeared in one film before starring in another film.)

The relation *Before* is also not irreflexive, as all of the other actors who have played James Bond have done so on more than one occasion, so each of them is related to himself by the *Before* relation.

The relation *FirstBefore* is irreflexive (and thus it is not reflexive), as an actor could not have starred as James Bond before starring as James Bond.

Exercise 7.12 (page 191)

The relation *Before* is not symmetric; for example, it contains the pair (SC,TD) but not the pair (TD,SC). Nor is it antisymmetric; for example, it contains the pairs (SC,GL) and (GL,SC), and SC$\neq$GL.

The relation *FirstBefore* is not symmetric; for example, it contains the pair (SC,GL) but not the pair (GL,SC). However, it is antisymmetric: given two James Bond actors, one of the two will not have starred as James Bond before the other.

Exercise 7.13 (page 192)

The relation *Before* is not transitive; for example, it contains the pairs (RM,SC) and (SC,GL), but not the pair (RM,GL).

The relation *FirstBefore* is transitive: if one actor starred as James Bond before a second actor, who in turned starred as James Bond before a third actor, then the first actor will naturally have starred as James Bond before the third actor.

Exercise 7.14 (page 192)

The *is-an-ancestor-of* relation is

- not reflexive, but in fact irreflexive, as a person cannot be their own ancestor;
- not symmetric, but in fact antisymmetric, as a person cannot be an ancestor of their own ancestor; and
- transitive, as an ancestor of an ancestor is again an ancestor.

The *is-married-to* relation is

- not reflexive, but in fact irreflexive, as a person cannot be married to themselves;
- symmetric, and not antisymmetric, as the person you are married to is of course married to you; and
- not transitive, as otherwise a married person, by symmetry, would then have to be married to themselves.

Exercise 7.18 (page 194)

1. This is a partial order but not a total order; and it is an equivalence relation.
2. This is not a partial order (it is not antisymmetric), and hence not a total order; but it is an equivalence relation.
3. This is not a partial order (it is not antisymmetric), and hence not a total order; but it is an equivalence relation.

Exercise 7.19 (page 194)

R_1 is an equivalence relation, as it is clearly reflexive (a student takes all the same courses as themselves), symmetric (if x takes all the same courses as y then y takes all the same courses as x) and transitive (if x takes all the same courses as y and y takes all the same courses as z then x takes all the same courses as z).

R_2 is not an equivalence relation, as it is not transitive (though it is reflexive and symmetric). For example, Alice and Bob might take the same Mathematics course, and Bob and Carol might take the same Computing course, while Alice and Carol do not take any of the same courses.

Exercise 7.21 (page 195)

The finest partition of a set A consists of singletons: $\{ \{ a \} : a \in A \}$.

The coarsest partition of a set A consists of one set: $\{ A \}$.

Exercise 7.23 (page 196)

The equivalence relation defined by the finest partition of a set A is the identity relation: $I_A = \{ (a,a) \ : \ a \in A \}$.

The equivalence relation defined by the coarsest partition of a set A is the universal relation: $U_A = \{ (a,b) \ : \ a,b \in A \}$.

Exercise 7.24 (page 196)

The relation R partitions the set A into the following 18 equivalence classes:

$[1] = \{ 1 \}$	$[2] = \{ 2, 4, 8, 16 \}$	$[3] = \{ 3, 9, 27 \}$
$[5] = \{ 5, 25 \}$	$[6] = \{ 6, 12, 18, 24 \}$	$[7] = \{ 7 \}$
$[10] = \{ 10, 20 \}$	$[11] = \{ 11 \}$	$[13] = \{ 13 \}$
$[14] = \{ 14, 28 \}$	$[15] = \{ 15 \}$	$[17] = \{ 17 \}$
$[19] = \{ 19 \}$	$[21] = \{ 21 \}$	$[22] = \{ 22 \}$
$[23] = \{ 23 \}$	$[26] = \{ 26 \}$	$[29] = \{ 29 \}$

Chapter 8

Exercise 8.1 (page 203)

$4 \in \mathbb{N}$: By clause (1), $0 \in \mathbb{N}$, so by clause (2), $1 \in \mathbb{N}$; so by clause (2), $2 \in \mathbb{N}$; so by clause (2), $3 \in \mathbb{N}$; and so finally by clause (2), $4 \in \mathbb{N}$.

$4.5 \notin \mathbb{N}$: Since $4.5 \neq 0$, clause 1 does not apply, so we could only infer that $4.5 \in \mathbb{N}$ from clause (2), and thus from first inferring that $3.5 \in \mathbb{N}$; but by a similar reasoning we could only infer this by first inferring that $2.5 \in \mathbb{N}$; which we could only infer by first inferring that $1.5 \in \mathbb{N}$; which we could only infer by first inferring that $0.5 \in \mathbb{N}$; which we could only infer by first inferring that $-0.5 \in \mathbb{N}$; which we could only infer by first inferring that $-1.5 \in \mathbb{N}$; *et cetera ad infinitum.* This process would never "bottom out", so we could never infer that any of these were in $\mathbb{N}$.

Alternatively, we can easily see that the set $\{ 0, 1, 2, 3, 4, \ldots \}$ satisfies clauses (1) and (2) of the definition; and since $\mathbb{N}$ is being defined to be the *smallest* set satisfying these clauses, $\mathbb{N}$ must be a subset of this; since this set does not contain 4.5, $4.5 \notin \mathbb{N}$.

Exercise 8.2 (page 204)

ODD is defined to be the ***smallest*** set satisfying the two clauses. The fact that $\mathbb{N}$ satisfies these two clauses only implies that ODD $\subseteq \mathbb{N}$; that is, $\mathbb{N}$ is not necessarily (and in fact is not) the smallest such set.

Exercise 8.3 (page 204)

POWERS-OF-2 is the smallest set satisfying the following:

1. $1 \in$ POWERS-OF-2.
2. If $n \in$ POWERS-OF-2 then $2n \in$ POWERS-OF-2.

Exercise 8.4 (page 205)

Given a set A, the smallest set $P(A)$ satisfying:

1. $\emptyset \in P(A)$; and
2. if $X \in P$ and $a \in A$ then $X \cup \{a\} \in P(A)$

is the set of all *finite* subsets of A. This is the same as the powerset $\mathcal{P}(A)$ of A only in the case when A is a finite set.

Exercise 8.5 (page 207)

POSDECIMALNUMBERS is inductively defined as the smallest set satisfying the following:

1. $1, 2, 3, 4, 5, 6, 7, 8, 9 \in$ POSDECIMALNUMBERS;
2. If $w \in$ POSDECIMALNUMBERS and $x \in$ DECIMALDIGITS then $wx \in$ POSDECIMALNUMBERS.

Exercise 8.6 (page 208)

The following is a BNF equation for formulæ of predicate logic.

$$p, q \ ::= \ \mathsf{true} \mid \mathsf{false} \mid P(x_1, \ldots, x_n) \mid \neg p \mid p \vee q \mid p \wedge q \mid p \Rightarrow q \mid p \Leftrightarrow q \mid \forall x\, p \mid \exists x\, p$$

Here, $P(x_1, \ldots, x_n)$ is taken to range over the set of predicates with free variables taken from $x_1, \ldots, x_n$ and x is taken to range over all variables.

Exercise 8.7 (page 212)

The dictionary data structure can be defined using the following BNF equation:

$$d \;=\; \star \mid N(w, d_1, d_2)$$

where w ranges over words (representing names). That is, a dictionary is either a leaf (if it is empty), or it consists of a name along with two sub-dictionaries d_1 and d_2. (Note that the semantic understanding of a dictionary, i.e., the property that the stored names are ordered lexicographically throughout the dictionary, is not reflected in this data structure definition, only its syntactic structure.)

Exercise 8.8 (page 213)

- $s_1 = s_0 + 2{\cdot}1 - 1 = 0 + 2 - 1 = 1$
- $s_2 = s_1 + 2{\cdot}2 - 1 = 1 + 4 - 1 = 4$
- $s_3 = s_2 + 2{\cdot}3 - 1 = 4 + 6 - 1 = 9$
- $s_4 = s_3 + 2{\cdot}4 - 1 = 9 + 8 - 1 = 16$
- $s_5 = s_4 + 2{\cdot}5 - 1 = 16 + 10 - 1 = 25$
- $s_6 = s_5 + 2{\cdot}6 - 1 = 25 + 12 - 1 = 36$

It would appear (though it is as yet uncertain) that $s_n = n^2$.

Exercise 8.9 (page 213)

We could readily compute

$$H_6 = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{49}{20} = 2.45.$$

However, by the inductive definition we would proceed as follows:

- $H_1 = H_0 + \frac{1}{1} = 0 + 1 = 1$
- $H_2 = H_1 + \frac{1}{2} = 1 + \frac{1}{2} = \frac{3}{2} = 1.5$
- $H_3 = H_2 + \frac{1}{3} = \frac{3}{2} + \frac{1}{3} = \frac{11}{6} \approx 1.833$
- $H_4 = H_3 + \frac{1}{4} = \frac{11}{6} + \frac{1}{4} = \frac{25}{12} \approx 2.083$
- $H_5 = H_4 + \frac{1}{5} = \frac{25}{12} + \frac{1}{5} = \frac{137}{60} \approx 2.283$
- $H_6 = H_5 + \frac{1}{6} = \frac{137}{60} + \frac{1}{6} = \frac{49}{20} = 2.45$

Exercise 8.10 (page 214)

At the start of month n you will have f_n pairs of rabbits, where f_n is the nth Fibonacci number.

- For a start, at the start of month 1 you have 1 pair, and at the start of month 2 you still have just the 1 pair. At the start of month 3, though, you will have 2 pairs, and at the start of month 4 you will have 3 pairs.

- In general, at the start of month n you will have $f_n = f_{n-1} + f_{n-1}$ pairs of rabbits, as you will have as many pairs as you had at the start of month $n-1$, namely f_{n-1}, plus a new pair for each pair you had at the start of month $n-2$, namely f_{n-2}.

Exercise 8.11 (page 215)

$$\begin{aligned} \text{mult}(m, 0) &= 0; \quad \textit{and} \\ \text{mult}(m, s(n)) &= \text{add}(\text{mult}(m, n), m). \end{aligned}$$

Exercise 8.12 (page 215)

$$\begin{aligned} \mathit{sum}([\,]) &= 0 \\ \mathit{sum}(n : L) &= n + \mathit{sum}(L) \end{aligned}$$

Thus for example,

$$\begin{aligned} \mathit{sum}([6,2,5]) &= 6 + \mathit{sum}([2,5]) \\ &= 6 + 2 + \mathit{sum}([5]) \\ &= 6 + 2 + 5 + \mathit{sum}([\,]) \\ &= 6 + 2 + 5 + 0 \\ &= 13. \end{aligned}$$

Exercise 8.13 (page 215)

$$\begin{aligned} [\,] +\!\!+ L_2 &= L_2 \\ (h : L) +\!\!+ L_2 &= h : (L +\!\!+ L_2). \end{aligned}$$

Exercise 8.14 (page 216)

$$\begin{aligned} &\mathit{fv}(\text{true}) = \mathit{fv}(\text{false}) = \emptyset \\ &\mathit{fv}(P(x_1, \ldots, x_n)) = \{x_1, \ldots, x_n\} \\ &\mathit{fv}(\neg p) = \mathit{fv}(p) \\ &\mathit{fv}(p \vee q) = \mathit{fv}(p \wedge q) = \mathit{fv}(p \Rightarrow q) = \mathit{fv}(p \Leftrightarrow q) = \mathit{fv}(p) \cup \mathit{fv}(q) \\ &\mathit{fv}(\forall x\, p) = \mathit{fv}(\exists x\, p) = \mathit{fv}(p) \setminus \{x\} \end{aligned}$$

Exercise 8.15 (page 216)

By definition, $f(n) = n-10$ for each $n > 100$. Thus we need only consider the value of $f(n)$ for each n from 0 to 100 and verify that $f(n) = 91$ in each case. We can do this starting from $n = 100$ and working down, using the values we calculate along the way.

- $f(100) = f(f(111)) = f(101) = 91.$
- $f(99) = f(f(110)) = f(100) = 91.$
- $f(98) = f(f(109)) = f(99) = 91.$

  ⋮
- $f(91) = f(f(102)) = f(92) = 91.$
- $f(90) = f(f(101)) = f(91) = 91.$
- $f(89) = f(f(100)) = f(91) = 91.$
- $f(88) = f(f(99)) = f(91) = 91.$

  ⋮
- $f(1) = f(f(12)) = f(91) = 91.$
- $f(0) = f(f(11)) = f(91) = 91.$

Exercise 8.16 (page 218)

$$(insert\,a)\;[\,] \quad = \; [a]$$
$$(insert\,a)\;(b : L) \; = \; if\; a{<}b\; then\; a : (b : L)\;\; else\; b : ((insert\,a)\; L)$$

Exercise 8.17 (page 220)

Moving a pyramid of n discs can be done as follows.

1. If n=1 then simply move the single disc to the new peg. Otherwise do the following.
2. Move the pyramid of $n-1$ discs sitting on top of the largest disc to a different peg.
3. Move the largest disc to the other empty peg.
4. Move the pyramid of $n-1$ discs onto the disc holding the largest disc.

Note the two recursive calls in steps 2 and 4.

Carried out on a tower of five discs, this would require 31 individual moves.

Chapter 9

Exercise 9.1 (page 226)

It would appear that the number of regions doubles every time a new spot is added, so it is tempting to guess that 32 regions will be created by connecting 6 spots. In general, our intuition is suggesting that 2^{n-1} regions are created by connecting n spots, based on the evidence with $n = 1, 2, 3, 4$ and 5.

Unfortunately for our intuition, this guess is wrong: no matter how hard you try, you can only create 31 regions by connecting 6 spots.

In fact, the formula for the number of regions created by connecting n spots is not 2^{n-1}, but the following rather astonishing formula:

$$\frac{n^4 - 6n^3 + 23n^2 - 18n + 24}{24}.$$

Where does this formula come from? Starting with no lines, the circle has just one region. Each time you draw a new line across the circle, you increase the number of regions by 1 more than the number of existing lines which this new line crosses. Thus the number of regions is one more than the total number of lines added to the total number of intersections.

The number of lines you can draw using n spots is $n(n-1)/2$, which is just the number of pairs of endpoints you can choose for the line; and the number of intersections is $n(n-1)(n-2)(n-3)/24$, which is the number of pairs of endpoints of two intersecting lines you could choose. The number of regions created is thus

$$1 + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)(n-3)}{24}$$

which simplifies to the formula given above.

Exercise 9.2 (page 228)

She would assume that the 26th child would confirm that the first 26 numbers add up to $\frac{26\times 27}{2}$, and from this show that the first 27 numbers add up to $\frac{27\times 28}{2}$ as follows:

$$\begin{aligned} 1 + 2 + 3 + \cdots + 27 &= \underbrace{1 + 2 + 3 + \cdots + 26}_{} + 27 \\ &= \frac{26\times 27}{2} + 27 \\ &= 27 \times \left(\frac{26}{2} + 1\right) \\ &= 27 \times \left(\frac{28}{2}\right) \\ &= \frac{27\times 28}{2} \end{aligned}$$

Exercise 9.3 (page 228)

Young Gauss is reputed to have carried out the following calculation, all in his head:

$$\begin{aligned} X &= \ 1 + 2 + 3 + \cdots + 48 + 49 + 50 \\ &\ + 100 + 99 + 98 + \cdots + 53 + 52 + 51 \\ \hline &= 101 + 101 + 101 + \cdots + 101 + 101 + 101 \\ &= 50 \times 101 = 5050 \end{aligned}$$

That is, he had noted that the sum consists of 50 pairs of numbers, where each pair sums to 101.

There are many stories about the prodigious Young Gauss; however – without taking away from his greatness as a mathematician – his biographers do note that these stories are mostly attributed to Old Gauss.

