SOLUTIONS MANUAL

Logic and Discrete Mathematics

A Concise Introduction

WILLEM CONRADIE
VALENTIN GORANKO
CLAUDETTE ROBINSON

WILEY

Logic and Discrete Mathematics

Logic and Discrete Mathematics

A Concise Introduction, Solutions Manual

Willem Conradie
University of Johannesburg, South Africa

Valentin Goranko
Stockholm University, Sweden

Claudette Robinson
University of Johannesburg, South Africa

Wiley

This edition first published 2015

© 2015 John Wiley and Sons Ltd

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. It is sold on the understanding that the publisher is not engaged in rendering professional services and neither the publisher nor the author shall be liable for damages arising herefrom. If professional advice or other expert assistance is required, the services of a competent professional should be sought

Library of Congress Cataloging-in-Publication Applied Data for.

A catalogue record for this book is available from the British Library.

ISBN: 9781118762677

Set in 9/11pt, PalatinoLTStd by Laserwords Private Limited, Chennai, India

1 2015

Contents

Preface vii

About the Companion Website ix

1. Preliminaries 1

2. Sets, Relations, Orders 5

3. Propositional Logic 29

4. First-Order Logic 57

5. Number Theory 99

6. Combinatorics 130

7. Graph Theory 159

Preface

This manual contains answers and solutions to roughly three quarters of the exercises in *Logic and Discrete Mathematics: A Concise Introduction* by Willem Conradie and Valentin Goranko. Most solutions are worked out in full detail. In deciding which solutions to include we were guided by two principles: fundamental exercises were given preference above the more esoteric ones intended mainly for enrichment; where a number of very similar exercises occur in succession, complete solutions were given for a few while the others were omitted or provided with answers only. We trust that these solutions will be a very valuable resource to students and instructors using *Logic and Discrete Mathematics*.

About the Companion Website

This book is accompanied by a companion website:

www.wiley.com/go/conradie/logic

The website includes:

- Lecture Slides
- Quizzes

1

Preliminaries

1.1. Sets

(1a) $A = \{-1, 4\}$

(1b) $B = \{-5, -3, -\frac{3}{2}, 1\}$

(1c) $C = \{-3, -2, -1, 0, 1, 2\}$

(1d) $D = \{-1\}$

(1e) $E = \{-3, -2, 0, 1, 2\}$

(1f) $F = \{1, 3, 5, 7, 9\}$

(2a) $B = \{x \in \mathbb{R} \mid x^2 - 3 = 0\}$

(2b) $A = \{x \mid x = 2k, \text{ where } k \in \mathbb{Z} \text{ and } 1 \leq k \leq 4\}$

(2c) $A = \{x \mid x = 2k, \text{ where } k \in \mathbb{Z}^+\}$

(2d) $A = \{x \mid x = 3k + 2, \text{ where } k \in \mathbb{Z}\}$

(2e) $A = \{x \mid x = n^3, \text{ where } n \in \mathbb{N}\}$

(2f) $B = \{x \in \mathbb{Z} \mid -3 \leq x \leq 6\}$

(2g) $B = \{x \in \mathbb{Z} \mid x \leq -3 \vee x \geq 5\}$

(3) Only a, d e, g, h and j are true.

(4) Only a, g, j and l are true.

(5a) $A \cap B = \{2, 7\}$

(5b) $A \cup B = \{0, 1, 2, 4, 5, 6, 7, 9\}$

(5c) $A - B = \{1, 4\}$

(5d) $B - A = \{0, 5, 6, 9\}$

(5e) $A - (A - B) = \{2, 7\}$

(5f) $B - (A - B) = B$

(5g) $B' = \{1, 3, 4, 8\}$

(5h) $(A \cap B)' = \{0, 1, 3, 4, 5, 6, 8, 9\}$

(5i) $A \cap B' = \{1, 4\}$

(5j) $(A \cup B)' = \{3, 8\}$

(5k) $(A \cup B)' - (B - A)' = \varnothing$

(6a) $A \cap B = \{0\}$

(6b) $A \cup B = \{0, A\}$

(6c) $B - A = \{A\}$

(6d) $A \cap (B \cup C) = \{0\}$

(6e) $(B \cup C) - A = \{A, \{0\}, \{A\}\}$

(6f) $(A \cap B) \cup (A \cap C) = \{0\}$

(6g) $(C - B) - A = \{\{0\}, \{A\}\}$

(6h) $A \cap (C - A) = \varnothing$

Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

(7) $A \times B = \{(1,0),(1,1),(2,0),(2,1),(3,0),(3,1),(4,0),(4,1)\}$
$B \times A = \{(0,1),(1,1),(0,2),(1,2),(0,3),(1,3),(0,4),(1,4)\}$

(8a) 30 (8c) 5 (8e) 42

(8b) 0 (8d) 0 (8f) 1

(9) Only a and e are graphs of functions.

(10) The right-to-left direction is obvious. For the converse direction, assume $(a_1, a_2) = (b_1, b_2)$. Then $\{\{a_1\}, \{a_1, a_2\}\} = \{\{b_1\}, \{b_1, b_2\}\}$. Hence,

$$\bigcap \{\{a_1\}, \{a_1, a_2\}\} = \bigcap \{\{b_1\}, \{b_1, b_2\}\},$$

and so $\{a_1\} = \{b_1\}$. This means that $a_1 = b_1$. Similarly,

$$\bigcup \{\{a_1\}, \{a_1, a_2\}\} = \bigcup \{\{b_1\}, \{b_1, b_2\}\},$$

which gives $\{a_1, a_2\} = \{b_1, b_2\}$. Thus, since $a_1 = b_1$, $a_2 = b_2$.

(11) Given the objects $a_1, a_2, \ldots, a_n$, the ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is defined by

$$(a_1, (a_2, \ldots, (a_{n-1}, a_n))).$$

1.2. Basics of logical connectives and expressions

(1) a, b, e, f, and h are propositions.

(2a) $A \wedge (\neg B \vee C) = \mathrm{T} \wedge (\neg \mathrm{T} \vee \mathrm{F}) = \mathrm{T} \wedge (\mathrm{F} \vee \mathrm{F}) = \mathrm{T} \wedge \mathrm{F} = \mathrm{F}$

(2e) $C \to (A \to D) = \mathrm{F} \to (\mathrm{T} \to \mathrm{F}) = \mathrm{F} \to \mathrm{F} = \mathrm{T}$

(3a) Denote "The sun is hot." by p, "The earth is larger than Jupiter." by q, and "There is life on Jupiter." by r. Then the composite proposition in symbolic form is $p \wedge (q \to r)$. It is true.

(3b) Denote "The sun rotates around the earth." by p, "The earth rotates around the moon." by q and "The sun rotates around the moon." by r. Then the composite proposition in symbolic form is $p \vee q \to r$. It is true.

(3c) Denote "The moon rotates around the earth." by p, "The sun rotates around the earth." by q and "The earth rotates around the moon." by r. Then the composite proposition in symbolic form is $\neg q \wedge \neg r \to \neg p$. It is false.

(3d) Denote "The earth rotates around itself." by p, "The sun rotates around the earth." by q and "The moon rotates around the earth." by r. Then the composite proposition in symbolic form is $p \to q \vee \neg r$. It is false.

(3e) Denote "The earth rotates around itself." by p, "The sun rotates around itself." by q and "The moon rotates around itself." by r. Then the composite proposition in symbolic form is $p \leftrightarrow (\neg q \vee \neg r)$. It is true.

(4a) Since B is true and $B \to A$ must be true, A must be true.

(4b) Since B is false and $A \to B$ must be true, A must be false.

(4c) B is false since $\neg B$ is true. Hence, since $A \vee B$ must be true, A is true.

(4d) $\neg C$ must be false, and since $\neg B \to \neg C$ is true, $\neg B$ must be false, i.e. B is true. Hence, since $B \to \neg A$ is true, $\neg A$ is true and so A is false.

(4e) Since $\neg C \wedge B$ is true, B and $\neg C$ are true. Hence, C is false. Since $\neg(A \vee C) \to C$ is true and C is false, $\neg(A \vee C)$ is false, i.e. $A \vee C$ is true. Therefore, since C is false, A must be true.

(5a) Not every number is different from 0. True in $\mathcal{R}$ and $\mathcal{N}$.

(5b) Every number is less than or equal to its cube. False in $\mathcal{R}$, take $x = -2$. True in $\mathcal{N}$.

(5c) Every number equal to its square is positive. False in $\mathcal{R}$ and $\mathcal{N}$, take $x = 0$.

(5d) There is a negative number equal to its square. False in both $\mathcal{R}$ and $\mathcal{N}$. The square of any number is always positive.

(5e) Any positive number is less than its square. False in both $\mathcal{R}$ and $\mathcal{N}$, take $x = 1$.

(5f) Every number is either zero or it is not equal to twice itself. True in $\mathcal{R}$ and $\mathcal{N}$.

(5g) For every pair of numbers x and y, one of them is less than the other. False in $\mathcal{R}$ and $\mathcal{N}$, take $x = y$.

(5h) Every number is greater than the square of some number. False in $\mathcal{R}$ and $\mathcal{N}$, as 0 is not greater than any square.

(5i) For every number x, there is a number y that is either positive or whose square is less than x. True in $\mathcal{R}$ and $\mathcal{N}$.

(5j) Every non-negative number is the square of a positive number. False in $\mathcal{R}$ and $\mathcal{N}$, as 0 is not equal to the square of any positive number.

(5k) For every number x, there is a number y such that if x is greater than y, then it is also greater than the square of y. True in $\mathcal{R}$ and $\mathcal{N}$. Given x, take $y = x$, which makes the antecedent false and hence the implication true.

(5l) For every number x, there is a number y such that, if it is different from x, then its square is less than x. True in $\mathcal{R}$ and $\mathcal{N}$. Given x, take $y = x$, which makes the antecedent false and hence the implication true.

(5m) There is number greater than all numbers. False in $\mathcal{R}$ and $\mathcal{N}$.

(5n) There is a number x such that adding any number to it again yields x. False in $\mathcal{R}$ and $\mathcal{N}$.

(5o) There is a number x that can be added to any number y to obtain y again. True in $\mathcal{R}$ and $\mathcal{N}$, take $x = 0$.

(5p) There is a number such that every number is either less than it or less than its additive inverse. False in $\mathcal{R}$. It is not a formula in the language $\mathcal{L}_{\mathcal{N}}$.

(5q) There is a number x that is greater than or not greater than any given number y. True in $\mathcal{R}$ and $\mathcal{N}$.

(5r) There is a number such that the square of every number greater than it is also greater than it. True in $\mathcal{R}$ and $\mathcal{N}$, take, for example, $x = 0$.

(5s) There is a number such that the square of every number less than it is also less than it. False in $\mathcal{R}$, while it is true in $\mathcal{N}$, take $x = 0$.

(5t) There exist two numbers whose sum is equal to their product. True in $\mathcal{R}$ and $\mathcal{N}$, take $x = y = 0$.

(5u) Between any two distinct numbers, there is another number. True in $\mathcal{R}$, while it is false in $\mathcal{N}$.

1.3. Mathematical induction

(1) For $n = 0$, $0^2 + 0 = 0$, which is clearly even. Our inductive hypothesis is that $k^2 + k$ is even. Now, for $n = k + 1$,

$$(k+1)^2 + k + 1 = k^2 + 2k + 1 + k + 1 = k^2 + k + 2(k+1).$$

However, we know that $k^2 + k$ is even from the inductive hypothesis and, furthermore, $2(k + 1)$ is also clearly even. Therefore, since the sum of two even numbers is even, $k^2 + k$ is even.

(2) For $n = 4$, $2^4 = 16$ and $4! = 24$, so, clearly, $2^4 < 4!$. Our inductive hypothesis is that $2^k < k!$ for some $k \geq 4$. Now, for $n = k + 1$,

$$2^{k+1} = 2 \cdot 2^k < 2 \cdot k! < 5 \cdot k! \leq (k+1) \cdot k! = (k+1)!$$

(3) First, the set $\{1\}$ has two subsets, namely $\{1\}$ and $\varnothing$, so, clearly, the power set of $\{1\}$ has 2^1 elements. Our inductive hypothesis is that the power set of $\{1, 2, 3, \ldots, k\}$ has 2^k elements for some $k \geq 1$. Now, let $A = \{1, 2, \ldots, k, k+1\}$. Choose an element $a \in A$ and set $A' = A - \{a\}$. Note that $\mathcal{P}(A) = \{X \subseteq A \mid a \notin X\} \cup \{X \subseteq A \mid a \in X\}$. It is clear that these sets are disjoint, so to find the number of elements in $\mathcal{P}(A)$, we need only find the number of the elements in each of these sets and add them together. First, clearly, $\mathcal{P}(A') = \{X \subseteq A \mid a \notin X\}$, and so, since A' has k elements, $\{X \subseteq A \mid a \notin X\}$ has 2^k elements by the inductive hypothesis. Next, note that $X = Y \cup \{a\}$ for all $X \in \{X \subseteq A \mid a \in X\}$, where $Y \in \mathcal{P}(A')$. Since there are k elements in the set A', there are 2^k such Y by the inductive hypothesis. Hence, the set $\{X \subseteq A \mid a \in X\}$ has 2^k elements. Thus, in total, $\mathcal{P}(A)$ has $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ elements.

2

Sets, Relations, Orders

2.1. Set inclusions and equalities

To keep the solutions as clear and concise as possible, we will make use of the logical notation introduced in Section 1.2. We will also be making use of the logical constant $\top$, which always takes the truth value "true", and the logical constant $\bot$, which always takes the truth value "false".

(1a) $x \in A \cap A$
$\iff x \in A \wedge x \in A$
$\iff x \in A$

(1b) $x \in A \cap B$
$\iff x \in A \wedge x \in B$
$\iff x \in B \wedge x \in A$
$\iff x \in B \cap A$

(1c) $x \in A \cap (B \cap C)$
$\iff x \in A \wedge x \in B \cap C$
$\iff x \in A \wedge (x \in B \wedge x \in C)$
$\iff (x \in A \wedge x \in B) \wedge x \in C$
$\iff x \in A \cap B \wedge x \in C$
$\iff x \in (A \cap B) \cap C$

(1d) Let $x \in A \cap B$. Then $x \in A$ and $x \in B$, which means that $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

(1e) Assume $A \subseteq B$. First, the left-to-right inclusion follows from 1(d). For the other inclusion, let $x \in A$. However, since $A \subseteq B$, $x \in B$. Hence, $x \in A \cap B$. For the converse direction, assume $A \nsubseteq B$. Then there is some x such that $x \in A$ but $x \notin B$. Hence, $x \in A$ but $x \notin A \cap B$, which means that $A \neq A \cap B$.

(1f) $x \in A \cup A$
$\iff x \in A \vee x \in A$
$\iff x \in A$

(1g) $x \in A \cup B$
$\iff x \in A \vee x \in B$
$\iff x \in B \vee x \in A$
$\iff x \in B \cup A$

(1h) $x \in A \cup (B \cup C)$
$\iff x \in A \vee x \in B \cup C$
$\iff x \in A \vee (x \in B \vee x \in C)$
$\iff (x \in A \vee x \in B) \vee x \in C$
$\iff x \in A \cup B \vee x \in C$
$\iff x \in (A \cup B) \cup C$

Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

(1i) For the sake of a contradiction, assume $A \nsubseteq A \cup B$ or $B \nsubseteq A \cup B$. If $A \nsubseteq A \cup B$, then there is some x such that $x \in A$ but $x \notin A \cup B$; $x \notin A \cup B$ implies that $x \notin A$ and $x \notin B$, which contradicts the fact that $x \in A$. On the other hand, if $B \nsubseteq A \cup B$, then there is some x such that $x \in B$ but $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$, which again is a contradiction.

(1j) Assume $A \subseteq B$ and let $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in B$, we are done. On the other hand, if $x \in A$, then $x \in B$ since $A \subseteq B$. Hence, $A \cup B \subseteq B$. For the other inclusion, let $x \in B$; then, clearly, $x \in A \cup B$. For the converse, assume $A \cup B = B$ and let $x \in A$. We have to show that $x \in B$. However, $x \in A$ implies that $x \in A \cup B$. Hence, since $A \cup B = B$, $x \in B$.

(1k) Assume $A \subseteq X$ and $B \subseteq X$, and let $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in A$, then $x \in X$ since $A \subseteq X$ and, similiarly, if $x \in B$, then $x \in X$ since $B \subseteq X$. Hence, in both cases, $x \in X$, which means that $A \cup B \subseteq X$.

(2a) For the sake of a contradiction, assume $\varnothing - A \neq \varnothing$. Then $\varnothing - A \nsubseteq \varnothing$ or $\varnothing \nsubseteq \varnothing - A$. However, since $\varnothing$ is a subset of any set, $\varnothing - A \nsubseteq \varnothing$. This means that there is some x such that $x \in \varnothing - A$ but $x \notin \varnothing$. Hence, $x \in \varnothing$ and $x \notin A$. This is a contradiction since $\varnothing$ has no elements.

(2b) For the right-to-left inclusion, let $x \in A$. However, $\varnothing$ has no elements, so $x \notin \varnothing$. Hence, $x \in A - \varnothing$. For the left-to-right inclusion, suppose $A - \varnothing \nsubseteq A$. Then there is some x such that $x \in A - \varnothing$ but $x \notin A$; $x \in A - \varnothing$ implies that $x \in A$ and $x \notin \varnothing$, which contradicts the fact that $x \notin A$.

(2c) For the sake of a contradiction, assume $A - B \nsubseteq A$. Then there is some x such that $x \in A - B$ and $x \notin A$. However, $x \in A - B$ implies that $x \in A$ and $x \notin B$, which contradicts the fact that $x \notin A$.

(2d) For the left-to-right direction, assume $A \nsubseteq B$. Then there is some x such that $x \in A$ but $x \notin B$. However, this means that $x \in A - B$. Hence, $A - B \neq \varnothing$. For the converse, assume $A - B \neq \varnothing$. Then there is some x in $A - B$. Hence, $x \in A$ but $x \notin B$, which means that $A \nsubseteq B$.

(2e) For the sake of a contradiction, assume $(A - B) \cap (B - A) \neq \varnothing$. Then there is some x such that $x \in (A - B) \cap (B - A)$. Hence, $x \in A - B$ and $x \in B - A$. This means that $x \in A$ while $x \notin B$ and $x \in B$ while $x \notin A$, which is a contradiction.

(2f)
$$\begin{aligned}
& x \in (A - B) \cup B \\
\iff & x \in A - B \vee x \in B \\
\iff & (x \in A \wedge \neg x \in B) \vee x \in B) \\
\iff & (x \in A \vee x \in B) \wedge (\neg x \in B \vee x \in B) \\
\iff & (x \in A \vee x \in B) \wedge \top \\
\iff & x \in A \vee x \in B \\
\iff & x \in A \cup B
\end{aligned}$$

(2g)
$$\begin{aligned}
& x \in A - (A \cap B) \\
\iff & x \in A \wedge \neg x \in A \cap B \\
\iff & x \in A \wedge \neg(x \in A \wedge x \in B) \\
\iff & x \in A \wedge (\neg x \in A \vee \neg x \in B) \\
\iff & (x \in A \wedge \neg x \in A) \vee (x \in A \wedge \neg x \in B) \\
\iff & \bot \vee x \in A - B \\
\iff & x \in A - B
\end{aligned}$$

(2h)
$$\begin{aligned}
& x \in A - (B \cap C) \\
\iff & x \in A \wedge \neg x \in B \cap C \\
\iff & x \in A \wedge \neg(x \in B \wedge x \in C) \\
\iff & x \in A \wedge (\neg x \in B \vee \neg x \in C) \\
\iff & (x \in A \wedge \neg x \in B) \vee (x \in A \wedge \neg x \in C) \\
\iff & x \in A - B \vee x \in A - C \\
\iff & x \in (A - B) \cup (A - C)
\end{aligned}$$

(2i) $x \in (A - B) \cup (B - A) \cup (A \cap B)$
$\iff x \in A - B \vee x \in B - A \vee x \in A \cap B$
$\iff (x \in A \wedge \neg x \in B) \vee (x \in B \wedge \neg x \in A) \vee (x \in A \wedge x \in B)$
$\iff ((x \in A \wedge \neg x \in B) \vee (x \in A \wedge x \in B)) \vee (x \in B \wedge \neg x \in A)$
$\iff (x \in A \wedge (\neg x \in B \vee x \in B)) \vee (x \in B \wedge \neg x \in A)$
$\iff (x \in A \wedge \top) \vee (x \in B \wedge \neg x \in A)$
$\iff x \in A \vee (x \in B \wedge \neg x \in A)$
$\iff (x \in A \vee x \in B) \wedge (x \in A \vee \neg x \in A)$
$\iff (x \in A \vee x \in B) \wedge \top$
$\iff (x \in A \vee x \in B)$
$\iff x \in A \cup B$

(2j) $x \in A \cup (B \cap C)$
$\iff x \in A \vee x \in B \cap C$
$\iff x \in A \vee (x \in B \wedge x \in C)$
$\iff (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
$\iff x \in A \cup B \wedge x \in A \cup C$
$\iff x \in (A \cup B) \cap (A \cup C)$

(2k) $A \subseteq A \cup B$, so, by 1(d), $A \cap (A \cup B) = A$.

(2l) $A \cap B \subseteq A$, so, by 1(i), $A \cup (A \cap B) = A$.

(3a) Assume $A \subseteq B$ and let $X \in \mathcal{P}(A)$. Then $X \subseteq A$. However, $A \subseteq B$, so $X \subseteq B$, which means that $X \in \mathcal{P}(B)$.

(3b) Assume $A \in \mathcal{P}(X)$ and $B \in \mathcal{P}(X)$. Then $A \subseteq X$ and $B \subseteq X$. To show that $A \cap B \in \mathcal{P}(X)$, we have to show that $A \cap B \subseteq X$. To see this, let $x \in A \cap B$. Then $x \in A$ and $x \in B$. However, $A \subseteq X$ and $B \subseteq X$, so $x \in X$, which proves that $A \cap B \subseteq X$. The fact that $A \cup B \in \mathcal{P}(X)$ follows from 1(k). To show that $A - B \in \mathcal{P}(X)$, let $x \in A - B$. Then $x \in A$ and $x \notin B$. However, since $A \subseteq X$, $x \in X$, and so $A - B \subseteq X$, which proves that $A - B \in \mathcal{P}(X)$. Finally, by 2(c), $X - A \subseteq X$, so $X - A \in \mathcal{P}(X)$.

(4a) $(x, y) \in (B \cup C) \times A$
$\iff x \in B \cup C \wedge y \in A$
$\iff (x \in B \vee x \in C) \wedge y \in A$
$\iff (x \in B \wedge y \in A) \vee (x \in C \wedge y \in A)$
$\iff (x, y) \in B \times A \vee (x, y) \in C \times A$
$\iff (x, y) \in (B \times A) \cup (C \times A)$

(4b) $(x, y) \in A \times (B \cap C)$
$\iff x \in A \wedge y \in B \cap C$
$\iff x \in A \wedge (y \in B \wedge y \in C)$
$\iff (x \in A \wedge x \in A) \wedge (y \in B \wedge y \in C)$
$\iff x \in A \wedge (x \in A \wedge y \in B) \wedge y \in C$
$\iff (x \in A \wedge y \in B) \wedge (x \in A \wedge y \in C)$
$\iff (x, y) \in (A \times B) \wedge (x, y) \in (A \times C)$
$\iff (x, y) \in (A \times B) \cap (A \times C)$

(4c) $(x, y) \in (B \cap C) \times A$
$\iff x \in B \cap C \wedge y \in A$
$\iff (x \in B \wedge x \in C) \wedge y \in A$
$\iff (x \in B \wedge x \in C) \wedge (y \in A \wedge y \in A)$
$\iff x \in B \wedge (x \in C \wedge y \in A) \wedge y \in A$
$\iff (x \in B \wedge y \in A) \wedge (x \in C \wedge y \in A)$
$\iff (x, y) \in B \times A \wedge (x, y) \in C \times A$
$\iff (x, y) \in (B \times A) \cap (C \times A)$

(4d) $(x, y) \in (A \times B) - (A \times C)$
$\iff (x, y) \in (A \times B) \wedge \neg(x, y) \in A \times C$
$\iff (x \in A \wedge y \in B) \wedge \neg(x \in A \wedge y \in C)$
$\iff (x \in A \wedge y \in B) \wedge (\neg x \in A \vee \neg y \in C)$
$\iff (x \in A \wedge y \in B \wedge \neg x \in A) \vee (x \in A \wedge y \in B \wedge \neg y \in C)$
$\iff \bot \vee (x \in A \wedge y \in B \wedge \neg y \in C)$
$\iff x \in A \wedge y \in B \wedge \neg y \in C$
$\iff x \in A \wedge y \in (B - C)$
$\iff (x, y) \in A \times (B - C)$

2.2. Functions

(1a) gf is the function from $\mathbb{Z}$ to $\mathbb{R}$ given by $x \mapsto x^3/27$, and, furthermore, $\mathrm{dom}(gf) = \mathbb{Z}$ $\mathrm{rng}(gf) = \left\{ \frac{m^3}{27} \mid m \in \mathbb{Z} \right\}$

(1b) gh is the function from $\mathbb{R}^2$ to $\mathbb{R}$ given by $(x, y) \mapsto (x \times y)^2$, and, furthermore, $\mathrm{dom}(gh) = \mathbb{R}^2$ $\mathrm{rng}(gh)$ is the set of non-negative real numbers.