Exercise 9.4 (page 231)

1. For all $n \geq 0$, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof: By induction on n.

Base Case: We note that

$$1^2 + 2^2 + 3^2 + \cdots + 0^2 = 0 = \frac{0(0+1)(2(0)+1)}{6}.$$

Induction Step: We assume that, for *some* k,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6},$$

and from this inductive hypothesis we prove that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

That is, we demonstrate that if the statement of the theorem is true when $n = k$, then it must also be true when $n = k+1$.

$$\begin{aligned} & 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 \\ = {} & \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \qquad \textit{(by the inductive hypothesis)} \\ = {} & \frac{(k+1)}{6}\Big(k(2k+1) + 6(k+1)\Big) \\ = {} & \frac{(k+1)}{6}\Big(2k^2 + 7k + 6\Big) \\ = {} & \frac{(k+1)}{6}\Big((k+2)(2k+3)\Big) \\ = {} & \frac{(k+1)(k+2)(2k+3)}{6} \end{aligned}$$

□

2. For all $n \geq 0$, $1 + 3 + 5 + \cdots + (2n-1) = n^2$.

Proof: By induction on n.

Base Case: We note that

$$1 + 3 + 5 + \cdots + (2(0)-1) = 0 = 0^2.$$

Induction Step: We assume that, for *some* k,

$$1 + 3 + 5 + \cdots + (2k-1) = k^2.$$

and from this inductive hypothesis we prove that

$$1 + 3 + 5 + \cdots + \Big(2(k+1)-1\Big) = (k+1)^2.$$

That is, we demonstrate that if the statement of the theorem is true when $n = k$, then it must also be true when $n = k+1$.

$$1 + 3 + 5 + \cdots + (2k-1) + \Big(2(k+1) - 1\Big)$$

$$= k^2 + \Big(2(k+1) - 1\Big) \quad \textit{(by the inductive hypothesis)}$$

$$= k^2 + 2k + 1$$

$$= (k+1)^2 \qquad \square$$

3. For all $n \geq 0$,

$$1{\cdot}2 + 2{\cdot}3 + 3{\cdot}4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Proof: By induction on n.

Base Case: We note that

$$1{\cdot}2 + 2{\cdot}3 + 3{\cdot}4 + \cdots + 0(0+1) = 0 = \frac{0(0+1)(0+2)}{3}.$$

Induction Step: We assume that, for *some* k,

$$1{\cdot}2 + 2{\cdot}3 + 3{\cdot}4 + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}$$

and from this inductive hypothesis we prove that

$$1{\cdot}2 + 2{\cdot}3 + 3{\cdot}4 + \cdots + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}.$$

That is, we demonstrate that if the statement of the theorem is true when $n = k$, then it must also be true when $n = k+1$.

$$1{\cdot}2 + 2{\cdot}3 + 3{\cdot}4 + \cdots + k(k+1) + (k+1)(k+2)$$

$$= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \quad \textit{(by the inductive hypothesis)}$$

$$= \frac{(k+1)(k+2)}{3}(k+3)$$

$$= \frac{(k+1)(k+2)(k+3)}{3} \qquad \square$$

Exercise 9.5 (page 232)

For all $n \geq 0$, $F_0 \times F_1 \times \cdots \times F_n = F_{n+1} - 2$, where $F_n = 2^{2^n} + 1$.

Proof: By induction on n.

Base Case: For the base case ($n{=}0$), we note that

$$F_0 = 3 = 5 - 2 = F_1 - 2.$$

Induction Step: For the induction step, we assume that, for *some* k,

$$F_0 \times F_1 \times \cdots \times F_k \;=\; F_{k+1} - 2$$

and from this assumption (the *"inductive hypothesis"*) we prove that

$$F_0 \times F_1 \times \cdots \times F_{k+1} \;=\; F_{k+2} - 2.$$

That is, we demonstrate that if the statement of the theorem is true when $n = k$, then it must also be true when $n = k+1$.

$$\begin{aligned} & F_0 \times F_1 \times F_2 \times \cdots \times F_k \times F_{k+1} \\ &= (F_{k+1} - 2) \times F_{k+1} \qquad \textit{(by the inductive hypothesis)} \\ &= (2^{2^{k+1}} - 1) \times (2^{2^{k+1}} + 1) \\ &= 2^{2^{k+2}} - 1 \;=\; F_{k+2} - 2 \quad \square \end{aligned}$$

Exercise 9.6 (page 232)

For any real number $r \neq 1$,

$$1 + r + r^2 + r^3 + \cdots + r^n \;=\; \frac{1 - r^{n+1}}{1 - r}$$

for all $n \geq 0$.

Proof: By induction on n.

Base Case: For the base case (n=0), we note that

$$1 + r + r^2 + r^3 + \cdots + r^0 \;=\; 1 \;=\; \frac{1 - r^1}{1 - r}.$$

Induction Step: For the induction step, we assume that, for *some* k,

$$1 + r + r^2 + r^3 + \cdots + r^k \;=\; \frac{1 - r^{k+1}}{1 - r},$$

and from this assumption (the *"inductive hypothesis"*) we prove that

$$1 + r + r^2 + r^3 + \cdots + r^{k+1} \;=\; \frac{1 - r^{k+2}}{1 - r}$$

That is, we demonstrate that if the statement of the theorem is true when $n = k$, then it must also be true when $n = k+1$.

By the inductive hypothesis we can rewrite the left-hand side of this equation that we want to prove true as

$$\frac{1 - r^{k+1}}{1 - r} + r^{k+1}$$

which we can successively rewrite as

$$\frac{1-r^{k+1}}{1-r} + \frac{(1-r)r^{k+1}}{1-r} = \frac{1-r^{k+1}+r^{k+1}-r^{k+2}}{1-r} = \frac{1-r^{k+2}}{1-r}$$

which is the result we seek. □

Exercise 9.7 (page 233)

Drawing $n \geq 1$ circles so that any two intersect at two points but no three intersect at any point divides the plane into $n^2 - n + 2$ regions.

Proof: By induction on n.

Base Case: One circle divides the plane into $1^2 - 1 + 2 = 2$ regions.

Induction Step: For the induction step, we assume that k circles divides the plane into $k^2 - k + 2$ regions, and show that adding a $(k+1)$st circle results in $(k+1)^2 - (k+1) + 2$ regions.

The $(k+1)$st circle must intersect the other k circles at $2k$ points, meaning that $2k$ regions are divided into two. Thus, $2k$ new regions are created, giving a total of $k^2 - k + 2 + 2k = (k+1)^2 - (k+1) + 2$ regions, which is as we needed to demonstrate. □

A Venn diagram depicting 4 sets would have to divide the plane into 16 regions. Therefore, it could not be drawn using circles, as by the above result 4 circles would only divide the plane into $4^2 - 4 + 2 = 14$ regions.

Exercise 9.8 (page 234)

$f(n) = n^2$ for all $n \geq 0$, where $f(n) = \begin{cases} 0, & \text{if } n=0 \\ f(n-1) + 2n - 1, & \text{if } n>0. \end{cases}$

Proof: By induction on n.

Base Case: For the base case ($n=0$), we simply note that $f(0) = 0 = 0^2$.

Induction Step: For the induction step, we assume that, for *some* k,

$$f(k-1) = (k-1)^2,$$

and from this assumption (the *"inductive hypothesis"*) we prove that

$$f(k) = k^2.$$

That is, we demonstrate that if the statement of the theorem is true when $n = k-1$, then it must also be true when $n = k$.

$$
\begin{aligned}
f(k) &= f(k-1) + 2k - 1 && \textit{(by definition)} \\
&= (k-1)^2 + 2k - 1 && \textit{(by the inductive hypothesis)} \\
&= k^2. && \square
\end{aligned}
$$

Exercise 9.9 (page 235)

Every $n > 1$ is either prime or a product of primes.

Proof: By strong induction on n. Suppose that $n>1$, and that for every integer k with $1<k<n$, k is either prime or the product of primes. If n itself is prime then we have nothing to prove, so suppose that $n = ab$ with $1<a<n$ and $1<b<n$. By the inductive hypothesis, each of a and b is either prime or a product of primes; but then since $n = ab$, n itself is a product of primes.

Exercise 9.10 (page 236)

For all $m \geq 1$ and all $n \geq m$, $\quad H_n - H_m \;\geq\; \frac{n-m}{n}$.

Proof: We assume that $m \geq 1$ is fixed, and we prove the result by induction on n.

Base Case $(n = m)$: $\;H_m - H_m \;=\; 0 \geq \frac{0}{m}$.

Induction Step: $(n > m)$:

$$
\begin{aligned}
H_n - H_m &= H_{n-1} - H_m + \frac{1}{n} \\
&\geq \frac{(n-1)-m}{n-1} + \frac{1}{n} && \textit{(by inductive hypothesis)} \\
&= \frac{(n-1)n - mn + (n-1)}{(n-1)n} \\
&\geq \frac{(n-1)n - mn + m}{(n-1)n} && \textit{(since } n-1 \geq m\textit{)} \\
&= \frac{n-m}{n} && \square
\end{aligned}
$$

Exercise 9.11 (page 236)

Fact: $(f_0)^2 + (f_1)^2 + (f_2)^2 + \cdots (f_n)^2 \;=\; f_n f_{n+1}$ for all $n \geq 0$.

Proof: By induction on n.

Base Case $(n = 0)$:

$$(f_0)^2 + (f_1)^2 + (f_2)^2 + \cdots + (f_0)^2 \;=\; (f_0)^2 \;=\; 0^2 \;=\; 0 \times 1 \;=\; f_0 f_1.$$

Induction Step $(n > 0)$:

$$(f_0)^2 + (f_1)^2 + (f_2)^2 + \cdots + (f_n)^2 + (f_{n+1})^2$$
$$= f_n f_{n+1} \ + \ (f_{n+1})^2 \qquad \textit{(by the inductive hypothesis)}$$
$$= f_{n+1}(f_n + f_{n+1}) \ = \ f_{n+1} f_{n+2} \qquad \square$$

Exercise 9.12 (page 238)

Fact: The quadratic equation $y^2 - xy - x^2 = \pm 1$ is satisfied by the pair $(x, y) = (f_n, f_{n+1})$ for any $n \geq 0$.

Proof: By induction on n.

Base Case $(n = 0)$: With $(x, y) = (f_0, f_1) = (0, 1)$ we have

$$y^2 - xy - x^2 \ = \ 1^2 - 0 \cdot 1 - 1^0 \ = \ 1.$$

Induction Step $(n > 0)$: Assuming that $(x, y) = (a, b)$ solves this equation, that is,

$$b^2 - ab - a^2 \ = \ \pm 1$$

it suffices to show that $(x, y) = (a{+}b, b)$ also solves this equation; this is because if $(a, b) = (f_n, f_{n+1})$ then $(f_{n+1}, f_{n+2}) = (a{+}b, b)$.

$$\begin{aligned}(a{+}b)^2 \ - \ (a{+}b)b \ - \ b^2 \ &= \ a^2 + 2ab + b^2 \ - \ ab - b^2 \ - \ b^2 \\ &= \ a^2 + ab - b^2 \\ &= \ -(b^2 - ab - a^2) \ = \ \mp 1. \quad \square\end{aligned}$$

Exercise 9.13 (page 238)

Fact: The positive integer solutions (x, y) to

$$y^2 - xy - x^2 \ = \ \pm 1$$

are of the form (f_n, f_{n+1}) for some $n \geq 0$.

Proof: By induction on $x{+}y$. We first note that since x and y are positive, we must have that $x \leq y$. If $x = y$ then we would have that $-x^2 = \pm 1$, in which case we must have that $x{=}y{=}1$, so $(x, y) = (f_1, f_2)$.

We now assume that $1 \leq x < y$ and that $y^2 - xy - x^2 = \pm 1$, and note that the pair $(a, b) = (y{-}x, x)$ also satisfies the equation:

$$\begin{aligned}b^2 \ - \ ab \ - \ a^2 \ &= \ x^2 \ - \ (y{-}x)x \ - \ (y{-}x)^2 \\ &= \ x^2 - xy + x^2 - y^2 + 2xy - x^2 \\ &= \ -(y^2 - xy - x^2) \ = \ \mp 1.\end{aligned}$$

By induction, $(a, b) = (f_n, f_{n+1})$ for some n, from which we get

$$x = b = f_{n+1} \quad \text{and}$$
$$y = a + x = f_n + f_{n+1} = f_{n+2},$$

so $(x, y) = (f_{n+1}, f_{n+2})$. □

Exercise 9.14 (page 239)

Fact: $f_{n+1}^2 - f_n f_{n+2} = (-1)^n$ for all $n \geq 0$.

Proof: By induction on n.

Base Case $(n = 0)$: $f_1^2 - f_0 f_2 = 1^2 - 0 \cdot 1 = 1 = (-1)^0$.

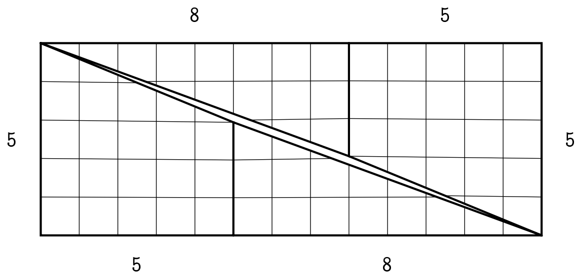
Induction Step $(n > 0)$:

$$\begin{aligned} f_{n+1}^2 - f_n f_{n+2} &= f_{n+1}(f_n + f_{n-1}) - f_n(f_{n+1} + f_n) \quad \textit{(by definition)} \\ &= f_{n+1} f_n + f_{n+1} f_{n-1} - f_n f_{n+1} - f_n^2 \\ &= -(f_n^2 - f_{n-1} f_{n+1}) \\ &= -(-1)^{n-1} \quad \textit{(by the inductive hypothesis)} \\ &= (-1)^n \end{aligned}$$

□

Exercise 9.15 (page 239)

The edges that supposedly make up the diagonal of the rectangle do not in fact line up. Drawn more carefully, a gap (or overlap) is discovered in the middle with an area of one unit.



Exercise 9.17 (page 243)

The induction argument cannot be applied when n=2: if S' and S'' are overlapping sets which together make up S, then either $S' = S$ or $S'' = S$, in which case you cannot apply induction to this set, as you can only apply induction to sets smaller than S.

Exercise 9.20 (page 246)

Fact: $\mathit{length}(L_1{+\!\!+}L_2) = \mathit{length}(L_1) + \mathit{length}(L_2)$ for all lists L_1 and L_2.

Proof: By induction on the structure of L_1.

Base Case ($L_1 = [\,]$):

$$\mathit{length}([\,]{+\!\!+}L_2) \;=\; \mathit{length}(L_2) \;=\; \mathit{length}([\,]) + \mathit{length}(L_2).$$

Induction Step ($L_1 = h : L$):

$$\begin{aligned}
&\mathit{length}\,((h : L){+\!\!+}L_2)\\
&= \mathit{length}\,(h : (L{+\!\!+}L_2)) \quad \textit{(by definition)}\\
&= 1 + \mathit{length}(L{+\!\!+}L_2)\\
&= 1 + \mathit{length}(L) + \mathit{length}(L_2) \quad \textit{(by the inductive hypothesis)}\\
&= \mathit{length}(h : L) + \mathit{length}(L_2).
\end{aligned}$$

□

Chapter 10

Exercise 10.1 (page 257)

1. By brute force reasoning, we get the following table:

n	1	2	3	4	5	6	7	8	9	10
$f(n)$	1	2	3	$\bot$	1	2	3	$\bot$	1	2

   $f(n)$ represents the number of coins the first player should take when there are n coins in the pile; we write $f(n) = \bot$ (meaning $f(n)$ is undefined) in the cases in which the second player has the winning strategy.

2. If the first player takes x coins, the second player can respond by taking $(4-x)$ coins, leaving the first player a pile of $(n-4)$ coins when starting from a pile of n coins. This gives a winning strategy for the second player in a game starting with $n{=}4k$ coins, that is, a number of coins divisible by 4.

   In all other cases, starting with $n = 4k{+}x$ coins (where x is 1, 2, or 3), the first player puts the second player in a losing position by taking x coins and leaving $4k$ coins.