(1c) No, fg is not defined.

(1d) No, h is binary, not unary.

(1e) No, g has range $\mathbb{R}$, while f has domain $\mathbb{Z}$.

(2a) $f_1(x) = x^2$

(2b) $f_2(x) = x^3 - x$

(2c) $f_3(x) = 2^x$

(2d) $f_4(x) = x + 2$

(3) Let $f\colon \mathbb{R}^+ \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$, where $f(x) = \sqrt{x}$ and $g(x) = x^2$.

(4) Let $f\colon \mathbb{R}^+ \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}^+$, where $f(x) = \sqrt{x}$ and $g(x) = x^2$.

(5a) $\mathrm{cod}(h) = \mathbb{R}$

(5b) $\mathrm{rng}(f) = \mathbb{R}$
$\mathrm{rng}(g) = \mathbb{R}^+$
$\mathrm{rng}(h) = \mathbb{R}$

(5c) f and g are injective.

(5d) f and h are surjective.

(5e) f is the only bijective function.

(6a) The fixed points of sq are 0 and 1.

(6b) $f(x) = x + 1$

(6c) abs has infinitely many fixed points.

(7) Let $f\colon A \to B$ and assume f is bijective. Then f has an inverse f^{-1} which is also bijective by Proposition 4.2.11. Hence, f^{-1} has an inverse $(f^{-1})^{-1}$. Now, let $a \in A$. Then $(f^{-1})^{-1}(a) = (f^{-1})^{-1}(f^{-1}(f(a))) = f(a)$, where the second and last steps follow from Definition 4.2.10.

(8a) Let $f\colon A \to B$ and $g\colon B \to C$ be surjective mappings and let $c \in C$. To show that gf is surjective, we have to find some $a \in A$ such that $gf(a) = c$. However, since g is surjective, there is some $b \in B$ such that $g(b) = c$. Similarly, since f is surjective, there is some $a \in A$ such that $f(a) = b$. Hence, $g(f(a)) = c$, as desired.

(8b) Let $f\colon A \to B$ and $g\colon B \to C$, and assume that gf is injective. Now, suppose $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$. Hence, by definition, $gf(a_1) = gf(a_2)$. However, gf is injective, so $a_1 = a_2$, and we are done.

(9) Let $h\colon A \to B$, $g\colon B \to C$ and $f\colon C \to D$. Then $f(gh)(a) = f(gh(a)) = f(g(h(a))) = fg(h(a)) = (fg)h(a)$.

(10) Let $f\colon A \to B$. To prove the left-to-right direction, assume f is surjective, and consider the mappings $g_1\colon B \to C$ and $g_2\colon B \to C$. Furthermore, suppose $g_1 f = g_2 f$. We have to show that $g_1 = g_2$. Now, let $b \in B$. Since f is surjective, there is some $a \in A$ such that $f(a) = b$. Hence,

$$g_1(b) = g_1(f(a)) = g_1 f(a) = g_2 f(a) = g_2(f(a)) = g_2(b).$$

For the converse, suppose f is not surjective. Then there is some $b \in B$ such that, for all $a \in A$, $f(a) \neq b$. We have to find two mappings g_1 and g_2 such that $g_1 f = g_2 f$ but $g_1 \neq g_2$. Let $g_1\colon B \to B$ and $g_2\colon B \to B$

such that $g_1(b') = b'$ for all $b' \in B$, and $g_2(b') = b'$ for all $b' \in B - \{b\}$ but $g_2(b) = f(a_0)$ for an arbitrary fixed element $a_0 \in A$. Then

$$g_1 f(a) = g_1(f(a)) = f(a) = g_2(f(a)) = g_2 f(a),$$

while $g_1(b) = b \neq f(a_0) = g_2(b)$, and we are done.

2.3. Binary relations and operations on them

(1) dom(ParentOf) is the set of all humans who have children, while rng(ParentOf) is the set of all humans.
dom(IsMArriedTo) and rng(IsMarriedTo) are the set of all married humans.
dom(OwnsDog) is the set of all humans owning a dog, while rng(OwnsDog) is the set of all dogs owned by some human.
dom(IsCitizenOf) is the set of all humans who are citizens of some country, while rng(IsCitizenOf) are the set all countries.
dom(IsMemberOf) is the set of all humans who are member of some club, while rng(IsMemberOf) is the set of all clubs that have at least one member.

(2a) $\{4, 6, 8, 10, \ldots\} \cup \{10, 15, 20, 25, \ldots\}$

(2b) $\{2, 3, 4, 5, 6\}$

(2c) $\{x \in \mathbb{Z} \mid x \geq 13\}$

(2d) $\{x \in \mathbb{Z} \mid x \leq 302\}$

(3a) The set of all Dachshunds owned by citizens of European countries.

(3b) The set of all Scotish Terriers owned by the children of members of the Rotary Club.

(3c) The set of all Scotish Terriers owned by parents of members of the Rotary Club.

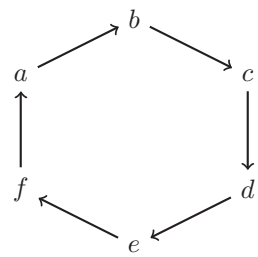
(3d) The set of all those humans who have a parent who is a citizen of a European country and a parent who is a citizen of an African country.

(3e) The set of parents whose children are citizens of both African and European countries.

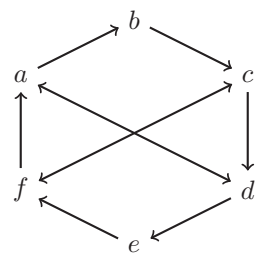
(3f) The set of all sons of members of the Rotary Club.

(3g) The set of all mothers of members of the Rotary Club.

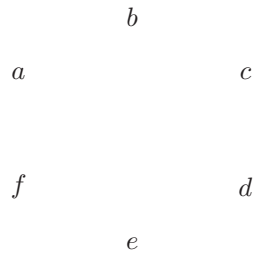
(4a) $R_1 \cap R_2$:



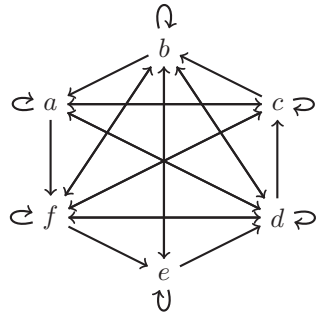
(4b) $R_1 \cup R_2$:



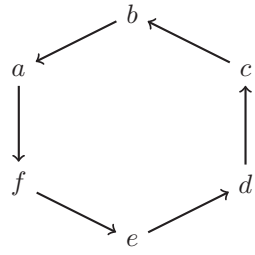
(4c) $R_1 - R_2$:



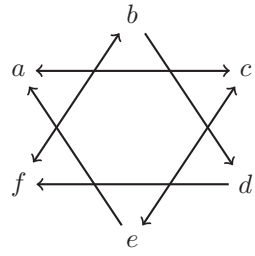
(4d) R_1':



(4e) R_1^{-1}:



(4f) $R_1 \circ R_2$:



(5a) The graphical representation of $R_1 \cap R_2$ contains the overlapping arrows if we were to put the graphical representations of R_1 and R_2 on top of each other.

(5b) The graphical representation of $R_1 \cup R_2$ contains the arrows of both graphical representations of R_1 and R_2.

(5c) The graphical representation of $R_1 - R_2$ contains the arrows of the graphical representation of R_1 but without those occurring in the graphical representation of R_2.

(5d) The graphical representation of R_1' contains all possible arrows between nodes but without those occurring in the graphical representation of R_1.

(5e) The graphical representation of R_1^{-1} is the same as the graphical representation of R_1 but with the arrows in the opposite direction.

(5f) If there is an arrow from x to y in R_1 and an arrow from y to z in R_2, there is an arrow from x to z in $R_1 \circ R_2$.

(6a)
$$\begin{array}{c} \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \end{array} \begin{array}{c} \begin{array}{ccccc} \alpha & \beta & \gamma & \delta & \epsilon \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

(6b)
$$\begin{array}{c} \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \end{array} \begin{array}{c} \begin{array}{ccccc} \alpha & \beta & \gamma & \delta & \epsilon \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

(6c)
$$\begin{array}{c} \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \end{array} \begin{array}{c} \begin{array}{ccccc} \alpha & \beta & \gamma & \delta & \epsilon \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

(6d)
$$\begin{array}{c} \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \end{array} \begin{array}{c} \begin{array}{ccccc} \alpha & \beta & \gamma & \delta & \epsilon \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

(6e)
$$\begin{array}{c} \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \end{array} \begin{array}{c} \begin{array}{ccccc} \alpha & \beta & \gamma & \delta & \epsilon \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

(6f)
$$\begin{array}{c} \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \end{array} \begin{array}{c} \begin{array}{ccccc} \alpha & \beta & \gamma & \delta & \epsilon \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

(7a) Place 1's everywhere where there are 1's in the matrix representations of both S_1 and S_2 and 0's everywhere else.

(7b) Place 1's everywhere where there is a 1 in at least one of the matrix representations of S_1 and S_2 and 0's everywhere else.

(7c) Change all the 1's in the matrix representation of S_1 to 0's if the matrix representation of S_2 also contains a 1 in the corresponding row and column, and leave the remaining entries the same as in the matrix representation of S_1.

(7d) In the matrix representation of S_1, change the 0's to 1's and the 1's to 0's.

(7e) Reflect the representation matrix of S_1 about its diagonal.

(7f) If there is a 1 in row i column j of the representation matrix of S_1 and a 1 in row j column k of the representation matrix of S_2, place a 1 in row i column k of the representation matrix of $S_1 \circ S_2$, and 0's everywhere else.

(8a) $y \in \mathrm{rng}(R \cup S)$
$\iff \exists x \in A((x, y) \in R \cup S)$
$\iff \exists x \in A((x, y) \in R \vee (x, y) \in S)$
$\iff \exists x \in A((x, y) \in R) \vee \exists x \in A((x, y) \in S)$
$\iff y \in \mathrm{rng}(R) \vee y \in \mathrm{rng}(S)$
$\iff y \in \mathrm{rng}(R) \cup \mathrm{rng}(S)$

(8b) $x \in \mathrm{dom}(R \cap S)$
$\Rightarrow \exists y \in B((x,y) \in R \cap S)$
$\Rightarrow \exists y \in B((x,y) \in R \wedge (x,y) \in S)$
$\Rightarrow \exists y \in B((x,y) \in R) \wedge \exists y \in B((x,y) \in S)$
$\Rightarrow x \in \mathrm{dom}(R) \wedge x \in \mathrm{dom}(S)$
$\Rightarrow x \in \mathrm{dom}(R) \cap \mathrm{dom}(S)$

(8c) $y \in \mathrm{rng}(R \cap S)$
$\Rightarrow \exists x \in A((x,y) \in R \cap S)$
$\Rightarrow \exists x \in A((x,y) \in R \wedge (x,y) \in S)$
$\Rightarrow \exists x \in A((x,y) \in R) \wedge \exists x \in A((x,y) \in S)$
$\Rightarrow y \in \mathrm{rng}(R) \wedge y \in \mathrm{rng}(S)$
$\Rightarrow y \in \mathrm{rng}(R) \cap \mathrm{rng}(S)$

(9a) Consider the set $X = \{a, b\}$ with $R = \{(a,b), (a,a), (b,b)\}$ and $S = \{(b,a)\}$ on X.

(9b) Consider the set $X = \{a, b\}$ with $R = \{(a,b), (a,a), (b,b)\}$ and $S = \{(b,a)\}$ on X.

(9c) Consider the set $X = \{a, b\}$ with $R = \{(a,b), (b,a)\}$ and $S = \{(a,b)\}$ on X.

(9d) Consider the set $X = \{a, b\}$ with $R = \{(a,b), (b,a)\}$ and $S = \{(a,b)\}$ on X.

(10a) $x \in \mathrm{rng}(R^{-1})$
$\iff \exists y \in B((y,x) \in R^{-1})$
$\iff \exists y \in B((x,y) \in R)$
$\iff x \in \mathrm{dom}(R)$

(10b) $(x,y) \in (R^{-1})^{-1}$
$\iff (y,x) \in R^{-1}$
$\iff (x,y) \in R$

(10c) $(x,y) \in (R \cap S)^{-1}$
$\iff (y,x) \in R \cap S$
$\iff (y,x) \in R \wedge (y,x) \in S$
$\iff (x,y) \in R^{-1} \wedge (x,y) \in S^{-1}$
$\iff (x,y) \in R^{-1} \cap S^{-1}$

(10d) $(x,y) \in (R')^{-1}$
$\iff (y,x) \in R'$
$\iff (y,x) \notin R$
$\iff (x,y) \notin R^{-1}$
$\iff (x,y) \in (R^{-1})'$

(11) $(x,y) \in (R \circ S)^{-1}$
$\iff (y,x) \in R \circ S$
$\iff \exists z((y,z) \in R \wedge (z,x) \in S)$
$\iff \exists z((z,y) \in R^{-1} \wedge (x,z) \in S^{-1})$
$\iff (x,y) \in S^{-1} \circ R^{-1}$

2.4. Special binary relations

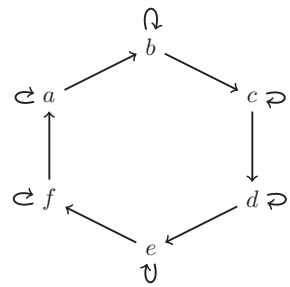
(2a) The relation $\sim_3$ on $\mathbb{Z}$, defined by $x \sim_3 y$ iff x and y leave the same remainder after division by 3.

(2b) The inclusion relation $\subseteq$ on a collections of sets.

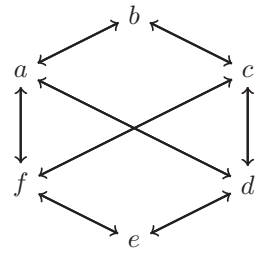
(2c) The inclusion relation $\subseteq$ on a collection of sets.

(2d) The relation given in Exercise 2(a).

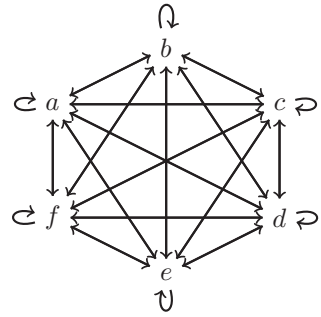
(3a) R_1^{ref}:



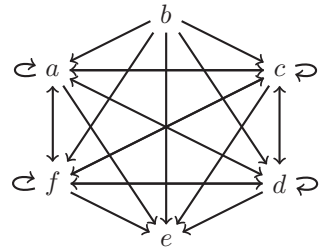
(3b) R_2^{sym}:



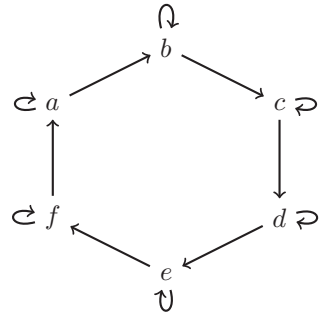
(3c) R_1^{tran}:



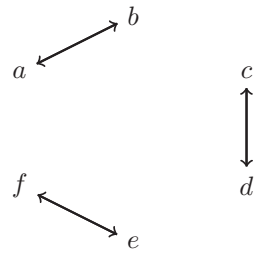
(3d) R_2^{tran}:



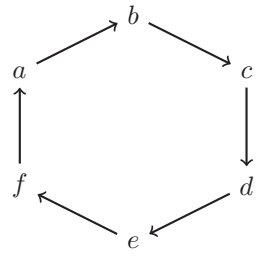
(4a) A relation which is serial but not functional:



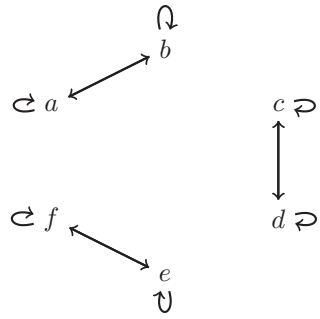
(4b) An irreflexive, functional and symmetric relation:



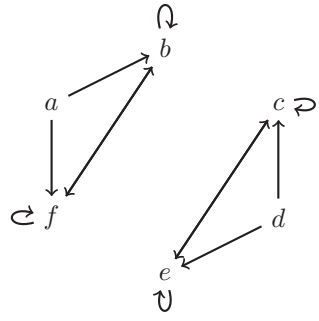
(4c) An irreflexive, serial and asymmetric relation:



(4d) An equivalence relation which is not connected:



(4e) An Euclidean relation which is serial but not functional:



(5a) Assume $(x, y) \in T$ and $(y, z) \in T$. Then there are $u, v \in X$ such that $(x, u), (v, z) \in R$ and $(u, y), (y, v) \in S$. However, then $(u, v) \in S$ by the transitivity of S. This means that $(u, z) \in S \circ R$, and so $(u, z) \in R \circ S$. Hence, there is some $w \in X$ such that $(u, w) \in R$ and $(w, z) \in S$. Now, since $(x, u) \in R$, $(x, w) \in R$ by the transitivity of R, and therefore $(x, z) \in R \circ S = T$.

(5c) Suppose it is S that is reflexive. Since S is reflexive, we have $E_X \subseteq S$. To show that $R \subseteq E_X$, let $(x, y) \in R$. However, $(y, y) \in S$, so $(x, y) \in R \circ S = E_X$. Thus, $(x, y) \in E_X$. For $E_X \subseteq R$, suppose $(x, x) \in E_X$. Since $E_X = R \circ S$, there is a $u \in X$ such that $(x, u) \in R$ and $(u, x) \in S$. However, since $R \subseteq E_X$, we have $(x, u) \in E_X$, i.e. $u = x$, so $(x, x) \in R$. To show that $S \subseteq E_X$, let $(x, y) \in S$. Since $E_X \subseteq R$, we have $(x, x) \in R$, and hence $(x, y) \in R \circ S = E_X$, so $(x, y) \in E_X$. Thus, we have proven that $R = E_X = S$, as desired. The case when it is R that is reflexive is similar.

(6a) $\mathrm{div}^{\mathrm{ref}}$ relates every member of $\mathbb{N}^+ - \{1\}$ to all its multiples and 1 to itself.

(6b) $\mathrm{div}^{\mathrm{sym}}$ relates every member of $\mathbb{N}^+ - \{1\}$ to all its proper multiples and all its proper divisors in $\mathbb{N}^+ - \{1\}$.

(6c) $\mathrm{div}^{\mathrm{tran}} = \mathrm{div}$

(6d) $<^{\mathrm{ref}} = \leq$

(6e) $\leq^{\mathrm{sym}}$ relates every member to every other member including to itself.

(6f) $\leq^{\mathrm{tran}} = \leq$

(7a) For the left-to-right direction, assume $E_X \nsubseteq R$. Then there is some $x \in X$ such that $(x, x) \in E_X$ but $(x, x) \notin R$. However, this means that R is not reflexive. For the converse, assume R is not reflexive. Then there is some $x \in X$ such that $(x, x) \notin R$, but $(x, x) \in E_X$, which means that $E_X \nsubseteq R$.

(7b) Assume R is symmetric and let $(x, y) \in R^{-1}$. Then $(y, x) \in R$ and so, since R is symmetric, $(x, y) \in R$, as required. For the converse, assume $R^{-1} \subseteq R$ and $(x, y) \in R$. We have to show that $(y, x) \in R$. However, $(x, y) \in R$ implies that $(y, x) \in R^{-1}$, and since $R^{-1} \subseteq R$, $(y, x) \in R$. For the second iff, the right-to-left direction is obvious. For the other direction, assume $R^{-1} \subseteq R$. To show that $R^{-1} = R$, we thus only need to show that $R \subseteq R^{-1}$. Let $(x, y) \in R$. However, $R^{-1} \subseteq R$ implies that R is symmetric, so $(y, x) \in R$. Hence, $(x, y) \in R^{-1}$, and we are done.

(7c) Assume R is antisymmetric and let $(x, y) \in R^{-1} \cap R$. Then $(x, y) \in R^{-1}$ and $(x, y) \in R$. However, $(x, y) \in R^{-1}$ implies that $(y, x) \in R$, so, since R in antisymmetric, $x = y$. Hence, $(x, y) \in E_X$. Conversely, assume $R^{-1} \cap R \subseteq E_X$. Now, let $(x, y) \in R$ and $(y, x) \in R$. However, from $(y, x) \in R$ we have that $(x, y) \in R^{-1}$. Hence, $(x, y) \in R^{-1} \cap R$, and so, since $R^{-1} \cap R \subseteq E_X$, $x = y$, as required.

(7d) Assume R is transitive and let $(x, z) \in R^2$. Then there is a $y \in X$ such that $(x, y) \in R$ and $(y, z) \in R$. However, since R is transitive, $(x, z) \in R$. Conversely, assume $R^2 \subseteq R$. Let $(x, y) \in R$ and $(y, z) \in R$. Then $(x, z) \in R^2$, and so, since $R^2 \subseteq R$, $(x, z) \in R$.

(8) R is functional iff it is the graph of the function $f : \mathrm{dom} R \to B$ given by $f : a \mapsto b$, where b is the unique element of B such that $R(a, b)$.

(9a) Let $\mathcal{X} = \{S \mid R \subseteq S \subseteq X^2 \text{ and } S \text{ is symmetric}\}$. We have to show that $R^{\mathrm{sym}} = \bigcap \mathcal{X}$. First, $\mathcal{X} \neq \varnothing$ since X^2 is symmetric and $R \subseteq X^2$. Now, by the definition of $\mathcal{X}$, $R \subseteq S$ for all $S \in \mathcal{X}$, so $R \subseteq \bigcap \mathcal{X}$ by Proposition 4.1.3. To show that $\bigcap \mathcal{X}$ is symmetric, let $(x, y) \in \bigcap \mathcal{X}$. Then $(x, y) \in S$ for all $S \in \mathcal{X}$. However, all S are symmetric, so $(y, x) \in S$ for all $S \in \mathcal{X}$. Hence, $(y, x) \in \bigcap \mathcal{X}$. All we have to check now is that $\bigcap \mathcal{X}$ is the smallest such relation, so let $R' \subseteq X^2$ be symmetric and assume $R \subseteq R'$. We have to show that $\bigcap \mathcal{X} \subseteq R'$. By the definition of $\mathcal{X}$, $R' \in \mathcal{X}$, and hence $\bigcap \mathcal{X} \subseteq R'$, as required.

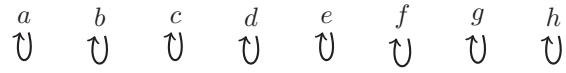
(9b) Let $\mathcal{X} = \{S \mid R \subseteq S \subseteq X^2 \text{ and } S \text{ is reflexive}\}$. We have to show that $R^{\mathrm{tran}} = \bigcap \mathcal{X}$. First, $\mathcal{X} \neq \varnothing$ since X^2 is reflexive and $R \subseteq X^2$. Now, by the definition of $\mathcal{X}$, $R \subseteq S$ for all $S \in \mathcal{X}$, so $R \subseteq \bigcap \mathcal{X}$ by Proposition 4.1.3. To show that $\bigcap \mathcal{X}$ is reflexive, let $x \in X$. Then $(x, x) \in S$ for all $S \in \mathcal{X}$, so $(x, x) \in \bigcap \mathcal{X}$. To check that $\bigcap \mathcal{X}$ is the smallest such relation, let $R' \subseteq X^2$ be reflexive and assume $R \subseteq R'$. By the definition of $\mathcal{X}$, $R' \in \mathcal{X}$ and so $\bigcap \mathcal{X} \subseteq R'$.

2.5. Equivalence relations and partitions

(1) First, it is obvious that $\equiv_3$ is reflexive and symmetric. To see that $\equiv_3$ is transitive, let $x \equiv_3 y$ and $y \equiv_3 z$. Then x and y have the same remainder after division by 3 and y and z have the same remainder after division by 3. Hence, x and z must have the same remainder after division by 3, which means that $x \equiv_3 z$.