3. The first player is in a losing position if the number of coins n is divisible by $(k+1)$; the second player wins by responding to every move of the first player by taking $(k+1)-x$ coins, where x is the number of coins that the first player takes.

   If the number of coins n is not divisible by $(k+1)$, then the first player wins by taking $n \bmod (k+1)$ coins, leaving the second player in a losing position.

4. The goal in the Misère game is to leave your opponent with one coin. Thus, the second player has a winning strategy when there are $4k+1$ coins, using the same strategy as the normal game.

Exercise 10.2 (page 258)

1. The second player can always place the first two noughts on adjacent sides. (The first nought can be placed on a side which has both adjacent sides empty, and one of these will still be empty after the first player places the second cross.)

   The third nought can then always be placed so that it is aligned with at most one of the first two noughts (i.e., not in the centre square nor in the corner between the two noughts). This is true because there are five such squares, and only three of them can be occupied by crosses.

   The fourth and final nought can then be placed safely, as there can only be at most one square which could create a line of three noughts, yet there will be two empty squares available to chose from.

2. Suppose the first player places the first cross in the centre and then places all subsequent crosses directly opposite the squares on which the second player places noughts. If a line of three crosses should arise, it clearly could not include the centre square, and in fact would imply that there is a line of three noughts already in place directly opposite the line of three crosses.

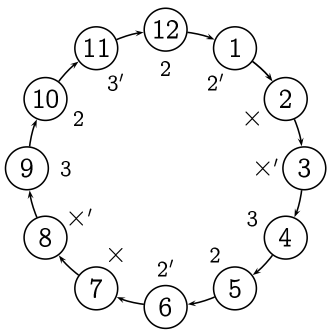
Exercise 10.3 (page 258)

Following on from the reasoning started in the question:

- 9 o'clock is a winning position (by moving 3 hours ahead to 12 o'clock), and
  10 o'clock is a winning position (by moving 2 hours ahead to 12 o'clock);
- 7 o'clock is a losing position (as you can only move to a winning position: either 2 hours ahead to 9 o'clock or 3 hours ahead to 10 o'clock);
- 4 o'clock is a winning position (by moving 3 hours ahead to 7 o'clock), and
  5 o'clock is a winning position (by moving 2 hours ahead to 7 o'clock);

- 2 o'clock is a losing position (as you can only move to a winning position: either 2 hours ahead to 4 o'clock or 3 hours ahead to 5 o'clock);
- 11 o'clock is a winning position (by moving 3 hours ahead to 2 o'clock), and
  12 o'clock is a winning position (by moving 2 hours ahead to 2 o'clock);
- 8 o'clock is a losing position (as you can only move to a winning position: either 2 hours ahead to 10 o'clock or 3 hours ahead to 11 o'clock);
- 6 o'clock is a winning position (by moving 2 hours ahead to 8 o'clock); and
- 3 o'clock is a losing position (as you can only move to a winning position: either 2 hours ahead to 5 o'clock or 3 hours ahead to 6 o'clock).

This is summarised as follows, where the hours on the clock are annotated with the winning move if one is available.



The symbol × indicates that the position is a losing position; and a prime means that the token will pass through the 12 o'clock position once before landing on it the second time around (assuming the losing player uses a particular strategy).

To see that this annotation is correct, it suffices to note that

- every valid move from an hour labelled × (i.e., forward by either two or three hours) leads to a position labelled 2 or 3, neither with a prime, without passing through 12 o'clock;
- every valid move from an hour labelled ×′ leads to a position labelled 2 or 3, (at least) one of which is primed, without passing through 12 o'clock;
- an hour labelled 2 (respectively 3) – by moving forward by 2 (respectively 3) hours – leads either to 12 o'clock, or without passing through 12 o'clock to an hour labelled by ×;

- an hour labelled $2'$ (respectively $3'$) – by moving forward by 2 (respectively 3) hours – leads either to an hour labelled by $\times'$ without passing through 12 o'clock, or by first passing through 12 o'clock to an hour labelled by $\times$.

Exercise 10.4 (page 259)

In this game:

- 9 is a losing position, as the other player will have won by having moved the counter there.
- 8 is a winning position, as a move of 1 takes the counter to the losing position 9.
- 7 is not a legal position, as it is at the head of a snake.
- 6 is a losing position, as moves of 1 and 2 take the counter to the winning positions 4 and 8, respectively.
- 5 is not a legal position, as it is at the foot of a ladder.
- 4 is a winning position, as a move of 1 takes the counter to the losing position 9.
- 3 is not a legal position, as it is at the foot of a ladder.
- 2 is a winning position, as a move of 1 takes the counter to the losing position 6.
- 1 is a winning position, as a move of 2 takes the counter to the losing position 6.

Exercise 10.5 (page 262)

If we ignore one of the piles and consider the column parity of the remaining $n-1$ piles, this indicates what size the final pile would have to be in order to balance the position. (For example, if the $n-1$ piles are balanced, then the final pile would have to be empty; and if all n piles are balanced, then the column parity of any $n-1$ piles would equal the size of the omitted pile.)

Thus, for each pile, there is at most one winning move involving that pile, which consists of leaving the number of coins equal to the column parity of the remaining $n-1$ piles.

Therefore, there are at most n different winning moves possible from a Nim position with n piles.

Exercise 10.6 (page 262)

If the position is initially unbalanced, then the first player need not use this new move in order to win; the first player already has the winning strategy in the original game.

If, on the other hand, the position is initially balanced, then this new move will still not help, as it will produce an unbalanced position, as does any normal move.

Hence this new rule gives the first player no new advantage.

There is another way to see that this new move is obviously of no help to the first player: the second player can respond to this new move by removing all of the coins in the new pile, thus putting the first player back into the same position as before the new move was made.

Exercise 10.7 (page 264)

For $n = f_{k_1}+f_{k_2}+\cdots+f_{k_r} > 0$ with $0 \ll k_1 \ll k_2 \ll \cdots \ll k_r$, let $\mu(n) = f_{k_1}$; that is, $\mu(n)$ is the smallest Fibonacci number appearing in the representation of n in the Fibonacci number system. Also, for convenience, define $\mu(0) = \infty$.

Consider the following two lemmas.

Lemma 1. If $n>0$ then $\mu(n-\mu(n)) > 2\mu(n)$.

This says that if you take $\mu(n)$ coins on your turn from a pile of n coins – which, in particular, the first person ***may*** do on their first move if, and only if, n is ***not*** a Fibonacci number, that is, $\mu(n) \neq n$ – then your opponent will be *unable* to do this in response; that is, they will be faced with some number $m = n-\mu(n)$ of coins and the most coins they can take, namely $2\mu(n)$, will be less than $\mu(m) = \mu(n-\mu(n))$.

Lemma 2. If $0 < m < \mu(n)$ then $\mu(n-m) \leq 2m$.

This says that if you take fewer than $\mu(n)$ coins on your turn from a pile of n coins – which, in particular, the first person ***must*** do on their first move if, and only if, n ***is*** a Fibonacci number – then your opponent *will* be able to take $\mu(n-m)$ coins from the pile of $n-m$ coins they are faced with, as $\mu(n-m)$ will be no more than than twice the number m of coins that you have taken.

Theorem 10.7 follows directly from these two lemmas. Given a pile of n_1 coins, if you take $\mu(n_1)$ coins then either you will have taken all coins and won the game, or you will leave some number n_2 of coins from which, by Lemma 1, your opponent cannot take $\mu(n_2)$ coins, and in particular cannot take all of the remaining coins; and by Lemma 2 your opponent will be forced to leave you with some number n_3 of coins from which you can once again use the strategy of taking $\mu(n_3)$ coins; the play will continue in this fashion until you succeed in taking all remaining coins.

It remains only to prove these two lemmas.

Proof of Lemma 1. Let $n = f_{k_1} + f_{k_2} + \cdots + f_{k_r}$ be the Fibonacci number system representation of n.

The result is immediate if n is a Fibonacci number (that is, if $r{=}1$), as then $n = \mu(n)$, so $\mu(n{-}\mu(n)) = \mu(0) = \infty > n = \mu(n)$.

Assume, then, that n is *not* a Fibonacci number (that is, $r{\geq}2$). Then

$$\begin{aligned} \mu(n{-}\mu(n)) &= f_{k_2} && (\text{as } n{-}\mu(n) = f_{k_2} + \cdots + f_{k_r}) \\ &\geq f_{k_1+2} && (\text{as } k_1 \ll k_2) \\ &= f_{k_1} + f_{k_1+1} \\ &> f_{k_1} + f_{k_1} \\ &= 2f_{k_1} \\ &= 2\mu(n). \end{aligned}$$

□

Proof of Lemma 2. Assume that $0 < m < \mu(n)$. Let the Fibonacci number system representations of n and m be

$$\begin{aligned} n &= f_{k_1} + f_{k_2} + \cdots + f_{k_r} \quad \text{and} \\ m &= f_{\ell_1} + f_{\ell_2} + \cdots + f_{\ell_s}. \end{aligned}$$

By assumption, $m < \mu(n) = f_{k_1}$, so $f_{k_1}{-}m > 0$. Let the Fibonacci number system representations of $f_{k_1}{-}m$ be

$$f_{k_1}{-}m = f_{u_1} + f_{u_2} + \cdots + f_{u_t}.$$

In particular, $f_{u_t}{<}f_{k_1}$, so $u_t{<}k_1{\ll}k_2$, and hence $u_t{\ll}k_2$.

Then

$$\begin{aligned} n{-}m &= (f_{k_1}{-}m) + f_{k_2} + f_{k_3} + \cdots + f_{k_r} \\ &= f_{u_1} + f_{u_2} + \cdots + f_{u_t} + f_{k_2} + f_{k_3} + \cdots + f_{k_r} \end{aligned}$$

and since $u_1{\ll}u_2{\ll}\cdots{\ll}u_t{\ll}k_2{\ll}k_3{\ll}\cdots{\ll}k_r$, this is the Fibonacci number system representation of $n{-}m$.

Thus $\mu(n{-}m) = f_{u_1}$.

Note that

$$\begin{aligned} f_{k_1} &= m + f_{u_1} + f_{u_2} + \cdots + f_{u_t} \\ &= f_{\ell_1} + f_{\ell_2} + \cdots + f_{\ell_s} + f_{u_1} + f_{u_2} + \cdots + f_{u_t}. \end{aligned}$$

Therefore we must have that $\ell_s \not\ll u_1$, that is, $u_1 \leq \ell_s{+}1$, as otherwise we would have two different Fibonacci number system representations for f_{k_1}. Thus $f_{u_1} \leq f_{\ell_s+1}$, and hence

$$\mu(n{-}m) = f_{u_1} \leq f_{\ell_s+1} = f_{\ell_s-1} + f_{\ell_s} \leq 2f_{\ell_s} \leq 2m.$$

□

Exercise 10.12 (page 270)

Assume to the contrary that the second player has successfully created a path connecting the top border to the bottom border. At some point this path must cross the main diagonal, either horizontally or vertically.

As this path approaches the main diagonal from above, a downwards move cannot turn towards the left border, and a rightwards move cannot turn upwards. Hence this path must continuously travel downwards and to the right. Therefore, it must reach the main diagonally vertically and thus cross it horizontally; it cannot cross the diagonal vertically.

On the other hand, as this path approaches the main diagonal from below, an upwards move cannot turn towards the right border, and a leftwards move cannot turn downwards. Hence this path must continuously travel upwards and to the left. Therefore, it must reach the main diagonally vertically and thus cross it vertically; that is, it cannot cross it horizontally.

Chapter 11

Exercise 11.3 (page 286)

At any given moment, there must be some number i of missionaries and some number j of cannibals on the left bank of the river, and $3-i$ missionaries and $3-j$ cannibals on the right bank. If $i \neq j$ then the cannibals outnumber the missionaries on one of the banks; this would only be safe if the number of missionaries on that bank is in fact zero. Hence the only safe states are those in which $i=3$ (all missionaries together on the left bank) or $i=0$ (all missionaries together on the right bank) or $i=j$ (an equal number of missionaries and cannibals on both banks). There are 10 such pairs of numbers (i, j).

Apart from this, the only information needed to completely describe the state of the system is where the boat is; it may be on the left bank or the right bank. Combined with the 10 possible placements of the missionaries and cannibals, this gives the system a total of 20 possible safe states. However, four of these are not feasible. For a start, we clearly cannot have all the people on one bank ($i=j=3$ or $i=j=0$) and the boat on the other. Furthermore, if the missionaries are all on one bank and the cannibals are all on the other ($\{i, j\} = \{0, 3\}$) then the boat must be with the cannibals; if it were with the missionaries, then one or two of them must have just ferried it across the river from the bank on which all three cannibals are, which would have been an unsafe position.

The remaining 16 states are depicted in Figure 15.4, along with the possible transitions between states drawn in. (To avoid clutter, the transitions are drawn bi-directionally, as they all represent reversible actions.) The groups

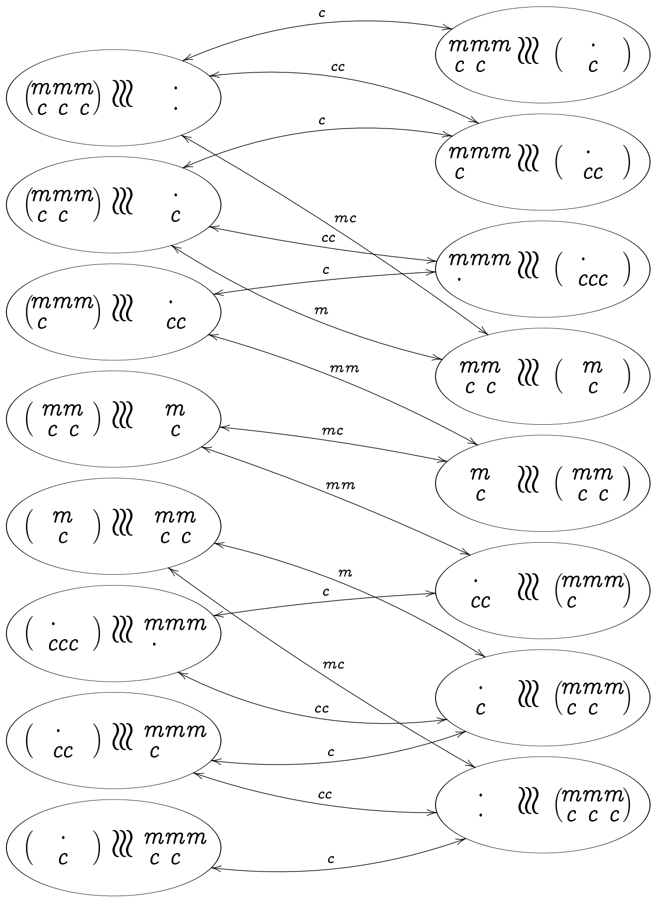


Figure 15.4: The LTS of the Missionaries and Cannibals Riddle.

on the two banks are depicted side-by-side divided by wiggly lines representing the river, with the group holding the boat enclosed in parentheses. There are five possible actions: m (a missionary crosses alone); mm (two missionaries cross together); c (a cannibal crosses alone); cc (two cannibals cross together); and mc (a missionary and a cannibal cross together). Notice that all of the transitions are drawn bi-directionally, as every transition can clearly be reversed.

The group start in the top-left state in which the whole group is on the left bank, and they wish to get to the bottom-right state in which they are all on the right bank. It is not hard to find a such path through the LTS which involves 11 crossings.

Exercise 11.4 (page 287)

A state of the system underlying this riddle consists of a pair of integers (i, j) with $0 \le i \le 5$ and $0 \le j \le 3$, representing the volume of water in the 5-gallon and 3-gallon jugs A and B, respectively. The initial state is $(0, 0)$ and the final state you wish to reach is $(4, 0)$.