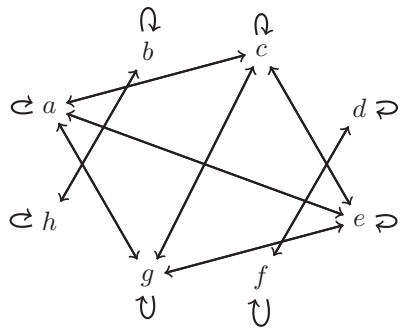
(2a) $\{\{a,c,e,g\},\{b,d\},\{h,f,c\}\}$ is not a partition of X since the subsets are not pairwise disjoint.

(2b) $\{\{a\},\{b\},\{c\},\{d\},\{e\},\{f\},\{g\},\{h\}\}$ is a partition:



(2c) $\{\{a,c,e,g\},\{d,f,h\}\}$ is not a partition of X since there is no subset that contains b.

(2d) $\{\{a,c,e,g\},\{b,h\},\{d,f\}\}$ is a partition:



(3a) First, every line in the Cartesian plane is obviously parallel to itself, so is reflexive. $\parallel$ is also clearly symmetric. Finally, assume $l_1 \parallel l_2$ and $l_2 \parallel l_3$. Then l_1 and l_2 are parallel and l_2 and l_3 are parallel, which means that l_1 and l_3 must also be parallel. Hence, $\parallel$ is transitive.

(3b) There are infinitely many elements in $L/_{\parallel}$.

(3c) The relation of being perpendicular (denoted $\perp$) is not an equivalence relation on L since it is not reflexive.

(4) In this solution we will assume that the empty string is not included in the set of finite strings of 0s and 1s. The solution requires only minor modifications if the empty string is included.

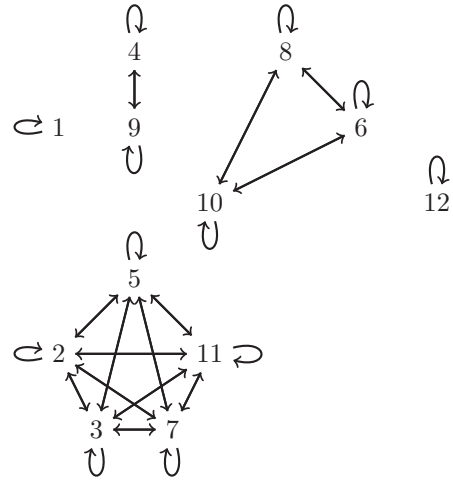
(4a) First, we show that $\sim_n$ is reflexive, so let $\overline{x} \in 2^*$. If $\overline{x}$ is shorter than n positions, then clearly $\overline{x} \sim_n \overline{x}$. On the other hand, if $\overline{x}$ has n or more positions, then $\overline{x}$ and $\overline{x}$ agree in their first n positions, so $\overline{x} \sim_n \overline{x}$. Second, $\sim_n$ is clearly symmetric. To show that $\sim_n$ is transitive, let $\overline{x} \sim_n \overline{y}$ and $\overline{y} \sim_n \overline{z}$. There are two possibilities, namely both $\overline{x}$ and $\overline{y}$ are shorter than n positions or $\overline{x}$ and $\overline{y}$ are both at least n positions long and agree in their first n positions. In the first case, $\overline{z}$ must also be shorter than n positions, for otherwise $\overline{y} \nsim_n \overline{z}$, which means $\overline{x} \sim_n \overline{z}$. In the second case, $\overline{z}$ must also have n or more positions and its first n positions agree with those of $\overline{y}$, for, if not, $\overline{y} \nsim_n \overline{z}$, and so both $\overline{x}$ and $\overline{z}$ have at least n positions and they agree in their first n positions, which means that $\overline{x} \sim_n \overline{z}$.

(4b) $[1]_{\sim_1}$ contains all strings starting with a 1.

(4c) 6

(4d) $[1]_{\sim_1}$ has infinitely many elements while $[1]_{\sim_n}$ has $\sum_{i=1}^{n-1} 2^i$ elements if $n \geq 2$.

(5) $\sim_p$:



(6) Let $(x, x) \in =$. However, we know that R is reflexive, so $(x, x) \in R$. Hence, $= \subseteq R$. Now, let R' be an equivalence relation on $\mathbb{Z}$ such that $R' \subseteq =$. However, we know that $= \subseteq R'$ from the result we have just proven. Hence $=$ is the equivalence relation R'.

(7a) Yes. First, since both R_1 and R_2 are reflexive, $(x, x) \in R_1$ and $(x, x) \in R_2$, for all $x \in X$. Hence $(x, x) \in R_1 \cap R_2$ for all $x \in X$ and so $R_1 \cap R_2$ is also reflexive. To see that $R_1 \cap R_2$ is symmetric, let $(x, y) \in R_1 \cap R_2$. Then $(x, y) \in R_1$ and $(x, y) \in R_2$. However, both R_1 and R_2 are symmetric, so $(y, x) \in R_1$ and $(y, x) \in R_2$. This means that $(y, x) \in R_1 \cap R_2$. Finally, to show that $R_1 \cap R_2$ is transitive, assume $(x, y) \in R_1 \cap R_2$ and $(y, z) \in R_1 \cap R_2$. Then both (x, y) and (y, z) belong to R_1 and both (x, y) and (y, z) belong to R_2. Hence, since both R_1 and R_2 are transitive, $(x, z) \in R_1$ and $(x, z) \in R_2$, and so $(x, z) \in R_1 \cap R_2$.

(7b) No. Consider the set $X = \{a, b, c\}$ with binary relations

$$R_1 = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

and

$$R_2 = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$$

on X. Then

$$R_1 \cup R_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}.$$

Clearly R_1 and R_2 are equivalence relations, while, since $R_1 \cup R_2$ is not transitive, it is not an equivalence relation.

(7c) No. Consider the set $X = \{a, b, c\}$ with binary the relation

$$R_1 = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

on X. Then

$$R_1' = \{(b, c), (c, b), (a, c), (c, a)\}.$$

Clearly, R_1 is an equivalence relation, while, since R_1' is not reflexive, it is not an equivalence relation.

(8a) Assume R is an equivalence relation on X. Then $(x, x) \in R$ since R is reflexive, and so $x \in [x]_R$.

(8b) Assume R is an equivalence relation on X and $x \in [y]_R$. Then $(y, x) \in R$, and so, since R is symmetric, $(x, y) \in R$. Now, suppose $z \in [y]_R$. Then $(y, z) \in R$, and so, by transitivity, $(x, z) \in R$; hence $z \in [x]_R$. Since z was arbitrary we conclude that $[y]_R \subseteq [x]_R$. Next, suppose that $z \in [x]_R$. Then $(x, z) \in R$, and so,

by transitivity, $(y, z) \in R$; hence $z \in [y]_R$. Since z was arbitrary we conclude that $[x]_R \subseteq [y]_R$. Therefore, $[x]_R = [y]_R$.

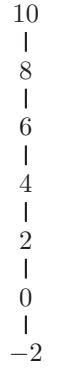
(8c) We prove the contrapositive, so assume that $[x]_R \cap [y]_R \neq \emptyset$. Then there is some $z \in X$ such that $z \in [x]_R \cap [y]_R$, and so $z \in [x]_R$ and $z \in [y]_R$. Hence, by Exercise (8b), $[x]_R = [z]_R$ and $[z]_R = [y]_R$, which means that $[x]_R = [y]_R$.

(9) For the right-to-left direction, assume R is reflexive and Euclidean. We have to show that R is reflexive, symmetric and transitive. First, R is reflexive by our assumption. To show that R is symmetric, let $(x, y) \in R$. We know that $(x, x) \in R$, so, since R is Euclidean, $(y, x) \in R$. To show that R is transitive, let $(x, y) \in R$ and $(y, z) \in R$. As R is symmetric, then $(y, x) \in R$. Hence, $(y, x) \in R$ and $(y, z) \in R$, which means that $(x, z) \in R$ since R is Euclidean. For the converse direction, assume that R is an equivalence relation. Then clearly R is reflexive. To show that R is Euclidean, let $(x, y) \in R$ and $(x, z) \in R$. We have to show that $(y, z) \in R$. Since R is symmetric, $(y, x) \in R$, and so $(y, z) \in R$ by the transitivity of R.

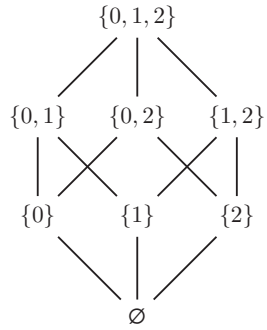
(10) Let E_1 and E_2 be equivalence relations on X. Suppose that $E_1 \circ E_2$ is an equivalent relation on X. Let $(x, y) \in E_1 \circ E_2$. However, $E_1 \circ E_2$ is symmetric, so $(y, x) \in E_1 \circ E_2$. This means there is some $z \in X$ such that $(y, z) \in E_1$ and $(z, x) \in E_2$. Hence, since E_1 and E_2 are symmetric, $(z, y) \in E_1$ and $(x, z) \in E_2$, which gives $(x, y) \in E_2 \circ E_1$. Conversely, let $(x, y) \in E_2 \circ E_1$. Then there is some $z \in X$ such that $(x, z) \in E_2$ and $(z, y) \in E_1$. As E_1 and E_2 are symmetric, so $(z, x) \in E_2$ and $(y, z) \in E_1$. We then get $(y, x) \in E_1 \circ E_2$, and so, since $E_1 \circ E_2$ is symmetric, $(x, y) \in E_1 \circ E_2$. For the right-to-left direction, assume $E_1 \circ E_2 = E_2 \circ E_1$. First, to show that $E_1 \circ E_2$ is reflexive, note that $(x, x) \in E_1$ and $(x, x) \in E_2$ since both E_1 and E_2 are reflexive. Then $(x, x) \in E_1 \circ E_2$. For the symmetry, assume $(x, y) \in E_1 \circ E_2$. Then there is a $z \in X$ such that $(x, z) \in E_1$ and $(z, y) \in E_2$. This means that $(z, x) \in E_1$ and $(y, z) \in E_2$ since both E_1 and E_2 are symmetric. Hence $(y, x) \in E_2 \circ E_1$, which gives $(y, x) \in E_1 \circ E_2$ by our assumption. Finally, for the transitivity, assume that $(x, y) \in E_1 \circ E_2$ and $(y, z) \in E_1 \circ E_2$. Now, $(y, z) \in E_1 \circ E_2$ implies $(y, z) \in E_2 \circ E_1$. We therefore have $u, v \in X$ such that $(x, u), (v, z) \in E_1$ and $(u, y), (y, v) \in E_2$. However, then $(u, v) \in E_2$ by the transitivity of E_2. This means that $(u, z) \in E_2 \circ E_1$, and so $(u, z) \in E_1 \circ E_2$. Hence, there is some $w \in X$ such that $(u, w) \in E_1$ and $(w, z) \in E_2$. Since $(x, u) \in E_1$, $(x, w) \in E_1$ by the transitivity of E_1, so $(x, z) \in E_1 \circ E_2$.

2.6. Ordered sets

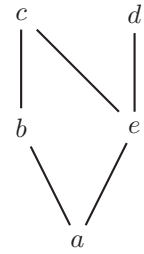
(1a) $(\{-2, 0, 2, 4, 6, 8, 10\}, \leq)$:



(1b) $(\mathcal{P}(\{0,1,2\}), \subseteq)$:



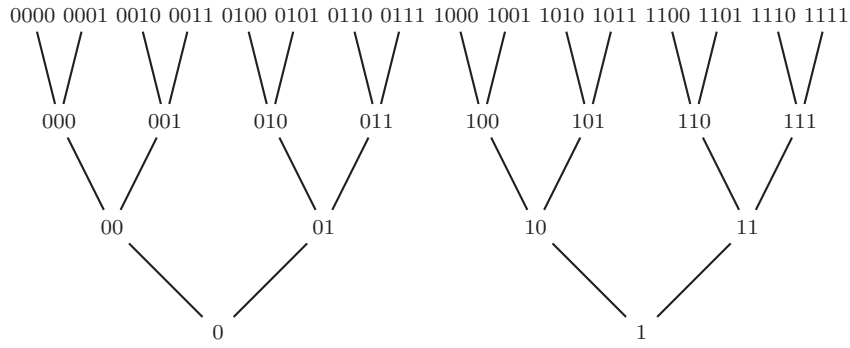
(1c) (X, R):



(2a) We have to show that the initial segment relation is reflexive, transitive and antisymmetric. First, let s be a binary string; s can obviously be obtained from itself by adding zero 0's and 1's to itself, so the initial segment relation is reflexive. To show that it is transitive, assume r is an initial segment of s and s is an initial segment of t. Then s can be obtained from r by adding zero or more 0's and/or 1's to the end of r, and, similarly, t can be obtained from s by adding zero or more 0's and/or 1's to the end of s. However, this is the same as combining these strings of 0's and/or 1's we added to r and s, respectively, and adding the combined string to r from the beginning to get t. Hence, t can be obtained from r by adding zero 0's and/or 1's to the end of r, and so r is an initial segment of t. Finally, to show that the initial segment relation is antisymmetric, assume r is an initial segment of s and s is an initial segment of r. This means that we can obtain s from r by adding zero or more 0's and/or 1's to the end of r and r can be obtained from s by adding zero or more 0's and/or 1's to the end of s. However, the only way this is possible is if s and r are the same binary strings.