There are six types of moves possible from any given state (i, j):

$$
\begin{array}{llll}
(i,j) & \xrightarrow{fillA} & (5, j) & (if\ i{=}0) \\
(i,j) & \xrightarrow{fillB} & (i, 3) & (if\ j{=}0) \\
(i,j) & \xrightarrow{emptyA} & (0, j) & (if\ i{>}0) \\
(i,j) & \xrightarrow{emptyB} & (i, 0) & (if\ j{>}0) \\
(i,j) & \xrightarrow{AtoB} & (\max(0, i{+}j{-}3), \min(3, i{+}j)) & (if\ i{>}0\ and\ j{<}3) \\
(i,j) & \xrightarrow{BtoA} & (\min(5, i{+}j), \max(0, i{+}j{-}5)) & (if\ i{<}5\ and\ j{>}0)
\end{array}
$$

Drawing out the LTS, we identify the following 7-step solution:

$$
\begin{array}{l}
(0,0) \xrightarrow{fillA} (5,0) \xrightarrow{AtoB} (2,3) \xrightarrow{emptyB} (2,0) \xrightarrow{AtoB} (0,2) \\
\qquad \xrightarrow{fillA} (5,2) \xrightarrow{AtoB} (4,3) \xrightarrow{emptyB} (4,0).
\end{array}
$$

Exercise 11.5 (page 287)

The beer mats must start in one of the following three non-winning configurations:

X: 3 one way, the 4th the other way.

Y: 2 face-up and 2 face-down, with diagonally-opposite corners different.

Z: 2 face-up and 2 face-down, with diagonally-opposite corners the same.

Furthermore, there are only three different moves which you may apply to the beer mats:

a: flip one beer mat.

b: flip two adjacent beer mats.

c: flip two diagonally-opposite beer mats.

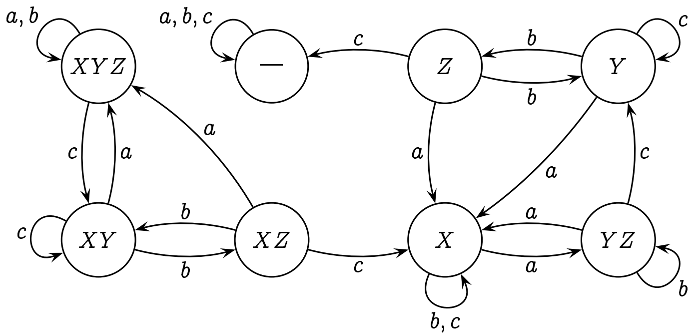
(Flipping 3 beer mats has the same effect on the possible configurations as flipping 1 beer mat; and flipping all four beer mats has no effect whatsoever on the configuration.)

In the following table, we indicate which non-winning configurations we may go to from each non-winning configuration.

	a	b	c
X	Y/Z	X	X
Y	X	Z	Y
Z	X	Y	–

For example, from an X-configuration, an a-move (flipping one beer mat) could lead to a winning configuration, or to either a Y-configuration or a Z-configuration; and from a Z-configuration, a c-move (flipping diagonally-opposite beer mats) is guaranteed to lead to a winning configuration.

We can use a labelled transition system to keep track of which configurations we may be in at any given time *assuming* that we have never passed through a winning configuration. The LTS looks as follows.



Here, we start in the state labelled "XYZ" signifying that we don't know which state X, Y or Z we are in. If we do an a move or a b move, then we may still be in any of these states; however, if we do a c move, then we will know that we *cannot* be in a Z state.

From this we can see that the shortest sequence of moves which guarantees a win is the sequence "cbcacbc" of seven moves.

Exercise 11.6 (page 288)

1. There are six states. In the graphical presentation of the transition system, these are represented by the following (x, y)-valued pairs:

$$\begin{pmatrix} x = 246 \\ y = 174 \end{pmatrix} \quad \begin{pmatrix} x = 72 \\ y = 30 \end{pmatrix} \quad \begin{pmatrix} x = 12 \\ y = 6 \end{pmatrix}$$

$$\begin{pmatrix} x = 72 \\ y = 174 \end{pmatrix} \quad \begin{pmatrix} x = 12 \\ y = 30 \end{pmatrix} \quad \begin{pmatrix} x = 0 \\ y = 6 \end{pmatrix}$$

(Of course, how the states are labelled is irrelevant.)

2. There are two actions, namely "$\texttt{x := x mod y}$" and "$\texttt{y := y mod x}$".
3. There are five transitions. Labelling the states as above, these transitions are:

$$\begin{pmatrix} x = 246 \\ y = 174 \end{pmatrix} \xrightarrow{\texttt{x := x mod y}} \begin{pmatrix} x = 72 \\ y = 174 \end{pmatrix}$$

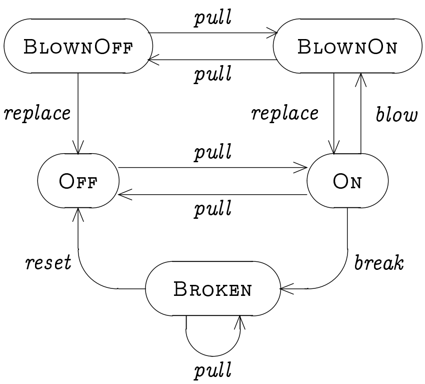
$$\begin{pmatrix} x = 72 \\ y = 174 \end{pmatrix} \xrightarrow{\texttt{y := y mod x}} \begin{pmatrix} x = 72 \\ y = 30 \end{pmatrix}$$

$$\begin{pmatrix} x = 72 \\ y = 30 \end{pmatrix} \xrightarrow{\texttt{x := x mod y}} \begin{pmatrix} x = 12 \\ y = 30 \end{pmatrix}$$

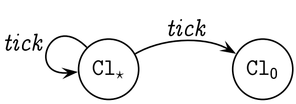
$$\begin{pmatrix} x = 12 \\ y = 30 \end{pmatrix} \xrightarrow{\texttt{y := y mod x}} \begin{pmatrix} x = 12 \\ y = 6 \end{pmatrix}$$

$$\begin{pmatrix} x = 12 \\ y = 6 \end{pmatrix} \xrightarrow{\texttt{x := x mod y}} \begin{pmatrix} x = 0 \\ y = 6 \end{pmatrix}$$

Exercise 11.7 (page 289)



Exercise 11.8 (page 290)



The above process has two states: $\texttt{Cl}_\star$ and $\texttt{Cl}_0$; one action: $\texttt{tick}$; and two transitions: $\texttt{Cl}_\star \xrightarrow{\texttt{tick}} \texttt{Cl}_\star$ and $\texttt{Cl}_\star \xrightarrow{\texttt{tick}} \texttt{Cl}_0$.

Exercise 11.9 (page 291)

As described, a state is a triple $\langle f, d, S \rangle$ where

$f \in \{1, 2^{\uparrow}, 2^{\downarrow}, 3, 1^{+}, 2^{+}, 2^{-}, 3^{-}\}$;

$d \in \{open, closed\}$; and

$S \subseteq \{1, 2^{\uparrow}, 2^{\downarrow}, 3\}$.

There are 11 actions that the system can possibly do. Firstly, any of the call buttons can be pressed on any of the floors:

p_1: (up) button on floor 1 is pressed;

$p_{2^{\uparrow}}$: up button on floor 2 is pressed;

$p_{2^{\downarrow}}$: down button on floor 2 is pressed;

p_3: (down) button on floor 3 is pressed.

Next, any of the floor buttons can be pressed in the elevator:

e_1: floor 1 button is pressed in the elevator;

e_2: floor 2 button is pressed in the elevator;

e_3: floor 3 button is pressed in the elevator.

Next, the elevator door can open or close:

op: the elevator door opens;

cl: the elevator door closes.

Finally, the elevator can move:

up: the elevator moves up;

dn: the elevator moves down.

Exactly when each of these actions can occur, and their effect on the state of the system, is detailed as follows.

Firstly, any button can be pressed on any of the floors at any time. If the elevator is at that floor with its door open and travelling in the right direction, then the button press will have no effect on the state; otherwise, the floor, tagged by the requested direction, will be added to the destination list:

$$\langle f, d, S\rangle \xrightarrow{p_b} \langle f, d, S'\rangle, \text{ where } S' = \begin{cases} S, & \text{if } f{=}b \text{ and } d{=}open \\ S \cup \{b\}, & \text{otherwise} \end{cases}$$

Next, any button can be pressed in the elevator at any time. If the elevator is at the floor being requested with its door open, then the button press will have no effect on the state; otherwise, the floor being requested, tagged by the direction to get to the requested floor (or the current direction being travelled if the elevator is at that floor), will be added to the destination list:

$$\langle f, d, S\rangle \xrightarrow{e_1} \langle f, d, S'\rangle, \text{ where}$$

$$S' = \begin{cases} S, & \text{if } f{=}1 \text{ and } d{=}\mathit{open} \\ S \cup \{1\}, & \text{otherwise} \end{cases}$$

$\langle f, d, S\rangle \xrightarrow{e_2} \langle f, d, S'\rangle$, where

$$S' = \begin{cases} S, & \text{if } f \in \{2^{\uparrow}, 2^{\downarrow}\} \text{ and } d{=}\mathit{open} \\ S \cup \{2^{\uparrow}\}, & \text{if } f \in \{1, 1^{+}, 2^{-}\} \\ & \text{or } f{=}2^{\uparrow} \text{ and } d{=}\mathit{closed} \\ S \cup \{2^{\downarrow}\}, & \text{if } f \in \{3, 3^{-}, 2^{+}\} \\ & \text{or } f{=}2^{\downarrow} \text{ and } d{=}\mathit{closed} \end{cases}$$

$\langle f, d, S\rangle \xrightarrow{e_3} \langle f, d, S'\rangle$, where

$$S' = \begin{cases} S, & \text{if } f{=}3 \text{ and } d{=}\mathit{open} \\ S \cup \{3\}, & \text{otherwise} \end{cases}$$

Next, the door can either open or close at appropriate times:

$$\langle f, \mathit{open}, S\rangle \xrightarrow{cl} \langle f, \mathit{closed}, S\rangle;$$
$$\langle f, \mathit{closed}, S\rangle \xrightarrow{op} \langle f, \mathit{open}, S \setminus \{f\}\rangle, \quad \text{if } f \in S;$$
$$\langle 2^{\uparrow}, \mathit{closed}, S\rangle \xrightarrow{op} \langle 2^{\downarrow}, \mathit{open}, S \setminus \{2^{\downarrow}\}\rangle, \quad \text{if } 2^{\downarrow} \in S \text{ and } 2^{\uparrow}, 3 \notin S;$$
$$\langle 2^{\downarrow}, \mathit{closed}, S\rangle \xrightarrow{op} \langle 2^{\uparrow}, \mathit{open}, S \setminus \{2^{\uparrow}\}\rangle, \quad \text{if } 2^{\uparrow} \in S \text{ and } 2^{\downarrow}, 1 \notin S.$$

Finally, the elevator can move as and when appropriate:

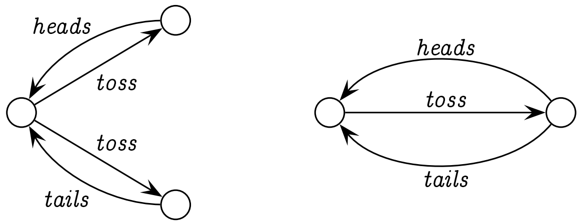
$$\langle 1, \mathit{closed}, S\rangle \xrightarrow{up} \langle 1^{+}, \mathit{closed}, S\rangle, \quad \text{if } 1 \notin S \text{ and } S \neq \emptyset;$$
$$\langle 2^{\uparrow}, \mathit{closed}, \{3\}\rangle \xrightarrow{up} \langle 2^{+}, \mathit{closed}, \{3\}\rangle;$$
$$\langle 2^{\downarrow}, \mathit{closed}, \{3\}\rangle \xrightarrow{up} \langle 2^{+}, \mathit{closed}, \{3\}\rangle;$$
$$\langle 1^{+}, \mathit{closed}, S\rangle \xrightarrow{up} \langle 1^{+}, \mathit{closed}, S\rangle;$$
$$\langle 1^{+}, \mathit{closed}, S\rangle \xrightarrow{up} \langle 2^{\uparrow}, \mathit{closed}, S\rangle;$$
$$\langle 2^{+}, \mathit{closed}, S\rangle \xrightarrow{up} \langle 2^{+}, \mathit{closed}, S\rangle;$$
$$\langle 2^{+}, \mathit{closed}, S\rangle \xrightarrow{up} \langle 3, \mathit{closed}, S\rangle;$$

$$\langle 3, \mathit{closed}, S\rangle \xrightarrow{dn} \langle 3^{-}, \mathit{closed}, S\rangle, \quad \text{if } 3 \notin S \text{ and } S \neq \emptyset;$$
$$\langle 2^{\downarrow}, \mathit{closed}, \{1\}\rangle \xrightarrow{dn} \langle 2^{-}, \mathit{closed}, \{1\}\rangle;$$
$$\langle 2^{\uparrow}, \mathit{closed}, \{1\}\rangle \xrightarrow{dn} \langle 2^{-}, \mathit{closed}, \{1\}\rangle;$$
$$\langle 3^{-}, \mathit{closed}, S\rangle \xrightarrow{dn} \langle 3^{-}, \mathit{closed}, S\rangle;$$
$$\langle 3^{-}, \mathit{closed}, S\rangle \xrightarrow{dn} \langle 2^{\downarrow}, \mathit{closed}, S\rangle;$$

$$\langle 2^-, \mathit{closed}, S\rangle \xrightarrow{dn} \langle 2^-, \mathit{closed}, S\rangle;$$
$$\langle 2^-, \mathit{closed}, S\rangle \xrightarrow{dn} \langle 1, \mathit{closed}, S\rangle;$$

Exercise 11.10 (page 291)

The two models for flipping coins are as follows:



As required, the outcome is determined in the first model already when the coin is tossed: the system will either be in a state in which it can do a *heads* action and not a *tails* action, or it will be in a state in which it can do a *tails* action and not a *heads* action. In contrast to this, when the coin is tossed in the second model, the system will be in a state in which it can do either a *heads* action or a *tails* action.

Which model is more realistic? We might introduce quantum mechanics and allude to the fate of Schrödinger's cat placed in a sealed box with a flask of poison, a radioactive source, and a mechanism which will shatter the flask – releasing the poison and killing the cat – if a Geiger counter detects a radioactive particle; according to quantum mechanics, after a while the cat will be *simultaneously dead and alive* until we open the box; only by observing the cat will its fate be sealed. With this in mind, we might choose the second model to be more realistic.

Barring the complexities of Schrödinger's cat, the first model is more realistic, in that it enforces the principle that the toss itself decides the fate of the coin; having tossed the coin, and with it resting on the back of one hand shielded from view by the palm of the other, no further forces can influence the outcome of the coin flip. The coin is decidedly showing heads or tails.

We can contrast this situation with the model of the simple vending machine from page 282 which accepts a 50p coin and allows the user to decide whether to press a coffee button or a tea button. Having inserted the 50p coin, the user is completely free to choose which button to press, and thus the model for the vending machine closely resembles the second coin-flipping model above. Such a free choice is of course undesirable in a coin flip. (It would be equally undesirable for the vending machine to eliminate the user's free choice of drinks when the 50p coin is inserted, as with the first coin-flipping model above.)