(2b) This is a direct consequence of Exercise 2(a).

(2c) The set of binary string of length at most 4 together with the initial segment relation:



(3) Consider the poset $(\mathbb{R}, \leq)$, where $\leq$ is the usual ordering on the reals, and let

(3a) $Y_1 = \mathbb{Z}$

(3b) $Y_2 = \mathbb{N}$

(3c) $Y_3 = \{y \in \mathbb{R} \mid y > 0\}$.

(4a) $\mathbb{N}$

(4b) $\{x \in \mathbb{Z} \mid x \leq 0\}$

(4c) Yes, take the set $\{0\}$ for instance. All integers greater than or equal to 0 are upper bounds of this set, and there are infinitely many integers greater than 0.

(4d) No, if $S \subseteq \mathbb{Z}$ and a is an upper bound for S, then every one of the numbers $a+1, a+2, a+3, \ldots$ is also an upper bound for S.

(4e) No, if $S \subseteq \mathbb{Z}$ has a lower bound, then it has a least element, which is also its infimum.

(5a) $\mathbb{Q}^+$

(5b) $\{x \in \mathbb{Q} \mid x \leq 0\}$

(5c) Yes, the set $\{0\}$ has infinitely many upper bounds.

(5d) No, if $S \subseteq \mathbb{Q}$ and a is an upper bound for S, then every number in $\{b \in \mathbb{Q} \mid a \leq b\}$ is also an upper bound for S.

(5e) Yes. The set $\{x \in \mathbb{Q} \mid \sqrt{2} < x\}$ has lower bounds, e.g. 0 and 1. However, it has no infimum. In $(\mathbb{R}, \leq)$ the only item that changes is the last: in $(\mathbb{R}, \leq)$ *every* subset that has a lower bound also has an infimum.

(6) The infimum of $\mathcal{X}$ is $\bigcap \mathcal{X}$ while its supremum is $\bigcup \mathcal{X}$.

(7) Consider the poset $(\{2, 4\} \cup \{3^n \mid n \in \mathbb{N}\}, |^{-1})$. Here $|^{-1}$ is the inverse of the "divides" relation $|$, i.e. $a \mid^{-1} b$ iff a is a multiple of b; 4 is the unique minimal element of this poset. The poset has no least element since there is no element less that or equal to all elements in the infinitely descending chain $\cdots 3^3 \mid^{-1} 3^2 \mid^{-1} 3^1$.

(8) Consider the poset $(\mathbb{Z}^+, |^{-1})$. Here $|^{-1}$ is the inverse of the "divides" relation $|$, i.e. $a \mid^{-1} b$ iff a is a multiple of b. Then the subset $\{2, 3, 4, \ldots\}$ has infinitely many maximal elements, i.e. the prime numbers.

(10) Assume $(X, \leq)$ is a poset and let $Y \subseteq X$. Suppose x and x' are both supremums of Y in X. Then both x and x' are upper bounds of Y, and since x is a supremum, $x \leq x'$. Similarly, since x' is a supremum, $x' \leq x$. Hence, by the antisymmetry of $\leq$, $x = x'$.

(11) Assume R is a pre-order on X. First, since R is reflexive, xRx, so $x \sim x$. To show that R is symmetric, let $x \sim y$. Then xRy and yRx, and so yRx and xRy, which means that $y \sim x$. Finally, to show that $\sim$ is transitive, assume $x \sim y$ and $y \sim z$. Then xRy, yRx, yRz and zRy. However, since R is transitive, xRz and zRx, which gives $x \sim z$, as required.

(12) Let $x \in Y$. Then $x \in X$, and so, by the reflexivity of $\leq$, $x \leq x$. However, since $x \in Y$, $x \leq |_Y$. For the transitivity, let $x, y, z \in Y$, and assume $x \leq |_Y y$ and $y \leq |_Y z$. Then $x \leq y$ and $y \leq z$, and so, since $\leq$ is transitive, $x \leq z$. However, since $x, z \in Y$, $x \leq |_Y z$. Finally, assume $x \leq |_Y y$ and $y \leq |_Y x$. Then $x \leq y$ and $y \leq x$, and so, by the antisymmetry of $\leq$, $x = y$.

(13) For the right-to-left direction, we prove the contrapositive. Suppose that $(X, \leq)$ is not well-founded. Then it must contain an infinite descending chain, say $x_1 > x_2 > x_3 > \cdots$. Now, let $Y = \{x_1, x_2, x_3, \ldots\}$. Clearly, Y is a nonempty subset of X that does not have a least element. For the converse, suppose that X has a subset $Y \neq \emptyset$ such that Y has no least element. Now, take an arbitrary element of Y and call it y_1. Since y_1 cannot be a least element of Y, there must be another element, say y_2, such that $y_1 \leqq y_2$. Since $(X, \leq)$ is a linear order, $y_1 > y_2$. Again, since y_2 cannot be a least element of Y, there must be another element in Y, say y_3, such that $y_2 \leqq y_3$. Hence, since $(X, \leq)$ is a linear order, $y_1 > y_2 > y_3$. Continuing in this way, we can construct an infinite descending chain, which means that $(X, \leq)$ is not well-founded.

2.7. An introduction to cardinality

(1) We have to find a bijective map from E to $\mathbb{Z}$. Consider the map $f\colon E \to \mathbb{Z}$ defined by $f(e) = \frac{e}{2}$. To show that f is surjective, let $n \in \mathbb{Z}$. We must find a $e \in E$ such that $f(e) = n$. Well, $2n$ is clearly even, and, furthermore, $f(2n) = \frac{2n}{2} = n$, so $2n$ works. Finally, to show that f is injective, assume that $f(e) = f(e')$. Then $\frac{e}{2} = \frac{e'}{2}$, and so multiplying on both sides by 2 gives $e = e'$.

(2a) $|\{\alpha, \beta, \gamma, \delta, \epsilon\}| = 5$

(2b) $|\{x \in \mathbb{Z} \mid x^2 = 4\}| = 2$

(2c) $|\{x \in \mathbb{Q} \mid 3 \leq x \leq 4\}| = \aleph_0$

(2d) $|\{(x, y) \in \mathbb{R} \mid x^2 + y^2 = 3\}| = \mathfrak{c}$

(3) We first show that f is surjective, so let $m \in \mathbb{Z}$. We have to find an $n \in \mathbb{N}$ such that $f(n) = m$. If m is non-negative, let $n = 2m$. Then, clearly, n is even, which means $f(n) = \frac{n}{2} = \frac{2m}{2} = m$, so $2m$ works. On the other hand, if m is negative, let $n = -2m - 1$. Then n is odd, which gives $f(n) = -\frac{n+1}{2} = -\frac{(-2m-1)+1}{2} = \frac{2m+1-1}{2} = \frac{2m}{2} = m$, so in this case $-2m - 1$ works. To show that f is injective, assume $f(n) = f(m)$. Now, since no integer is both positive and negative, we have two cases, namely $\frac{n}{2} = \frac{m}{2}$ or $-\frac{n+1}{2} = -\frac{m+1}{2}$. If $\frac{n}{2} = \frac{m}{2}$, multiplying both sides by 2 gives $n = m$, as required. On the other hand, if $-\frac{n+1}{2} = -\frac{m+1}{2}$, multiplying by -2 on both sides gives $n + 1 = m + 1$, i.e. $n = m$.

(4) Consider the map $f\colon \mathcal{P}(\mathbb{N}_n) \to S_n$ defined by $f(X) = a_0 a_1 \cdots a_{n-1}$, where $a_i = 1$ if $i \in X$ and $a_i = 0$ otherwise. It is clear that f is surjective from $\mathcal{P}(\mathbb{N}_n)$ on to S_n. To show that f is injective, assume $X \neq Y$. Then there is some $i \in \mathbb{N}_n$ such that $i \in X$ but $i \notin Y$ or $i \in Y$ and $i \notin X$. In the first case, $f(X)$ has a 1 in position i while $f(Y)$ has a 0 in position i, which means that $f(X) \neq f(Y)$. Similarly, in the second case, $f(X) \neq f(Y)$.

(5) If A and B are both finite then there are bijections $f : A \to \mathbb{N}_m$ and $g : B \to \mathbb{N}_n$, for some $m, n \in \mathbb{N}$. Define $h : A \times B \to \mathbb{N}_{m \times n}$ by $h(a, b) = n \times f(a) + g(b)$. To show that h is an injection, suppose that $h(a, b) = h(a', b')$, i.e. that $n \times f(a) + g(b) = n \times f(a') + g(b')$. Then $g(b) - g(b') = n \times (f(a') - f(a))$. If $a = a'$ this reduces to $g(b) - g(b') = 0$ and hence $g(b) = g(b')$; therefore, by the injectivity of g, $b = b'$, and we are done. Suppose that $a \neq a'$. By the injectivity of f we have $f(a') \neq f(a)$. Then $g(b) - g(b') = n \times (f(a') - f(a)) \neq 0$, so $|g(b) - g(b')| = n \times k$ for some $k \in \mathbb{N}^+$. However, this is impossible, since $0 \leq g(b), g(b') \leq n - 1$. To show that h is surjective, let $k \in \mathbb{N}_{m \times n}$. Dividing k by n with a remainder, we have $k = q \times n + r$ where $0 \leq r < n$ and $0 \leq q < m$. Since $f : A \to \mathbb{N}_m$ and $g : B \to \mathbb{N}_n$ are surjective, there are elements $a \in A$ and $b \in B$ such that $f(a) = q$ and $g(b) = r$, and hence $h(a, b) = n \times f(a) + g(b) = n \times q + r = k$.

(6) Let $\mathcal{X}$ be a set of sets. We first show that $\approx$ is reflexive, so let $X \in \mathcal{X}$. We have to find a bijective map from X on to X. The identity map $\mathsf{id}\colon X \to X$ defined by $\mathsf{id}(x) = x$ is obviously bijective. To show that $\approx$ is symmetric, assume $X \approx Y$. Then there is a bijection $f\colon X \to Y$. By Proposition 2.2.11, $f^{-1}\colon Y \to X$ is also bijective. Hence, $Y \approx X$. Finally, to show that $\approx$ is transitive, assume $X \approx Y$ and $Y \approx Z$. Then there are bijections $f\colon X \to Y$ and $g\colon Y \to Z$. Now, from Exercise 8(a) in Section 2.2, we know that gf is also surjective, so we need only check if gf is injective. To this end, assume $gf(x) = gf(y)$. Then $g(f(x)) = g(f(y))$ by definition. Hence, since g is injective, $f(x) = f(y)$ and so $x = y$ by the injectivity of f. The map gf is thus a bijection from X on to Z, so $X \approx Z$.