Exercise 11.11 (page 296)

By the rule for action prefix,

$$pull.\textsc{Broken} \xrightarrow{pull} \textsc{Broken} \quad \text{and}$$
$$reset.\textsc{Off} \xrightarrow{reset} \textsc{Off}.$$

Hence, by the rule for choice,

$$pull.\textsc{Broken} + reset.\textsc{Off} \xrightarrow{pull} \textsc{Broken} \quad \text{and}$$
$$pull.\textsc{Broken} + reset.\textsc{Off} \xrightarrow{reset} \textsc{Off}.$$

As $\textsc{Broken} \stackrel{\text{def}}{=} pull.\textsc{Broken} + reset.\textsc{Off}$, the rule for Process Variables gives us to infer our result:

$$\textsc{Broken} \xrightarrow{pull} \textsc{Broken} \quad \text{and}$$
$$\textsc{Broken} \xrightarrow{reset} \textsc{Off}.$$

Exercise 11.12 (page 297)

$$\texttt{Cl}_* \stackrel{\text{def}}{=} \texttt{tick.Cl}_* + \texttt{tick.Cl}_0.$$

Exercise 11.13 (page 298)

1.

$$C_n \stackrel{\text{def}}{=} \begin{cases} i5.C_5 + i10.C_{10} + i20.C_{20}, & \text{if } n = 0; \\ d1.C_0, & \text{if } n = 1; \\ d1.C_{n-1} + d2.C_{n-2}, & \text{if } 2 \leq n \leq 4; \\ d1.C_{n-1} + d2.C_{n-2} + d5.C_{n-5}, & \text{if } 5 \leq n \leq 20. \end{cases}$$

2. The transition diagram is depicted in Figure 15.5.

Exercise 11.14 (page 300)

The five states of the second vending machine are:

V_2

$\texttt{10p.coffee.collect.}V_2 \texttt{ + 10p.tea.collect.}V_1$

$\texttt{coffee.collect.}V_2$

$\texttt{tea.collect.}V_2$

$\texttt{collect.}V_2$

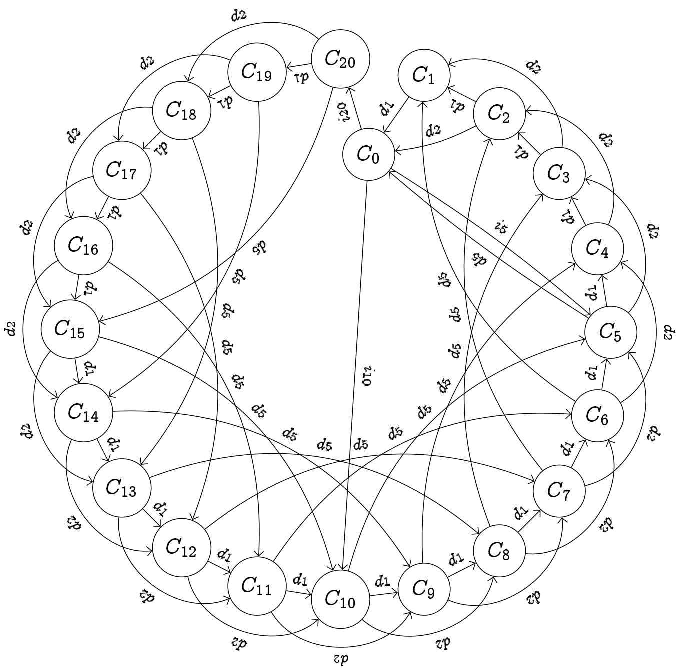


Figure 15.5: The LTS of the change-making machine.

The six states of the third vending machine are:

V_3
`10p.coffee.collect.`V_3
`10p.tea.collect.`V_3
`coffee.collect.`V_3
`tea.collect.`V_3
`collect.`V_3

Exercise 11.15 (page 301)

No matter how we do a 10p action,
we *must* end up in a state in which
  we *may* do a 10p action
  and end up in a state in which
    we *may* do a `tea` action.

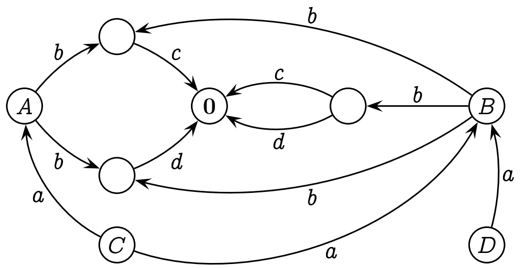


Figure 15.6: The LTS for Exercise 11.16.

Exercise 11.16 (page 301)

1. The transition system is depicted in Figure 15.6.
2. From state C you may do an a action and be in a state in which, no matter how you do a b action you will either not be able to do a c action or you will not be able to do a d action.

   On the other hand, from state D no matter how you do an a action, you will be able to do a b action and end up in a state in which you can both do a c action as well as a d action.

Exercise 11.17 (page 302)

The given definition of equality is:

reflexive: Clearly $E \xrightarrow{a} G$ if, and only if, $E \xrightarrow{a} G$, so $E = E$.

symmetric: Suppose that $E = F$. To show that $F = E$ we need to demonstrate that $F \xrightarrow{a} G$ if, and only if, $E \xrightarrow{a} G$. However, this must be true, as this is exactly the same criterion that makes $E = F$, namely that $E \xrightarrow{a} G$ if, and only if, $F \xrightarrow{a} G$.

transitive: Suppose that $E = F$ and $F = G$. To show that $E = G$ we need to demonstrate that $E \xrightarrow{a} H$ if, and only if, $G \xrightarrow{a} H$. However,

$$\begin{aligned} E \xrightarrow{a} H \text{ if, and only if, } & F \xrightarrow{a} H && (\text{since } E = F) \\ \text{if, and only if, } & G \xrightarrow{a} H && (\text{since } F = G). \end{aligned}$$

Exercise 11.18 (page 303)

The only way to infer that $A = A_0$ would be to first show that $a.A = a.A_1$, which would require us to show that $A = A_1$.

However, the only way to infer that $A = A_1$ would be to first show that $a.A = a.A_2$, which would require us to show that $A = A_2$.

Likewise, the only way to infer that $A = A_2$ would be to first show that $a.A = a.A_3$, which would require us to show that $A = A_3$.

Continuing in this fashion, we would never finish, and so we could never reach our goal of inferring that $A = A_0$.

Chapter 12

Exercise 12.2 (page 312)

Fact: For any games $G_n(E, F)$, either the first player has a winning strategy, or the second player has a winning strategy.

Proof: By induction on n.

For the base case, the second player clearly has a winning strategy for any game $G_0(E, F)$ of length n=0.

For the inductive case, assume that for any game $G_n(E', F')$ of length n, either the first player has a winning strategy, or the second player has a winning strategy. Suppose then that the following two properties hold:

- for all actions a and all states E', if $E \xrightarrow{a} E'$ then $F \xrightarrow{a} F'$ for some state F' such that the second player has a winning strategy for the game $G_n(E', F')$; and
- for all actions a and all states F', if $F \xrightarrow{a} F'$ then $E \xrightarrow{a} E'$ for some state E' such that the second player has a winning strategy for the game $G_n(E', F')$.

That is, suppose that no matter what the first player does as her first move in the game $G_{n+1}(E, F)$ – either a move $E \xrightarrow{a} E'$ or a move $F \xrightarrow{a} F'$ – the second player can respond in such a way that he gets into a position in which he has a winning strategy in the game of length n. This clearly defines a winning strategy for the second player in the game $G_{n+1}(E, F)$.

Hence, if the second player does *not* have a winning strategy in the game $G_{n+1}(E, F)$, then one of the above two properties fails to hold. That is, either

- $E \xrightarrow{a} E'$ in such a way that whenever $F \xrightarrow{a} F'$ the second player does not have a winning strategy in the game $G_n(E', F')$; but then by the inductive hypothesis, this implies that the first player has a winning strategy in the game $G_n(E', F')$, which means she can use the $E \xrightarrow{a} E'$ transition as the first move in a winning strategy for the game $G_{n+1}(E, F)$; or

- $F \xrightarrow{a} F'$ in such a way that whenever $E \xrightarrow{a} E'$ the second player does not have a winning strategy in the game $G_n(E', F')$; but then by the inductive hypothesis, this implies that the first player has a winning strategy in the game $G_n(E', F')$, which means she can use the $F \xrightarrow{a} F'$ transition as the first move in a winning strategy for the game $G_{n+1}(E, F)$. □

Exercise 12.3 (page 313)

$C \sim_2 D$ (and hence $C \sim_0 D$ and $C \sim_1 D$) since from either C or D you can do an a action and nothing else, and regardless of where that takes you, you will be able to do a b action and nothing else. Therefore the second player can obviously copy whatever two moves the first player makes in the Bisimulation Game when the tokens start on the pair of states (C, D).

$C \not\sim_3 D$ (and hence $C \not\sim_n D$ for all $n{\geq}3$) since the first player has a strategy which will win her the game within three moves starting from the pair of states (C, D):

- For her first move she can do $C \xrightarrow{a} A$, to which the second player would have to respond with $D \xrightarrow{a} B$; the two tokens will then be on the pair of states (A, B).
- For her second move she could then do $B \xrightarrow{b} c.\mathbf{0} + d.\mathbf{0}$, to which the second player would have to respond with either with $A \xrightarrow{b} c.\mathbf{0}$ or with $A \xrightarrow{b} d.\mathbf{0}$; the two tokens will then be on the pair of states $(c.\mathbf{0}, c.\mathbf{0} + d.\mathbf{0})$ or the pair of states $(d.\mathbf{0}, c.\mathbf{0} + d.\mathbf{0})$.
- For her third move, if the tokens are on the pair of states $(c.\mathbf{0}, c.\mathbf{0}{+}d.\mathbf{0})$ then she should do $c.\mathbf{0} + d.\mathbf{0} \xrightarrow{d} \mathbf{0}$, and if the tokens are on the pair of state $(d.\mathbf{0}, c.\mathbf{0} + d.\mathbf{0})$ then she should do $c.\mathbf{0} + d.\mathbf{0} \xrightarrow{c} \mathbf{0}$; in either case the second player will not be able to respond.

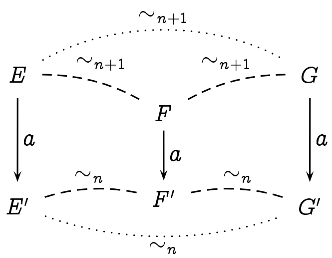
Exercise 12.4 (page 315)

Fact: For all $n \in \mathbb{N}$, and for all states E, F, and G, if $E \sim_n F$ and $F \sim_n G$ then $E \sim_n G$.

Proof: By induction on $n \in \mathbb{N}$.

For the base case $n{=}0$, Theorem 12.3(1) gives us that $E \sim_0 G$.

For the induction step, we assume that $E \sim_{n+1} F$ and $F \sim_{n+1} G$. Referring to the pictorial representations of Theorem 12.3 (page 313), for the induction step the argument will be based on the following picture:



Suppose that the first player makes a transition $E \xrightarrow{a} E'$. By Theorem 12.3(2), since $E \sim_{n+1} F$ we have that $F \xrightarrow{a} F'$ for some F' such that $E' \sim_n F'$; and hence again by Theorem 12.3(2) since $F \sim_{n+1} G$ we have that $G \xrightarrow{a} G'$ for some G' such that $F' \sim_n G'$. Thus, by induction $E' \sim_n G'$. In summary,

- If $E \xrightarrow{a} E'$ then $G \xrightarrow{a} G'$ for some G' such that $E' \sim_n G'$.

Suppose instead that the first player makes a transition $G \xrightarrow{a} G'$. By Theorem 12.3(2), since $F \sim_{n+1} G$ we have that $F \xrightarrow{a} F'$ for some F' such that $F' \sim_n G'$; and hence again by Theorem 12.3(2) since $E \sim_{n+1} F$ we have that $E \xrightarrow{a} E'$ for some E' such that $E' \sim_n F'$. Thus, by induction $E' \sim_n G'$. In summary,

- If $G \xrightarrow{a} G'$ then $E \xrightarrow{a} E'$ for some E' such that $E' \sim_n G'$.

These two bullet points, by Theorem 12.3(2), gives us that $E \sim_{n+1} G$. □

Exercise 12.5 (page 315)

Fact: For all $n \in \mathbb{N}$, $\mathtt{Cl}_n \sim_n \mathtt{Cl}$, while $\mathtt{Cl}_n \not\sim_{n+1} \mathtt{Cl}$.

Proof: We can show the equivalence by induction on n.

Base Case: $\mathtt{Cl}_0 \sim_0 \mathtt{Cl}$, by Theorem 12.3(1).

Induction Step: Assuming, for some n, that $\mathtt{Cl}_n \sim_n \mathtt{Cl}$, we can conclude from Theorem 12.3(2) that $\mathtt{Cl}_{n+1} \sim_{n+1} \mathtt{Cl}$

The inequivalence follows from noting that in the bisimulation game played with the tokens on $\mathtt{Cl}_n$ and $\mathtt{Cl}$, after an exchange of n moves the tokens will necessarily be on $\mathtt{Cl}_0$ and $\mathtt{Cl}$, and the first person will be able to make the move $\mathtt{Cl} \xrightarrow{tick} \mathtt{Cl}$ which the second person cannot match. □

Fact: For all $n \in \mathbb{N}$, $\mathtt{Clock} \sim_n \mathtt{Clock}_\star$, while $\mathtt{Clock} \not\sim_\infty \mathtt{Clock}_\star$.

Proof: We can firstly note that if the first player is to have any chance of winning the bisimulation game with the tokens on the states Clock and $\texttt{Clock}_\star$, then he must start with the move $\texttt{Clock}_\star \xrightarrow{tick} \texttt{Cl}$; the second player could respond to any other opening move in such a way as to leave the two tokens on the same state, leaving him with the obvious copycat strategy to win.

In response to this opening move $\texttt{Clock}_\star \xrightarrow{tick} \texttt{Cl}$, the second player can move $\texttt{Clock} \xrightarrow{tick} \texttt{Cl}_n$; and since (from above) $\texttt{Cl}_n \sim_n \texttt{Cl}$ for all n, by Theorem 12.3(2) we can deduce that $\texttt{Clock} \sim_n \texttt{Clock}_\star$ for all n.

The inequivalence follows from the fact (from above) that $\texttt{Cl}_n \not\sim_{n+1} \texttt{Cl}$. □

Exercise 12.6 (page 317)

To prove that $\mathcal{R}$ is a bisimulation relation, we need to demonstrate that the bisimulation property from Definition 12.5 holds of each of the five pairs of states related by $\mathcal{R}$.

- $(P_1, Q_1) \in \mathcal{R}$:
  - $P_1 \xrightarrow{a} P_2$ is matched by $Q_1 \xrightarrow{a} Q_2$, and vice versa, as $(P_2, Q_2) \in \mathcal{R}$.
  - $P_1 \xrightarrow{a} P_3$ is matched by $Q_1 \xrightarrow{a} Q_3$, and vice versa, as $(P_3, Q_3) \in \mathcal{R}$.
- $(P_2, Q_2) \in \mathcal{R}$:
  - $P_2 \xrightarrow{b} P_3$ is matched by $Q_2 \xrightarrow{b} Q_3$, and vice versa, as $(P_3, Q_3) \in \mathcal{R}$.
- $(P_2, Q_4) \in \mathcal{R}$:
  - $P_2 \xrightarrow{b} P_3$ is matched by $Q_4 \xrightarrow{b} Q_5$, and vice versa, as $(P_3, Q_5) \in \mathcal{R}$.
- $(P_3, Q_3) \in \mathcal{R}$:
  - $P_3 \xrightarrow{b} P_1$ is matched by $Q_3 \xrightarrow{b} Q_1$, and vice versa, as $(P_1, Q_1) \in \mathcal{R}$.
  - $P_3 \xrightarrow{b} P_2$ is matched by $Q_3 \xrightarrow{b} Q_4$, and vice versa, as $(P_2, Q_4) \in \mathcal{R}$.
- $(P_3, Q_5) \in \mathcal{R}$:
  - $P_3 \xrightarrow{b} P_1$ is matched by $Q_5 \xrightarrow{b} Q_1$, and vice versa, as $(P_1, Q_1) \in \mathcal{R}$.
  - $P_3 \xrightarrow{b} P_2$ is matched by $Q_5 \xrightarrow{b} Q_2$, and vice versa, as $(P_2, Q_2) \in \mathcal{R}$.

Exercise 12.7 (page 317)

Assume that $\mathcal{R}$ and $\mathcal{S}$ are bisimulation relations over the states of a labelled transition system, and that $(E, G) \in \mathcal{R} \circ \mathcal{S}$. This means that $E\mathcal{S}F$ and $F\mathcal{R}G$ for some state F.

- If $E \xrightarrow{a} E'$, then from $E\mathcal{S}F$ we get that $F \xrightarrow{a} F'$ for some F' such that

$E'\mathcal{S}F'$; and thus from $F\mathcal{R}G$ we get that $G \xrightarrow{a} G'$ for some G' such that $F'\mathcal{R}G'$ and hence such that $(E', G') \in \mathcal{R} \circ \mathcal{S}$.

- If $G \xrightarrow{a} G'$, then from $F\mathcal{R}G$ we get that $F \xrightarrow{a} F'$ for some F' such that $F'\mathcal{R}G'$; and thus from $E\mathcal{R}F$ we get that $E \xrightarrow{a} E'$ for some E' such that $E'\mathcal{R}F'$ and hence such that $(E', G') \in \mathcal{R} \circ \mathcal{S}$.

Thus $\mathcal{R} \circ \mathcal{S}$ is a bisimulation relation.

Exercise 12.8 (page 318)

Let $E \prec_n F$ (where n may be ∞) mean that the second player has a winning strategy in the n-round game in which the first player must always move the token which starts on state E. Then clearly $\asymp_n = \prec_n \cap \prec_n^{-1}$.

(a) $\asymp_n$ is an equivalence relation, as it is:

reflexive: If both tokens are on the same node, then the second player has the obvious winning strategy of following the lead of the first player, copying each move.

symmetric: This follows from the fact that $\asymp_n = \prec_n \cap \prec_n^{-1}$.

transitive: We first show, by induction on n, that $E \prec_n G$ whenever $E \prec_n F$ and $F \prec_n G$. If $n = 0$ then we immediately have that $E \prec_n G$, so suppose $n = k+1$, and suppose that the first player makes a transition $E \xrightarrow{a} E'$; then we must have that $F \xrightarrow{a} F'$ with $E' \prec_n F'$, and thus we have that $G \xrightarrow{a} G'$ with $F' \prec_n G'$; hence by induction $E \prec_{n+1} G$.

To demonstrate that $\prec_\infty$ is transitive, we modify Definition 12.5 (page 316) to define a ***simulation relation*** to be a binary relation $\mathcal{R}$ over states which satisfies the following property: if $E\mathcal{R}F$ then

– if $E \xrightarrow{a} E'$ then $F \xrightarrow{a} F'$ for some F' such that $E'\mathcal{R}F'$.

We then rephrase Theorem 12.6 (page 316) as

> The second player has a winning strategy in an infinite simulation game with the tokens starting on states E and F if, and only if, $E\mathcal{R}F$ for some simulation relation $\mathcal{R}$. Hence in particular, $\mathcal{R} \subseteq \prec_\infty$ for any simulation relation $\mathcal{R}$.

The proof of this result is completely analogous to that for Theorem 12.6. Our result then follows by showing that $\mathcal{R} \circ \mathcal{S}$ is a simulation relation whenever $\mathcal{R}$ and $\mathcal{S}$ are: this is shown as for the solution to Exercise 12.7.

Assume then that $\mathcal{R}$ and $\mathcal{S}$ are simulation relations, and that $(E, G) \in \mathcal{R} \circ \mathcal{S}$. This means that $E\mathcal{S}F$ and $F\mathcal{R}G$ for some state F.

If $E \xrightarrow{a} E'$, then from $E\mathcal{S}F$ we get that $F \xrightarrow{a} F'$ for some F' such that $E'\mathcal{S}F'$; and thus from $F\mathcal{R}G$ we get that $G \xrightarrow{a} G'$ for some G' such that $F'\mathcal{R}G'$ and hence such that $(E', G') \in \mathcal{R} \circ \mathcal{S}$.

Thus $\mathcal{R} \circ \mathcal{S}$ is a simulation relation.

(b) If the second player has a winning strategy in the bisimulation game, then he can use this same strategy to win the new game. The new game only restricts the possible moves of the first player

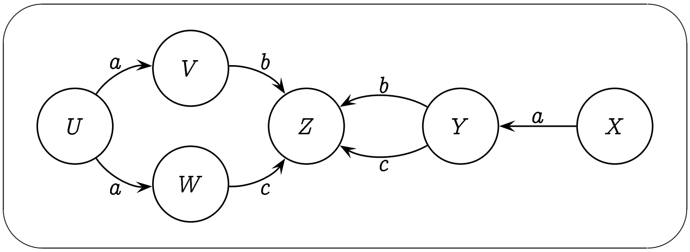
(c) It is easily verified that $a.b.\mathbf{0} \not\preceq_2 a.b.\mathbf{0} + a.\mathbf{0}$, while $a.b.\mathbf{0} \asymp_2 a.b.\mathbf{0} + a.\mathbf{0}$.

Exercise 12.9 (page 321)

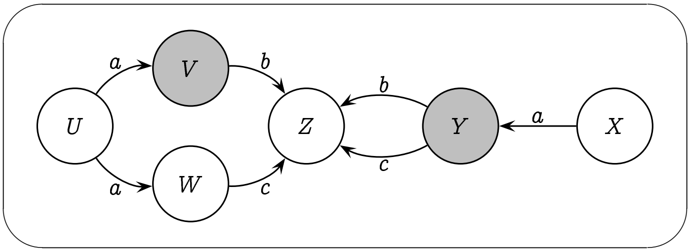
Suppose, by way of contradiction, that the first transition system of Figure 12.1 is coloured with a bisimulation colouring which assigns the same colour to the two states X and U. Since $U \xrightarrow{a} V$, there must be an a-labelled transition out of X leading to a state with the same colour as V. This state must be Y, and hence V and Y must have the same colour in this supposed bisimulation colouring. But then since $Y \xrightarrow{c} Z$, there must be a c-labelled transition out of V leading to a state with the same colour as Z. However, there is no such state, of any colour, which provides us with our desired contradiction.

Exercise 12.10 (page 322)

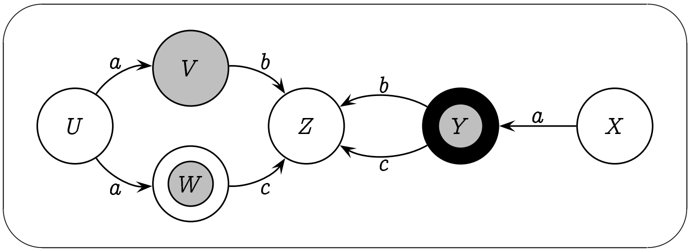
Consider the first transition system of Figure 12.1.



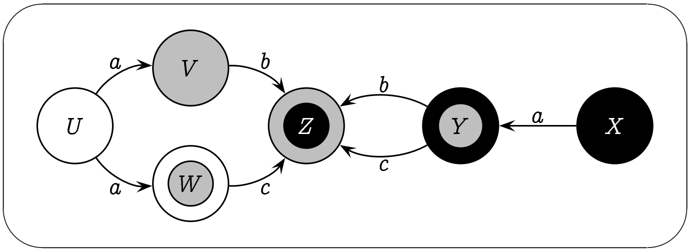
The initial all-white colouring is *not* a bisimulation colouring, as the white states V and Y have b-transition to white states, whereas the other white states U, W, X and Z do not have b-transitions to white states. Hence, by the invariant, states V and Y cannot be equivalent to the other white states; in any bisimulation colouring, states V and Y must each have a different colour from states U, W, X and Z. Hence we may safely refine our colouring by making states V and Y a different colour (gray, say).



This is still not a bisimulation colouring, as the gray states Y has a c-transitions to a white, whereas the other white state V does not. Hence, by the invariant, states V and Y cannot be equivalent, and so we may safely refine our colouring by making Y a different colour, say gray-on-black. At the same time we can note that the white state W has a c-transitions to a white, whereas the other white states U, X and Z do not, and so we can safely make W a different colour, say gray-on white.



Again this is still not a bisimulation colouring, as the white states U has an a-transitions to a gray state, whereas the other white states X and Z do not; and the white state X has an a-transition to a gray-on-black state, whereas the other white states U and Z do not. Hence, we may safely refine our colouring by making X a different colour, say black, and Z a different colour, say black-on-gray.



This colouring *is* a bisimulation colouring, which by construction satisfies our invariant. That it is a bisimulation colouring is clear, since there are no two states with the same colour.

Exercise 12.11 (page 326)

Take:

$$E_0 \stackrel{\text{def}}{=} \texttt{Clock} \qquad F_0 \stackrel{\text{def}}{=} \texttt{Clock}_\star$$

$$E_{n+1} \stackrel{\text{def}}{=} tick.E_n \qquad F_{n+1} \stackrel{\text{def}}{=} tick.F_n$$

By a straightforward induction argument we can show that, for each $n \in \mathbb{N}$, $E_n \sim_{\omega+n} F_n$ but $E_n \not\sim_{\omega+n+1} F_n$.

Chapter 13

Exercise 13.1 (page 336)

1. $\langle \texttt{coffee} \rangle$true says:

   we may do a '`coffee`' action and end up in a state in which true is true.

   This property will be true if it is possible to do a '`coffee`' action.

2. $\langle \texttt{coffee} \rangle$false says:

   we may do a '`coffee`' action and end up in a state in which false is true.

   Such a '`coffee`' action cannot therefore be possible, as false could not possibly be true in any subsequent state. Therefore this property can never be satisfied; it is equivalent to the property false.

3. $[\texttt{coffee}]$true says:

   no matter how we do a '`coffee`' action, we must end up in a state in which true is true.

   This property will always be true – regardless of whether or not we can do a '`coffee`' action – as true will of course be true in any subsequent state. This property is therefore equivalent to the property true.

4. $[\texttt{coffee}]$false says:

   no matter how we do a '`coffee`' action, we must end up in a state in which false is true.

   A '`coffee`' action must therefore not be possible, since false can never be true in any subsequent state. This formula thus says the same thing as $\neg\langle \texttt{coffee} \rangle$true.

Exercise 13.2 (page 336)

$\neg\langle a \rangle \langle a \rangle$true.

In words, this says that it is *not* the case that I can do an 'a' action and get into a state in which I can do another 'a' action.

Exercise 13.3 (page 336)

$[\texttt{tick}]\langle\texttt{tick}\rangle\mathsf{true}$.

In words, this says that no matter how I do a '`tick`' action, I must end up in a state in which I can do another '`tick`' action. This is true of the clock `Cl` but not of the clock $\texttt{Cl}_\star$, as the latter clock may stop after just one tick.

Exercise 13.4 (page 340)

1, 4, 5, 6, 7 and 10 are valid, whereas 2, 3, 8, 9, 11 and 12 are not valid.

Exercise 13.5 (page 341)

1. $\langle \mathit{pull}\rangle\langle \mathit{pull}\rangle\langle \mathit{break}\rangle\mathsf{true}$.

   This is true only of the state ON.

2. $\langle \mathit{pull}\rangle\langle \mathit{pull}\rangle\langle \mathit{reset}\rangle\mathsf{true}$.

   This is true only of the state BROKEN.

3. $\neg\langle \mathit{pull}\rangle\mathsf{true}$.

   This is not true of any state; you can do a '*pull*' action from any state.

4. $\langle \mathit{pull}\rangle\mathsf{true} \ \wedge\ \neg\langle \mathit{break}\rangle\mathsf{true} \ \wedge\ \neg\langle \mathit{reset}\rangle\mathsf{true}$.

   This is true only of the state OFF.

   Note that this assumes that the only actions available of the process are '*pull*', '*break*' and '*reset*'. We need to include a conjunct $\neg\langle a\rangle\mathsf{true}$ for every action $a \neq \mathit{pull}$ to explicitly disallow the possibility of such an action 'a' being possible.

Exercise 13.6 (page 342)

Fact: $\neg[a]P \ \Leftrightarrow\ \langle a\rangle\neg P$

Proof:
$$\begin{aligned} E \models \neg[a]P &\Leftrightarrow E \not\models [a]P \\ &\Leftrightarrow \neg\forall F\,(E \xrightarrow{a} F \ \Rightarrow\ F \models P) \\ &\Leftrightarrow \exists F\neg(E \xrightarrow{a} F \ \Rightarrow\ F \models P) \\ &\Leftrightarrow \exists F(E \xrightarrow{a} F \ \wedge\ F \not\models P) \\ &\Leftrightarrow \exists F(E \xrightarrow{a} F \ \wedge\ F \models \neg P) \\ &\Leftrightarrow E \models \langle a\rangle\neg P \qquad \Box \end{aligned}$$

Exercise 13.7 (page 343)

Theorem 13.6: For any process E and any property P of **HML**:

1. $E \models \mathsf{pos}(P)$ if, and only if, $E \models P$; and
2. $E \models \mathsf{neg}(P)$ if, and only if, $E \not\models P$.

Proof: By induction on the structure of P. That is, we demonstrate that

1. $E \models \mathsf{pos}(P)$ if, and only if, $E \models P$; and
2. $E \models \mathsf{neg}(P)$ if, and only if, $E \not\models P$

under the assumption that, for any process F and any property Q smaller than P,

1. $F \models \mathsf{pos}(Q)$ if, and only if, $F \models Q$; and
2. $F \models \mathsf{neg}(Q)$ if, and only if, $F \not\models Q$.

We thus argue by cases on the structure of P:

$\underline{P = \mathsf{true}}$:

1. $E \models \mathsf{pos}(\mathsf{true})$

   $\Leftrightarrow$ $E \models \mathsf{true}$ [*by definition of* $\mathsf{pos}(\mathit{true})$]

2. $E \models \mathsf{neg}(\mathsf{true})$

   $\Leftrightarrow$ $E \models \mathsf{false}$ [*by definition of* $\mathsf{neg}(\mathit{true})$]

   $\Leftrightarrow$ $E \not\models \mathsf{true}$ [*by semantic definition for true and false*]

$\underline{P = \mathsf{false}}$:

1. $E \models \mathsf{pos}(\mathsf{false})$

   $\Leftrightarrow$ $E \models \mathsf{false}$ [*by definition of* $\mathsf{pos}(\mathit{false})$]

2. $E \models \mathsf{neg}(\mathsf{false})$

   $\Leftrightarrow$ $E \models \mathsf{true}$ [*by definition of* $\mathsf{neg}(\mathit{false})$]

   $\Leftrightarrow$ $E \not\models \mathsf{false}$ [*by semantic definition for true and false*]

$\underline{P = \neg Q}$:

1. $E \models \mathsf{pos}(\neg Q)$

   $\Leftrightarrow$ $E \models \mathsf{neg}(Q)$ [*by definition of* $\mathsf{pos}(\neg Q)$]

   $\Leftrightarrow$ $E \not\models Q$ [*by induction hypothesis 2*]

   $\Leftrightarrow$ $E \models \neg Q$ [*by semantic definition for* $\neg$]

2. $E \models \mathsf{neg}(\neg Q)$

   $\Leftrightarrow$ $E \models \mathsf{pos}(Q)$ [*by definition of* $\mathsf{neg}(\neg Q)$]

   $\Leftrightarrow$ $E \models Q$ [*by induction hypothesis 1*]

   $\Leftrightarrow$ $E \not\models \neg Q$ [*by semantic definition for* $\neg$]

<u>$P = Q_1 \wedge Q_2$:</u>

1. $E \models \mathsf{pos}(Q_1 \wedge Q_2)$
$$\begin{array}{lll}
\Leftrightarrow & E \models \mathsf{pos}(Q_1) \wedge \mathsf{pos}(Q_2) & [\textit{by definition of } \mathsf{pos}(Q_1 \wedge Q_2)] \\
\Leftrightarrow & E \models \mathsf{pos}(Q_1) \text{ and } E \models \mathsf{pos}(Q_2) & [\textit{by semantic definition for } \wedge] \\
\Leftrightarrow & E \models Q_1 \text{ and } E \models Q_2 & [\textit{by induction hypothesis 1}] \\
\Leftrightarrow & E \models Q_1 \wedge Q_2 & [\textit{by semantic definition for } \wedge]
\end{array}$$