(7) Assume S is countable and let $a \notin S$. If S is finite, then there exists a bijection f between S and $\mathbb{N}_n$ for some $n \in \mathbb{N}$. Define

$$g(x) = \begin{cases} n & \text{if } x = a \\ f(x) & \text{otherwise .} \end{cases}$$

It is then easy to check that g, so defined, is a bijection between $S \cup \{a\}$ and $\mathbb{N}_{n+1}$, and hence that $S \cup \{a\}$ is finite and therefore countable. On the other hand, suppose S is countably infinite. Then there is a bijective map f from S on to $\mathbb{N}$. Now consider the map $g\colon S \cup \{a\} \to \mathbb{N}$ defined by

$$g(x) = \begin{cases} 0 & \text{if } x = a \\ f(x) + 1 & \text{otherwise .} \end{cases}$$

We first show that g is surjective, so let $n \in \mathbb{N}$. If $n = 0$, then $f(a) = 0 = n$. On the other hand, if $n \neq 0$, then $n = m + 1$ for some $m \in \mathbb{N}$. However, we know that f is surjective, so there is some $s \in S$ such that $f(s) = m$. Hence, $g(s) = f(s) + 1 = m + 1 = n$. To show that g is injective, assume $g(x) = g(y)$. If $g(x) = g(y) = 0$, then clearly $x = y = a$, so if $g(x) = g(y) \neq 0$, we have $f(x) + 1 = f(y) + 1$. Subtracting 1 on both sides gives $f(x) = f(y)$. However, f is injective, so $x = y$.

(9a) Assume A and B are countable sets. Now, we know that $A \cap B \subseteq A$ and $A \cap B \subseteq B$, so, by Lemma 2.7.6, $A \cap B$ is also countable.

(9b) We will use the fact, which can be easily proven, that a set S is countable iff there exists an injection $f : S \to \mathbb{N}$. We can write $A \cup B$ as the union of two disjoint sets: $A \cup (B - A)$. Since $(B - A) \subseteq B$, we can conclude by Lemma 2.7.6 that $(B - A)$ is countable. Hence there are injective maps $f : A \to \mathbb{N}$ and $g : (B - A) \to \mathbb{N}$. Define $h : A \cup B \to \mathbb{N}$ as follows:

$$h(x) = \begin{cases} 2^{f(x)} & \text{if } x \in A \\ 3^{g(x)} & \text{if } x \in B - A. \end{cases}$$

It is easy to prove that h, so defined, is an injection.

(9c) As above, we will use the fact that a set S is countable iff there exists an injection $f : S \to \mathbb{N}$. Since A and B are countable there exist injections $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$. Define $h : A \times B \to \mathbb{N}$ as follows:

$$h(a, b) = 2^{f(a)} \times 3^{g(b)}.$$

To see that h is an injection, suppose that $h(a, b) = h(a', b')$, i.e. $2^{f(a)} \times 3^{g(b)} = 2^{f(a')} \times 3^{g(b')}$. If follows by the uniqueness of the prime factorization of integers (see the Fundamental Theorem of Arithmetic, Theorem 5.4.8) that $f(a) = f(a')$ and $f(b) = f(b')$. Hence, by the injectivity of f and h, we have $a = a'$ and $b = b'$, i.e. $(a, b) = (a', b')$.

(10) Consider the map $g\colon \mathcal{P}(\mathbb{N}_n) \to F_n$ defined by $g(X) = f$ such that $f(i) = 1$ if $i \in X$ and $f(i) = 0$ otherwise. It is easy to see that g is surjective. To show that g is injective, assume $X \neq Y$. Then there is some $i \in \mathbb{N}_n$ such that $i \in X$ but $i \notin Y$ or $i \in Y$ but $i \notin X$. In the first case, $g(X) = f'$ and $g(Y) = f''$ such that $f'(i) = 1$ and $f''(i) = 0$. Hence, $g(X) \neq g(Y)$, and similarly for the second case.

(11) First, note that $\mathbb{N}_n \subseteq \mathbb{N}$ for every $n \in \mathbb{N}$. Hence, by Proposition 2.7.10, $|\mathbb{N}_n| \leq |\mathbb{N}|$. However, $|\mathbb{N}_n| = n$ and $|\mathbb{N}| = \aleph_0$, so $n \leq \aleph_0$ for every $n \in \mathbb{N}$.

(12a) Assume $|K_1| = \kappa = |K_2|$ and $|L_1| = \lambda = |L_2|$, and suppose there is an injection $f\colon K_1 \to L_1$. Then $|K_1| \leq |L_1|$ by Definition 2.7.9, and so, by our assumption, $|K_2| \leq |L_2|$. Hence, by Definition 2.7.9, there is an injection $g\colon K_2 \to L_2$. The converse is proved in a similar fashion.

(12b) Consider the identity map $\mathsf{id}\colon X \to X$ defined by $\mathsf{id}(x) = x$. To show that id is injective, assume $\mathsf{id}(x) = \mathsf{id}(y)$. Then $x = y$ by the definition of id, so we are done. Now, by Definition 2.7.9, $|X| \leq |X|$, meaning that $\leq$ is reflexive.

(12c) Suppose that there exist injections $f : X \to Y$ and $g : Y \to Z$. Now, consider the map $gf\colon X \to Z$. We have to show that gf is injective, so assume $gf(x) = gf(y)$. By definition, $g(f(x)) = g(f(y))$. However, g is injective, so $f(x) = f(y)$, and so, since f is also injective, $x = y$. Now, assume $|X| \leq |Y|$ and $|Y| \leq |Z|$. Then there are injections $f : X \to Y$ and $g : Y \to Z$. Using the result we have just proven, we know there is an injection $gf : X \to Z$. Hence, by Definition 2.7.9, $|X| \leq |Z|$.

(12d) Assume $X \subseteq Y$. The map $f\colon X \to Y$ defined by $f(x) = x$ works here. Therefore $|X| \leq |Y|$ by Definition 2.7.9.

2.8. Isomorphisms of ordered sets. Ordinal numbers

(1) Let S be the set of binary strings of length at most 2, and consider the map $f\colon X \to S$ defined by $f(\varnothing) = \varnothing$, $f(\{1\}) = 0, f(\{2\}) = 1, f(\{1,3\}) = 00, f(\{1,4\}) = 01, f(\{2,5\}) = 10$ and $f(\{2,6\}) = 11$. It is not difficult to see that f is an order preserving bijection from X on to S, which means that $(X, \subseteq)$ is order isomorphic to the set S ordered by the initial segment relation.

(2) If posets $(X, \leq_X)$ and $(Y, \leq_Y)$ are order isomorphic, there is an order preserving bijection from X on to Y. For X and Y to be equinumerous, we only need a bijection from X on to Y, which we indeed have.

(3) We have to show that $f\colon \mathbb{N}^+ \to \omega + 1$ is bijective and preserves order. First, we show that f is surjective, so let $x \in \omega + 1$. If $x \in \mathbb{N}$, we know that $f(x) = x$. On the other hand, if $x = \omega$, we have $f(0') = \omega = x$. Next we show that f preserves order. For the left-to-right direction, assume $n_1 \leq n_2$. We now have the following cases:

Case 1: both n_1 and n_2 are naturals.
Then we have $f(n_1) = n_1 \leq n_2 = f(n_2)$.

Case 2: n_1 is a natural number and $n_2 = 0'$.
Then $f(n_1) = n_1$ and $f(n_2) = \omega$ and so, since $\omega > n_1, f(n_1) \leq f(n_2)$.

Case 3: $n_1 = n_2 = 0'$.
Here $f(n_1) = f(n_2) = \omega$, so $f(n_1) \leq f(n_2)$. Conversely, assume $n_1 \leqq n_2$. Then we have two cases:

Case a: both n_1 and n_2 are naturals.
In this case, $f(n_1) = n_1 \leqq n_2 = f(n_2)$.

Case b: n_2 is a natural number and $n_1 = 0'$.
Then we have $f(n_1) = \omega \leqq n_2 = f(n_2)$. Since every order preserving map is injective, we are done.

(4) We have to show that $g\colon A \to \omega \cdot 2$ is an order preserving bijection. First, to show that g is surjective, let $m \in \omega \cdot 2$. If $m \in \mathbb{N}$, then $g(m) = m$. On the other hand, if $m = \omega + n$ for some $n \in \mathbb{N}$, then $g(n') = \omega + n = m$ (specifically, $g(0') = \omega + 0 = \omega$). Next we show that g is order preserving. For the left-to-right direction, assume $n_1 \leq n_2$. Then we have the following cases:

***Case 1: both n_1 and n_2* are natural numbers.**
Then $f(n_1) = n_1 \leq n_2 = f(n_2)$.

Case 2: $n_1 = m_1'$ and $n_2 = m_2'$ for $m_1, m_2 \in \mathbb{N}$.
Since $m_1' \leq m_2'$, $m_1 \leq m_2$, so $f(n_1) = \omega + m_1 \leq \omega + m_2 = f(n_2)$.

Case 3: $n_1 \in \mathbb{N}$ and $n_2 = m_2'$ for $m_2 \in \mathbb{N}$.

Then $f(n_1) = n_1 \leq \omega + m_2 = f(m_2') = f(n_2)$. For the converse direction, assume $n_1 \leqq n_2$. We then have the following cases:

Case a: both n_1 and n_2 are naturals.
Then $f(n_1) = n_1 \leqq n_2 = f(n_2)$.

Case b: $n_1 = m_1'$ and $n_2 = m_2'$ for $m_1, m_2 \in \mathbb{N}$.
Clearly, $m_1 \leqq m_2$, so $f(n_1) = \omega + m_1 \leqq \omega + m_2 = f(n_2)$.

Case c: $n_2 \in \mathbb{N}$ and $n_1 = m_1'$ for $m_1 \in \mathbb{N}$.
Here $f(n_1) = \omega + m_1 \leqq n_2 = f(n_2)$.

(5) It is enough to show that there exists an injection from $\omega \cdot n$ into $\mathbb{N}$. Let p_i denote the ith prime number, starting with 2 as the 0th prime number. Then $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, etc. Define $f : \omega \cdot n \to \mathbb{N}$ by letting $f(\omega \cdot m + k) = p_m^{k+1}$. For example, $f(144) = f(\omega \cdot 0 + 144) = 2^{145}$ and $f(\omega \cdot 2) = f(\omega \cdot 2 + 0) = 5^1$. Using the Fundamental Theorem of Arithmetic (Theorem 5.4.8), it is not difficult to check that f, so defined, is an injection.

(6a) First, $f(x) \leq f(x)$ for all $x \in X$, so $f \leqq f$, which means that $\leqq$ is reflexive. To show that $\leqq$ is transitive, assume $f_1 \leqq f_2$ and $f_2 \leqq f_3$. Then $f_1(x) \leq f_2(x)$ for all $x \in X$ and $f_2(x) \leq f_3(x)$ for all $x \in X$. However, $\leq$ is transitive on $\{0, 1\}$, so $f_1(x) \leq f_3(x)$ for all $x \in X$, which means that $f_1 \leqq f_3$. Finally, to show that $\leqq$ is antisymmetric, assume $f_1 \leqq f_2$ and $f_2 \leqq f_1$. Then $f_1(x) \leq f_2(x)$ for all $x \in X$ and $f_2(x) \leq f_1(x)$ for all $x \in X$, and so, since $\leq$ is antisymmetric on $\{0, 1\}$, we have $f_1(x) = f_2(x)$ for all $x \in X$. Hence, $f_1 = f_2$.

(6b) We have to find an order preserving bijection from 2^X on to $\mathcal{P}(X)$. Consider the map g: $2^X \to \mathcal{P}(X)$ defined by

$$g(f) = \{x \in X \mid f(x) = 1\}.$$

It is easy to see that g is surjective. Next we show that g is order preserving, so for the left-to-right direction, assume $f_1 \not\leqq f_2$. This means that $f_1(x) \leq f_2(x)$ for all $x \in X$. We have to show that $g(f_1) \subseteq g(f_2)$, so let $x \in g(f_1)$. Then $f_1(x) = 1$, and so, since $f_1(x) \leq f_2(x)$, it must be the case that $f_2(x) = 1$. Hence, $x \in g(f_2)$, which means that $g(f_1) \subseteq g(f_2)$. Conversely, assume $f_1 \not\leqq f_2$. Then there is an $x \in X$ such that $f_1(x) \not\leq f_2(x)$. This can only mean that $f_1(x) = 1$, while $f_2(x) = 0$. Then $x \in g(f_1)$, while $x \notin g(f_2)$, and so $g(f_1) \not\subseteq g(f_2)$.