2. $E \models \mathsf{neg}(Q_1 \wedge Q_2)$
$$\begin{array}{lll}
\Leftrightarrow & E \models \mathsf{neg}(Q_1) \vee \mathsf{neg}(Q_2) & [\textit{by definition of } \mathsf{neg}(Q_1 \wedge Q_2)] \\
\Leftrightarrow & E \models \mathsf{neg}(Q_1) \text{ or } E \models \mathsf{neg}(Q_2) & [\textit{by semantic definition for } \vee] \\
\Leftrightarrow & E \not\models Q_1 \text{ or } E \not\models Q_2 & [\textit{by induction hypothesis 2}] \\
\Leftrightarrow & \neg(E \models Q_1 \text{ and } E \models Q_2) & [\textit{by De Morgan's Law}] \\
\Leftrightarrow & E \not\models Q_1 \wedge Q_2 & [\textit{by semantic definition for } \wedge]
\end{array}$$

<u>$P = Q_1 \vee Q_2$:</u>

1. $E \models \mathsf{pos}(Q_1 \vee Q_2)$
$$\begin{array}{lll}
\Leftrightarrow & E \models \mathsf{pos}(Q_1) \vee \mathsf{pos}(Q_2) & [\textit{by definition of } \mathsf{pos}(Q_1 \vee Q_2)] \\
\Leftrightarrow & E \models \mathsf{pos}(Q_1) \text{ or } E \models \mathsf{pos}(Q_2) & [\textit{by semantic definition for } \vee] \\
\Leftrightarrow & E \models Q_1 \text{ or } E \models Q_2 & [\textit{by induction hypothesis 1}] \\
\Leftrightarrow & E \models Q_1 \vee Q_2 & [\textit{by semantic definition for } \vee]
\end{array}$$

2. $E \models \mathsf{neg}(Q_1 \vee Q_2)$
$$\begin{array}{lll}
\Leftrightarrow & E \models \mathsf{neg}(Q_1) \wedge \mathsf{neg}(Q_2) & [\textit{by definition of } \mathsf{neg}(Q_1 \vee Q_2)] \\
\Leftrightarrow & E \models \mathsf{neg}(Q_1) \text{ and } E \models \mathsf{neg}(Q_2) & [\textit{by semantic definition for } \wedge] \\
\Leftrightarrow & E \not\models Q_1 \text{ and } E \not\models Q_2 & [\textit{by induction hypothesis 2}] \\
\Leftrightarrow & \neg(E \models Q_1 \text{ or } E \models Q_2) & [\textit{by De Morgan's Law}] \\
\Leftrightarrow & E \not\models Q_1 \vee Q_2 & [\textit{by semantic definition for } \vee]
\end{array}$$

<u>$P = \langle a \rangle Q$:</u>

1. $E \models \mathsf{pos}(\langle a \rangle Q)$

$\Leftrightarrow\ E \models \langle a\rangle\mathsf{pos}(Q)$ [*by definition of* $\mathsf{pos}(\langle a\rangle Q)$]

$\Leftrightarrow\ F \models \mathsf{pos}(Q)$ for some F such that $E \xrightarrow{a} F$

[*by semantic definition for* $\langle a\rangle$]

$\Leftrightarrow\ F \models Q$ for some F such that $E \xrightarrow{a} F$

[*by induction hypothesis 1*]

$\Leftrightarrow\ E \models \langle a\rangle Q$ [*by semantic definition for* $\langle a\rangle$]

2. $E \models \mathsf{neg}(\langle a\rangle Q)$

$\Leftrightarrow\ E \models [a]\mathsf{neg}(Q)$ [*by definition of* $\mathsf{neg}(\langle a\rangle Q)$]

$\Leftrightarrow\ F \models \mathsf{neg}(Q)$ for all F such that $E \xrightarrow{a} F$

[*by semantic definition for* $[a]$]

$\Leftrightarrow\ F \not\models Q$ for all F such that $E \xrightarrow{a} F$

[*by induction hypothesis 2*]

$\Leftrightarrow\ E \not\models \langle a\rangle Q$ [*by semantic definition for* $\langle a\rangle$]

$\underline{P = [a]Q}$:

1. $E \models \mathsf{pos}([a]Q)$

$\Leftrightarrow\ E \models [a]\mathsf{pos}(Q)$ [*by definition of* $\mathsf{pos}([a]Q)$]

$\Leftrightarrow\ F \models \mathsf{pos}(Q)$ for all F such that $E \xrightarrow{a} F$

[*by semantic definition for* $[a]$]

$\Leftrightarrow\ F \models Q$ for all F such that $E \xrightarrow{a} F$

[*by induction hypothesis 1*]

$\Leftrightarrow\ E \models [a]Q$ [*by semantic definition for* $[a]$]

2. $E \models \mathsf{neg}([a]Q)$

$\Leftrightarrow\ E \models \langle a\rangle\mathsf{neg}(Q)$ [*by definition of* $\mathsf{neg}([a]Q)$]

$\Leftrightarrow\ F \models \mathsf{neg}(Q)$ for some F such that $E \xrightarrow{a} F$

[*by semantic definition for* $\langle a\rangle$]

$\Leftrightarrow\ F \not\models Q$ for some F such that $E \xrightarrow{a} F$

[*by induction hypothesis 2*]

$\Leftrightarrow\ E \not\models [a]Q$ [*by semantic definition for* $[a]$]

$\square$

Exercise 13.8 (page 343)

Fact: For all modal properties P, $\mathsf{neg}(\mathsf{neg}(P)) = P$.

Proof: By induction on the structure of P, arguing by cases on the structure of P.

$\underline{P = \textbf{true}}$: $\mathsf{neg}(\mathsf{neg}(\mathsf{true})) = \mathsf{neg}(\mathsf{false}) = \mathsf{true}$.

$\underline{P = \textbf{false}}$: $\mathsf{neg}(\mathsf{neg}(\mathsf{false})) = \mathsf{neg}(\mathsf{true}) = \mathsf{false}$.

$\underline{P = Q_1 \wedge Q_2}$: By the inductive hypothesis we assume that $\mathsf{neg}(\mathsf{neg}(Q_1)) = Q_1$ and $\mathsf{neg}(\mathsf{neg}(Q_2)) = Q_2$.

Then $\mathsf{neg}(\mathsf{neg}(Q_1 \wedge Q_2)) = \mathsf{neg}(\mathsf{neg}(Q_1) \vee \mathsf{neg}(Q_2)) = \mathsf{neg}(\mathsf{neg}(Q_1)) \wedge \mathsf{neg}(\mathsf{neg}(Q_2)) = Q_1 \wedge Q_2$

$\underline{P = Q_1 \vee Q_2}$: By the inductive hypothesis we assume that $\mathsf{neg}(\mathsf{neg}(Q_1)) = Q_1$ and $\mathsf{neg}(\mathsf{neg}(Q_2)) = Q_2$.

Then $\mathsf{neg}(\mathsf{neg}(Q_1 \vee Q_2)) = \mathsf{neg}(\mathsf{neg}(Q_1) \wedge \mathsf{neg}(Q_2)) = \mathsf{neg}(\mathsf{neg}(Q_1)) \vee \mathsf{neg}(\mathsf{neg}(Q_2)) = Q_1 \vee Q_2$

$\underline{P = \langle a \rangle Q}$: By the inductive hypothesis we assume that $\mathsf{neg}(\mathsf{neg}(Q)) = Q$.

Then $\mathsf{neg}(\mathsf{neg}(\langle a \rangle Q)) = \mathsf{neg}([a]\mathsf{neg}(Q)) = \langle a \rangle \mathsf{neg}(\mathsf{neg}(Q)) = \langle a \rangle Q$

$\underline{P = [a]Q}$: By the inductive hypothesis we assume that $\mathsf{neg}(\mathsf{neg}(Q)) = Q$.

Then $\mathsf{neg}(\mathsf{neg}([a]Q)) = \mathsf{neg}(\langle a \rangle \mathsf{neg}(Q)) = [a]\mathsf{neg}(\mathsf{neg}(Q)) = [a]Q$

□

Exercise 13.9 (page 345)

The properties distinguishing between C and D were presented informally in the solution to Exercise 11.16(b). We need simply express these properties in the language of **HML**.

- From state C you may do an 'a' action and be in a state in which, no matter how you do a 'b' action you will either not be able to do a 'c' action or you will not be able to do a 'd' action. Formally:

$$C \models \langle a \rangle [b]([c]\mathsf{false} \vee [d]\mathsf{false})$$

- On the other hand, from state D no matter how you do an 'a' action, you will be able to do a 'b' action and end up in a state in which you can both do a 'c' action as well as a 'd' action. Formally:

$$D \models [a]\langle b\rangle(\langle c\rangle\mathsf{true} \wedge \langle d\rangle\mathsf{true})$$

Note that these properties are, naturally, the negations of each other: $D = \mathsf{neg}(C)$ and $C = \mathsf{neg}(D)$.

Exercise 13.11 (page 350)

1. Consider the formula

$$\langle a\rangle\mathsf{true} \;\wedge\; [-a]\mathsf{false} \;\wedge\; [-][-]\mathsf{false}.$$

Clearly this characterises the process $a.\mathbf{0}$:

- The first conjunct says that it is possible to do an a transition;
- The second conjunction says that it is not possible to do anything other than an a transition.
- The final conjunct says that it is not possible to do two transitions.

2. The characteristic formula for $a.(b.\mathbf{0} + c.\mathbf{0})$ is

$$\langle a\rangle\mathsf{true} \;\wedge\; [-a]\mathsf{false} \;\wedge\; [a]\Big(\langle b\rangle\mathsf{true} \;\wedge\; \langle c\rangle\mathsf{true} \;\wedge\; [-][-]\mathsf{false}\Big).$$

Exercise 13.12 (page 353)

1. $||\langle a\rangle\mathsf{true}|| \;=\; \{\, E,\, E_1,\, F \,\}$
2. $||\langle b\rangle\mathsf{true}|| \;=\; \{\, E_1,\, E_2 \,\}$
3. $||\langle a\rangle\langle a\rangle\mathsf{true}|| \;=\; \{\, E,\, E_1 \,\}$
4. $||\langle b\rangle\langle b\rangle\mathsf{true}|| \;=\; \emptyset$
5. $||\langle a\rangle[a]\mathsf{false}|| \;=\; \{\, F \,\}$
6. $||[b]\langle a\rangle\mathsf{true}|| \;=\; \{\, E,\, E_1,\, E_2,\, F \,\}$

Chapter 14

Exercise 14.2 (page 360)

Let $A \stackrel{\text{def}}{=} \mathbf{0}$ with $\mathsf{Sort}(A) = \emptyset$, and $B \stackrel{\text{def}}{=} \mathbf{0}$ with $\mathsf{Sort}(B) = \{a\}$.

Then clearly $A \sim B$ although $\mathsf{Sort}(A) \neq \mathsf{Sort}(B)$.

If we let $X \stackrel{\text{def}}{=} a.\mathbf{0}$ with $\mathsf{Sort}(X) = \emptyset$, then $A \parallel X \sim a.\mathbf{0}$, but $B \parallel X \sim \mathbf{0}$.

Thus, $A \sim B$ whereas $A \parallel X \not\sim B \parallel X$.

Exercise 14.3 (page 362)

The relevant bisimulation relation is

$$\Big\{(\mathrm{C}_2, \mathrm{C} \parallel \mathrm{C}),\ (\mathrm{C}'_2, \mathit{dec}.\mathrm{C} \parallel \mathrm{C}),\ (\mathrm{C}'_2, \mathrm{C} \parallel \mathit{dec}.\mathrm{C}),\ (\mathrm{C}''_2, \mathit{dec}.\mathrm{C} \parallel \mathit{dec}.\mathrm{C})\ \Big\}.$$

Exercise 14.4 (page 365)

The safety property holds: a car may cross only if the barrier is up, and a train may cross only if the signal is green; and the controller ensures that the barrier is never up at the same time that the signal is green by raising the barrier only when the signal is red and turning the signal green only when the barrier is down.

The liveness properties, however, fail to hold as given. When a car arrives, it is not necessarily the case that the barrier will eventually go up. It may be the case that an endless stream of trains arrive, and that the controller repeatedly turns the signal green to allow each of these trains to cross the intersection without ever raising the barrier to allow the waiting car to pass. Equally, the controller may allow an endless stream of cars to pass, never changing the signal to green to allow a waiting train to pass.

These liveness properties can be weakened to read:

- If a car arrives, eventually the barrier may go up.
- If a train arrives, eventually the signal may turn green.

These weakened properties do hold of the system.

In reality, a barrier typically remains up, to allow cars to cross the intersection freely, until a train arrives; the arrival of a train signals the controller, which then lowers the barrier, then turns the signal to green, then turns the signal to red again, and finally raises the barrier once again. If the components are built correctly following this protocol, then the original liveness properties will hold, along with the safety properties.

Exercise 14.5 (page 368)

The only way that the system can deadlock is if every philosopher is wanting to pick up a fork which is not available. (No philosopher would ever be hindered from eating nor from setting a fork down on the table.) No two philosophers can be wanting to pick up the same fork, as each one of them must be prevented from picking it up by the other already holding it. Since each philosopher is stopped by the absence of a different fork, every fork must be in the hand of some philosopher, and thus each philosopher must be in the state of having just picked up their first fork. But that would mean that philosophers 1 and 2 are both holding fork 2, which is impossible.

Exercise 14.6 (page 371)

We argue that if the first process reaches the state where it is ready to enter the critical section, then the second process will not be able to reach the analogous state until the first process enters and then exist the critical section. A symmetric argument shows that the second process being in the critical section prevents the first from also being so.

- When the first process becomes ready to enter the critical section (ie, enters state R_1), then the b1 process must be in the state B_1t, and either the b2 process is in the state B_2f or the k processor is in the state K_1.
- Before the first process enters and exists the critical section, if the second process is waiting to be allowed to enter the critical section (ie, is in state W_2), then the b2 process must be in state B_2t. Hence (from above) the k processor is in the state K_1. Thus this process will not be able to move to state R_2 and enter the critical section.

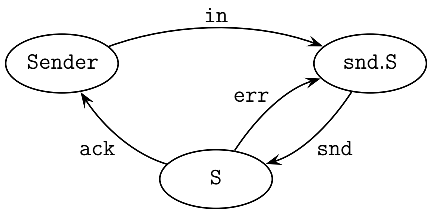
Exercise 14.7 (page 373)

The enhanced message-passing protocol requires no change to the SENDER, only to the RECEIVER and the MEDIUM. The acknowledgement that the SENDER is awaiting will come from the MEDIUM rather than directly from the RECEIVER, but this difference is not noticeable from the point of view of the SENDER. Thus its definition remains unchanged:

$$\mathsf{Sender} \stackrel{\text{def}}{=} \mathtt{in}.\mathtt{snd}.\mathsf{S} \qquad \mathsf{S} \stackrel{\text{def}}{=} \mathtt{ack}.\mathsf{Sender} + \mathtt{err}.\mathtt{snd}.\mathsf{S}$$

$$\mathsf{Sort}(\mathsf{Sender}) = \{\mathtt{snd}, \mathtt{ack}, \mathtt{err}\}$$

Again, its transition system is depicted thus:

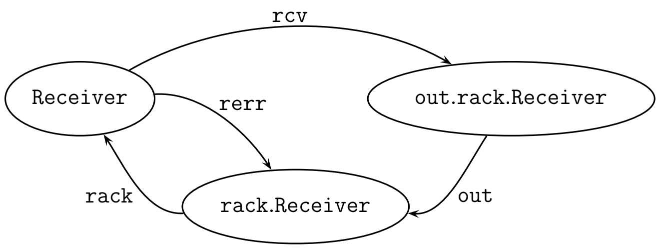


The enhanced RECEIVER must cater for the possibility of its acknowledgement being lost. After receiving a message (via the "rcv" action) and forwarding it on (via the "out" action), it will issue an auxiliary acknowledgement to the MEDIUM (via a "rack" action). At this point it will be ready to receive a new message. However, it may instead receive an auxiliary error message from the MEDIUM (modelled by a "rerr" action), indicating that the acknowledgement was lost, in which case it will retransmit this acknowledgement. The new definition is as follows:

$$\texttt{Receiver} \stackrel{\text{def}}{=} \texttt{rcv.out.rack.Receiver} + \texttt{rerr.rack.Receiver}$$

$$\text{Sort}(\texttt{Receiver}) = \{\texttt{rcv}, \texttt{rack}, \texttt{rerr}\}$$

Its transition system is depicted thus:



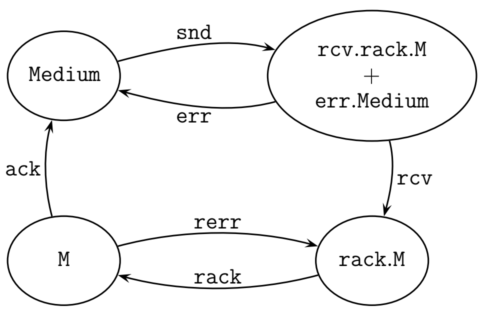
The behaviour of the MEDIUM must now interact with the RECEIVER in delivering the acknowledgement from the RECEIVER to the SENDER of the safe arrival of the message being delivered. After passing the message to the RECEIVER (via the "rcv" action), the Medium awaits the auxiliary acknowledgement from the RECEIVER (modelled by the "rack" action). It then either passes the acknowledgement along to the SENDER (via the "ack" action); or it may lose the acknowledgement (modelled by a "rerr" action), and await a new acknowledgement from the RECEIVER. The new definition is as follows:

$$\texttt{Medium} \stackrel{\text{def}}{=} \texttt{snd.(rcv.rack.M} + \texttt{err.Medium)}$$

$$\texttt{M} \stackrel{\text{def}}{=} \texttt{ack.Medium} + \texttt{rerr.rack.M}$$

$$\text{Sort}(\texttt{Medium}) = \{\texttt{snd}, \texttt{rcv}, \texttt{err}\}$$

Its transition system is depicted thus:



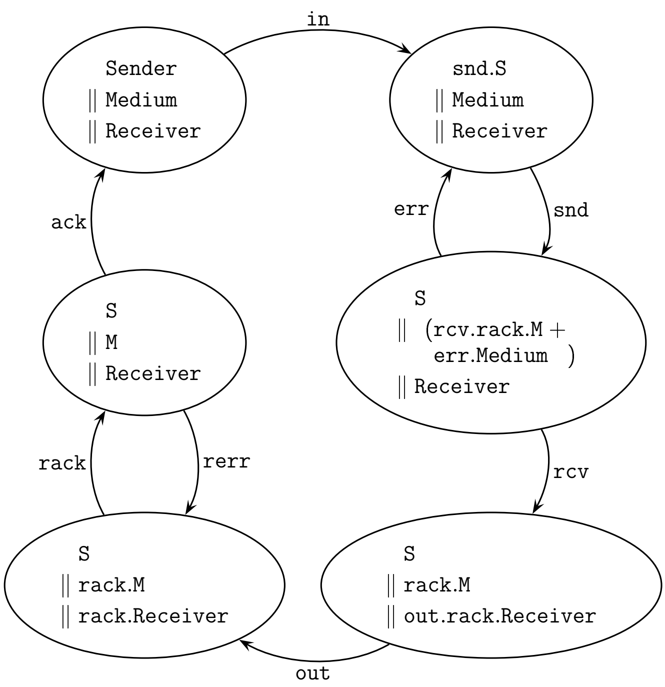


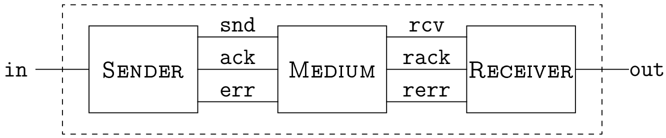
Figure 15.7: The enhanced message-passing system.

The symmetry reflected in the transition diagram makes clear the similarity in the manner that the MEDIUM treats the SENDER and RECEIVER.

The complete system is again defined to be the composition of these three components:

$$\texttt{System} \stackrel{\text{def}}{=} \texttt{Sender} \parallel \texttt{Medium} \parallel \texttt{Receiver}$$

but now the following configuration:



The behaviour of the complete enhanced system is thus depicted by the transition system depicted in Figure 15.7. The symmetry between the SENDER and the RECEIVER is immediately noticeable in this transition system.

Exercise 14.8 (page 377)

- From the state $S_i \parallel M \parallel R_i$ (the initial state being $S_0 \parallel M \parallel R_0$) the system can do an `in` action and nothing else, leaving the system in the state $S_i' \parallel M \parallel R_i$.
- From here, the system will not be able to do a further `in` action until the `Sender` process reaches the state S_{1-i}.
- This can only happen after the `Sender` action synchronises with the `Medium` on an $\mathtt{ack}_i$ action, leaving the `Sender` in the state S_{1-i} and the `Medium` in the state M.
- Until this $\mathtt{ack}_i$ synchronisation occurs, the `Sender` can repeatedly alternate between the actions s_i and t, so the system will not deadlock.
- The `Medium` can only do this $\mathtt{ack}_i$ action after it synchronises with the `Receiver` on a $\mathtt{rack}_i$ action.
- The `Receiver` in turn can only do this $\mathtt{rack}_i$ action after doing an `out` action, and then leaves the `Receiver` in the state R_{1-i}.
- The system will then be in the state $S_{1-i} \parallel M \parallel R_{1-i}$, from which the above argument applies.

Chapter 15

Exercise 15.2 (page 384)

$$\begin{aligned}
\text{Deadlock-free} &= \Box\langle-\rangle\mathsf{true} && \text{(by definition)}\\
&= \neg\Diamond\neg\langle-\rangle\mathsf{true} && (\text{since } \Box P \;=\; \neg\Diamond\neg P)\\
&= \neg\Diamond[-]\mathsf{false} && (\text{since } \neg\langle-\rangle P \;=\; [-]\neg P)\\
&= \neg\text{Deadlockable} && \text{(by definition)}
\end{aligned}$$

Exercise 15.3 (page 385)

$\mathrm{Ev}\, P$ asserts that P must eventually become true.

This is almost the same as $Q \,\mathrm{U}\, P$ which also asserts that P must eventually become true; the only difference is the added requirement that until P becomes true, Q must remain true.

However, this added requirement is vacuous if we take the property Q to be true, as of course true is always true anyways.

Hence, $\mathrm{Ev}\, P \;=\; \mathsf{true}\,\mathrm{U}\, P$.

Exercise 15.4 (page 386)

Fact: $E \models_V P$ if, and only if, $E \in \|P\|_V$.

Proof: By induction on the structure of P, arguing by cases on the structure of P.

$\underline{P = \textbf{true}}$: $E \models_V \text{true} \Leftrightarrow E \in \text{States} \Leftrightarrow E \in \|\text{true}\|_{V[X \mapsto S]}$

$\underline{P = \textbf{false}}$: $E \models_V \text{false} \Leftrightarrow E \in \emptyset \Leftrightarrow E \in \|\text{false}\|_{V[X \mapsto S]}$

$\underline{P = X}$: $E \models_V X \Leftrightarrow E \in V(X) \Leftrightarrow E \in \|X\|_{V[X \mapsto S]}$

$\underline{P = \neg P}$:
$$\begin{aligned} E \models_V \neg P &\Leftrightarrow E \not\models_V P \\ &\Leftrightarrow E \notin \|P\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \overline{\|P\|_{V[X \mapsto S]}} \Leftrightarrow E \in \|\neg P\|_{V[X \mapsto S]} \end{aligned}$$

$\underline{P = Q_1 \wedge Q_2}$:
$$\begin{aligned} E \models_V Q_1 \wedge Q_2 &\Leftrightarrow E \models_V Q_1 \text{ and } E \models_V Q_2 \\ &\Leftrightarrow E \in \|Q_1\|_{V[X \mapsto S]} \text{ and } E \in \|Q_2\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \|Q_1\|_{V[X \mapsto S]} \cap \|Q_2\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \|Q_1 \wedge Q_2\|_{V[X \mapsto S]} \end{aligned}$$

$\underline{P = Q_1 \vee Q_2}$:
$$\begin{aligned} E \models_V Q_1 \vee Q_2 &\Leftrightarrow E \models_V Q_1 \text{ or } E \models_V Q_2 \\ &\Leftrightarrow E \in \|Q_1\|_{V[X \mapsto S]} \text{ or } E \in \|Q_2\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \|Q_1\|_{V[X \mapsto S]} \cup \|Q_2\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \|Q_1 \vee Q_2\|_{V[X \mapsto S]} \end{aligned}$$

$\underline{P = \langle a \rangle Q}$:
$$\begin{aligned} E \models_V \langle a \rangle Q &\Leftrightarrow E \xrightarrow{a} E' \text{ such that } E' \models_V Q \\ &\Leftrightarrow E \xrightarrow{a} E' \text{ such that } E' \in \|Q\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \|\langle a \rangle Q\|_{V[X \mapsto S]} \end{aligned}$$

$\underline{P = [a]Q}$:
$$\begin{aligned} E \models_V [a]Q &\Leftrightarrow E \xrightarrow{a} E' \text{ implies } E' \models_V Q \\ &\Leftrightarrow E \xrightarrow{a} E' \text{ implies } E' \in \|Q\|_{V[X \mapsto S]} \\ &\Leftrightarrow E \in \|[a]Q\|_{V[X \mapsto S]} \end{aligned}$$

□

Exercise 15.5 (page 388)

$$\|\langle a \rangle X\|_{V[X \mapsto \emptyset]} = \{ E \in \text{States} : E \xrightarrow{a} E' \text{ for some } E' \in \emptyset \} = \emptyset.$$

Exercise 15.6 (page 389)

By Exercise 15.5, the empty set $S = \emptyset$ satisfies $S = \|\langle a\rangle X\|_{\mathsf{V}[X\mapsto S]}$ and hence must be the least fixed point of the function $f(S) = \|\langle a\rangle X\|_{\mathsf{V}[X\mapsto S]}$.

Let $A = \{ E \in \mathsf{States} \ : \ E \xrightarrow{a} \cdot \xrightarrow{a} \cdot \xrightarrow{a} \cdots \}$ be the set of states which we intended to capture in Example 15.4 with the recursive property $X = \langle a\rangle X$. As demonstrated in Example 15.4, this set is a fixed point; we shall demonstrate that A must in fact be the greatest fixed point.

To this end, suppose that S is any fixed point:

$$S \ = \ f(S) = \|\langle a\rangle X\|_{\mathsf{V}[X\mapsto S]} \\ = \{ E \in \mathsf{States} \ : \ E \xrightarrow{a} E' \text{ for some } E' \in S \}$$

and suppose further that $E \in S$. We need to show that $E \in A$.

- Since $E \in S$, $E \xrightarrow{a} E'$ for some $E' \in S$.
- Since $E' \in S$, $E' \xrightarrow{a} E''$ for some $E'' \in S$.
- Since $E'' \in S$, $E'' \xrightarrow{a} E'''$ for some $E''' \in S$.

Continuing in this fashion, it becomes clear that $E \in S$.

As for a fixed point of the function $f(S) = \|\langle a\rangle X\|_{\mathsf{V}[X\mapsto S]}$ which is neither the least nor greatest fixed point, consider the process with two states A and B and two transitions $A \xrightarrow{a} A$ and $B \xrightarrow{a} A$. Then $\emptyset$, $\{ A \}$ and $\{ A, B \}$ are all fixed points of this function.

Exercise 15.7 (page 392)

We prove this by induction – and arguing by cases – on the structure of P. However, we only present the three cases which don't appear in the proof of the analogous result for **HML** (Theorem 13.6, page 343).

$\underline{P = X}$:

$$E \models_{\overline{\mathsf{V}}} \mathsf{neg}(X) \ \Leftrightarrow \ E \models_{\overline{\mathsf{V}}} X \ \Leftrightarrow \ E \in \overline{\mathsf{V}}(X) \ \Leftrightarrow \ E \notin \mathsf{V}(X) \ \Leftrightarrow \ E \not\models_{\mathsf{V}} X$$

$\underline{P = \mu X.Q}$:

$$E \models_{\overline{\mathsf{V}}} \mathsf{neg}(\mu X.Q) \ \Leftrightarrow \ E \models_{\overline{\mathsf{V}}} \nu X.\mathsf{neg}(Q)$$
$$\Leftrightarrow \ \exists S \subseteq \mathsf{States} : \ E \in S \text{ and } \forall F \in S : \ F \models_{\overline{\mathsf{V}}[X\mapsto S]} \mathsf{neg}(Q)$$
$$\Leftrightarrow \ \exists S \subseteq \mathsf{States} : \ E \notin S \text{ and } \forall F \notin S : \ F \models_{\overline{\mathsf{V}[X\mapsto S]}} \mathsf{neg}(Q)$$
$$\Leftrightarrow \ \exists S \subseteq \mathsf{States} : \ E \notin S \text{ and } \forall F \notin S : \ F \not\models_{\mathsf{V}[X\mapsto S]} Q$$
$$\Leftrightarrow \ E \not\models_{\mathsf{V}} \mu X.Q$$

$\underline{P = \nu X.Q}$:

$$E \models_{\overline{V}} \mathsf{neg}(\nu X.Q) \;\Leftrightarrow\; E \models_{\overline{V}} \mu X.\mathsf{neg}(Q)$$
$$\Leftrightarrow \forall S \subseteq \mathsf{States} : \text{if } E \notin S \text{ then } \exists F \notin S \text{ such that } F \models_{\overline{V}[X\mapsto S]} \mathsf{neg}(Q)$$
$$\Leftrightarrow \forall S \subseteq \mathsf{States} : \text{if } E \in S \text{ then } \exists F \in S \text{ such that } F \models_{\overline{V[X\mapsto S]}} \mathsf{neg}(Q)$$
$$\Leftrightarrow \forall S \subseteq \mathsf{States} : \text{if } E \in S \text{ then } \exists F \in S \text{ such that } F \not\models_{V[X\mapsto S]} Q$$
$$\Leftrightarrow E \not\models_{V} \nu X.Q \qquad \square$$

Exercise 15.12 (page 399)

1. With a least fixed point, we cannot be allowed to unroll the recursive equation infinitely often in verifying that the property P is true in every state.

   At every state we reach, the property P must hold. But we must eventually have nowhere to go; that it, the process must eventually deadlock.

   Thus this property is true as long as P is true in every state of the process and every run of the process deadlocks.

2. With a greatest fixed point, we are allowed to unroll the recursive property infinitely often in our search for a state in which P is true.

   At each state, either the property P must hold, or it must be possible to make a transition and continue the search for a state in which P holds; however, we need never complete this search.

   Thus this property is true if P is true in some state, or if there is an infinite path through the process.

3. With a greatest fixed point, we are allowed to unroll the recursive property infinitely often in our search for a state in which Q is true.

   Thus the property is true if P is true for as long as Q is not true, but until Q becomes true – if ever – it must be possible to do something.

Exercise 15.13 (page 401)

1. **P almost always holds along some a^ω path.**

   In order for this property to hold, there must be a state reachable by a sequence of a transitions from which an a^ω path exists along which P is always true.

   We have already seen how to express the property that P always holds along some a^ω path:

   $$\Phi \;=\; \nu X.P \;\wedge\; \langle a\rangle X.$$

   We need only find a state satisfying this property which can be reached by a sequence of a-transitions:

$$\mu X.\Phi \ \vee \ \langle a \rangle X.$$

Writing this out in full by substituting in the formula for Φ – whilst at the same time changing one of the variables to avoid confusion – we get the following:

$$\mu Z.\Big(\nu X.P \ \wedge \ \langle a \rangle X\Big) \ \vee \ \langle a \rangle Z.$$

2. **P holds infinitely often along some a^ω path.**

   In order for this property to be true, we must be able to reach a state by doing a sequence of a transitions in which P holds, and then to repeat this forever.

   We will, therefore, have a least fixed point construction – to allow us to look for the state in which P holds – embedded within a greatest fixed point construction – to allow us to repeat this search over and over again forever.

$$\nu Z.\mu X.(P \ \wedge \ \langle a \rangle Z) \ \vee \ \langle a \rangle X.$$

Index

F. Moller, G. Struth, *Modelling Computing Systems*,
Undergraduate Topics in Computer Science,
DOI 10.1007/978-1-84800-322-4, © Springer-Verlag London 2013