(7a) We have to show that $\leq_Z'$ is a well-founded linear order. For the reflexivity of $\leq_Z'$, let $z \in Z - \{z_0\}$. However, $Z - \{z_0\} \subseteq Z$, so $z \in Z$. Hence, by the reflexivity of $\leq_Z$, $z \leq_Z z$, which means that $z \leq_Z' z$ since $z \in Z - \{z_0\}$. To show that $\leq_Z'$ is transitive, assume $z_1 \leq_Z' z_2$ and $z_2 \leq_Z' z_3$. Since $z_1, z_2, z_3 \in Z - \{0\}$, $z_1, z_2, z_3 \in Z$, which means that $z_1 \leq_Z z_2$ and $z_2 \leq_Z z_3$. Hence, by the transitivity of $\leq_Z$, $z_1 \leq_Z z_3$, and so, since $z_1, z_3 \in Z - \{0\}$, we have $z_1 \leq_Z' z_3$. For the antisymmetry, assume $z_1 \leq_Z' z_2$ and $z_2 \leq_Z' z_1$. Then $z_1 \leq_Z z_2$ and $z_2 \leq_Z z_1$, which means that $z_1 = z_2$ by the antisymmetry of $\leq_Z$. To show that $\leq_Z'$ is connected, let $z_1, z_2 \in Z - \{z_0\}$. Then $z_1, z_2 \in Z$, and so, by the connectedness of $\leq_Z$, $z_1 \leq_Z z_2$ or $z_2 \leq_Z z_1$ or $z_1 = z_2$. Hence, since $z_1, z_2 \in Z - \{z_0\}$, $z_1 \leq_Z' z_2$ or $z_2 \leq_Z' z_1$ or $z_1 = z_2$. Finally, for the well-foundedness, assume $(Z - \{z_0\}, \leq_Z')$ contains an infinite strictly descending chain $\cdots <_Z' z_2 <_Z' z_1$. However, since $Z - \{z_0\} \subseteq Z$, $z_1, z_2, \ldots$ all belong to Z as well, so $\cdots <_Z z_2 <_Z z_1$, contradicting the fact that $(Z, \leq_Z)$ is well-founded.

(7b) First, for the reflexivity, let $z \in Z \cup \{a\}$. If $z = a$, $a \leq_Z^+ a$ by definition. If $z \neq a$, $z \in Z$, and so $z \leq_Z z$. Hence, by the definition of $\leq_Z^+$, $z \leq_Z^+ z$. For the transitivity, assume $z_1 \leq_Z^+ z_2$ and $z_2 \leq_Z^+ z_3$. We then have the following cases:

Case 1: $z_1, z_2, z_3 \in Z$.
Then $z_1 \leq_Z z_2$ and $z_2 \leq_Z z_3$, which means that $z_1 \leq_Z z_3$ by the transitivity of $\leq_Z$. Hence, by the definition of $\leq_Z^+$, $z_1 \leq_Z^+ z_3$.

Case 2: $z_1 = a$ and $z_2, z_3 \in Z$.
By the definition of $\leq_Z^+$, $(a, z_3) \in \leq_Z^+$, so $z_1 \leq_X^+ z_3$.

Case 3: $z_1 = z_2 = a$ and $z_3 \in Z$.
Again, by the definition of $\leq_Z^+$, $(a, z_3) \in \leq_Z^+$, which means $z_1 \leq_Z^+ z_3$.

Case 4: $z_1 = z_2 = z_3 = a$.

By the definition of $\leq_Z^+$, $z_1 \leq_Z^+ z_3$. To show that $\leq_Z^+$ is antisymmetric, assume $z_1 \leq_Z^+ z_2$ and $z_2 \leq_Z^+ z_1$. We have two cases:

Case a: $z_1, z_2 \in Z$.
Then $z_1 \leq_Z z_2$ and $z_2 \leq_Z z_1$, so, by the antisymmetry of $\leq_Z$, $z_1 = z_2$.

Case b: $z_1 = a = z_2$.

Clearly, $z_1 = z_2$. Finally, we show that $(Z \cup \{a\},\ \leq_Z^+)$ is well-founded, so suppose $(Z \cup \{a\},\ \leq_Z^+)$ contains an infinitely descending chain $\cdots <_Z^+ z_2 <_Z^+ z_1$. Note that none of the elements in this chain can be a (since there is no element strictly less than a), so this means that $\cdots <_Z z_2 <_Z z_1$, contradicting the fact that $(Z,\ \leq_Z)$ is well-founded.

(7c) Assume that $(X,\ \leq_X) \cong (Y,\ \leq_Y)$. Then there is an order preserving bijection $f\colon X \to Y$. We have to find an order preserving bijection from $X \cup \{a\}$ on to $Y \cup \{a\}$. Consider the map $g\colon X \cup \{a\} \to Y \cup \{b\}$ defined by

$$g(x) = \begin{cases} f(x) & \text{if } x \in X \\ b & \text{if } x = a. \end{cases}$$

First, to show that g is surjective, let $y \in Y \cup \{b\}$. If $y = b$, then a works since $g(a) = b$. On the other hand, if $y \in Y$, we know from the surjectivity of f that there is an $x \in X$ such that $f(x) = y$. Thus $g(x) = f(x) = y$, meaning that x works here. Next we show that g is order preserving, so for the left-to-right direction, assume $x \leq_X^+ x'$. We then have the following cases:

Case 1: $x, x' \in X$.
Then $x \leq_X x'$ by the definition of $\leq_X^+$, and so, since f preserves order, $f(x) \leq_Y f(x')$. Hence, $g(x) \leq_Y^+ g(x')$.

Case 2: $x = a$ ***and*** $x' \in X$.
Then $g(x) = b$ and $g(x') = f(x') \in Y$, which means that $g(x) \leq_Y^+ g(x')$ by the definition of $\leq_Y^+$.

Case 3: $x = a = x'$.
Then $g(x) = g(x') = b$, so $g(x) \leq_Y^+ g(x')$. Conversely, assume $x \not\leq_X^+ x'$. Again we have the following cases:

Case a: $x, x' \in X$.
Since f preserves order, $f(x) \not\leq_Y f(x')$, which means that $g(x) \not\leq_Y^+ g(x')$.

Case b: $x \in X$ ***and*** $x' = a$.
Then $g(x) = f(x) \in Y$ and $g(x') = g(a) = b$, so $g(x) \not\leq_Y^+ g(x')$.

(7d) The base case is obvious. Our inductive hypothesis is that if $(X,\ \leq_X)$ and $(Y,\ \leq_Y)$ are finite well orders such that $|X| = |Y| = k$, then $(X,\ \leq_X) \cong (Y,\ \leq_Y)$. Now, assume that $(X', \leq_{X'})$ and $(Y', \leq_{Y'})$ are finite well orders such that $|X'| = |Y'| = k + 1$. We now consider the sets $X' - \{a\}$ and $Y' - \{b\}$, where a and b are the least elements of X' and Y', respectively (note that these exist since both X' and Y' are well orders). We know that $(X' - \{a\},\ \leq'_{X'})$ and $(Y' - \{b\},\ \leq'_{Y'})$ are well orders by (7a). Furthermore, $|X' - \{a\}| = |Y' - \{b\}| = k$ so, by the inductive hypothesis, $(X' - \{a\},\ \leq'_{X'}) \cong (Y' - \{b\},\ \leq'_{Y'})$. Now, we add a and b back to $X' - \{a\}$ and $Y' - \{b\}$, respectively, to obtain X' and Y' back again. From Exercise 7(b), we know that these are also well orders and, by Exercise 7(c), $(X', \leq_{X'}) \cong (Y', \leq_{Y'})$.

2.9. Application: relational databases

(1a) Table 2.1

Table 2.1 *Enrollment*2013 ∩ *Enrollment*2014

Student ID	Course
647537	Psychology
723934	Algebra

(1b) Table 2.2

Table 2.2 *Enrollment*2014 – *Enrollment*2013

Student ID	Course
268356	Algebra
268356	Chemistry
186753	Psychology
647537	French

(1c) Table 2.3

Table 2.3 *Student* × *Lecturer*

Name	Student ID	Study year	Lecturer name	Course
W Adams	186753	2	W Morton	Algebra
S Nkosi	268356	1	W Morton	Algebra
T Ling	647537	3	W Morton	Algebra
U de Klerk	723934	1	W Morton	Algebra
W Adams	186753	2	F Jung	Psychology
S Nkosi	268356	1	F Jung	Psychology
T Ling	647537	3	F Jung	Psychology
U de Klerk	723934	1	F Jung	Psychology
W Adams	186753	2	D Shkatov	AI
S Nkosi	268356	1	D Shkatov	AI
T Ling	647537	3	D Shkatov	AI
U de Klerk	723934	1	D Shkatov	AI
W Adams	186753	2	B Mamba	Chemistry
S Nkosi	268356	1	B Mamba	Chemistry
T Ling	647537	3	B Mamba	Chemistry
U de Klerk	723934	1	B Mamba	Chemistry
W Adams	186753	2	J Southey	French
S Nkosi	268356	1	J Southey	French
T Ling	647537	3	J Southey	French
U de Klerk	723934	1	J Southey	French
W Adams	186753	2	Y Jacobs	Calculus
S Nkosi	268356	1	Y Jacobs	Calculus
T Ling	647537	3	Y Jacobs	Calculus
U de Klerk	723934	1	Y Jacobs	Calculus

(1d) Table 2.4

Table 2.4 $\pi_{\text{Name, StudyYear}}(\textit{Student})$

Name	Study year
W Adams	2
S Nkosi	1
T Ling	3
U de Klerk	1

(1e) Table 2.5

Table 2.5 $\Theta_{1<\text{StudyYear}}(\textit{Student})$

Name	Student ID	Study year
W Adams	186753	2
T Ling	647537	3

(1f) Table 2.6

Table 2.6 $\textit{Student} \bowtie \textit{Enrollment}2014$

Name	Student ID	Study year	Course
W Adams	186753	2	Psychology
S Nkosi	268356	1	Algebra
S Nkosi	268356	1	Chemistry
T Ling	647537	3	Psychology
T Ling	647537	3	French
U de Klerk	723934	1	Algebra

(1g) Table 2.7

Table 2.7 $\pi_{\text{Name, Course}}(\textit{Student} \bowtie \textit{Enrollment}2014)$

Name	Course
W Adams	Psychology
S Nkosi	Algebra
S Nkosi	Chemistry
T Ling	Psychology
T Ling	French
U de Klerk	Algebra

(2a) $\pi_{\text{Student ID}}(\Theta_{\text{Course=Psychology}}(\textit{Enrollment}2014 \cap \textit{Enrollment}2013))$

(2b) $\pi_{\text{Student ID}}(\Theta_{\text{Course=Algebra}}(\textit{Enrollment}2013))$

(2c) $\pi_{\text{Lecturer Name}}(\Theta_{\text{Study } \textit{Year}=2}(\textit{Student} \bowtie \textit{Enrollment}2014 \bowtie \textit{Lecturer}))$

(2d) $\pi_{\text{Lecturer Name}}(\Theta_{\text{Name=S } \textit{Nkosi}}(\textit{Student} \bowtie \textit{Enrollment}2014 \bowtie \textit{Lecturer}))$

(3a) $\pi_{\text{Pet } \textit{Name}}(\Theta_{\text{Type=Dog}\wedge\text{Vet } \textit{Name}=\text{DrYang}}(\textit{Pets}))$

(3b) $\pi_{\text{Pet } \textit{Name}, \text{Owner}}(\Theta_{\text{Type=Dog}}(\textit{Pets}))$

(3c) $\pi_{\text{Pet } \mathit{Name}}(\Theta_{\text{Day } \mathit{off}=\text{Sun} \wedge \text{Type}=\text{Dog}}(\mathit{Pets} \bowtie \mathit{Vets}))$

(3d) $\pi_{\text{Owner}}(\Theta_{\text{Client Name}=\text{Owner} \wedge \text{Day } \mathit{off}=\text{Sun}}((\mathit{Pets} \bowtie \mathit{Vets}) \times \mathit{Clients}))$

(4a) Let R and S be two relations which share the attributes $A_1, \ldots, A_k$. Then the semi-join of R and S is given by

$$\pi_{\langle \text{list} \rangle}(\Theta_{\text{R}.A_1=\text{S}.A_1, \ldots, \text{R}.A_k=\text{S}.A_k}(R \times S)),$$

where $\langle$list$\rangle$ is the list of all attributes of R.

(4b) Table 2.8

Table 2.8 *Lecturer* $\ltimes$ *Enrollment*2013

Lecturer name	Course
W Morton	Algebra
F Jung	Psychology
D Shkatov	AI
J Southey	French

(4c) Let R and S be two relations with attributes $A_1, \ldots, A_k, B_1, \ldots, B_n$ and $A_1, \ldots, A_k, C_1, \ldots, C_m$, respectively. Then

$$\begin{aligned}
&(a_1, \ldots, a_{k+m+n}) \in R \bowtie S \\
&\iff (a_1, \ldots, a_{k+m+n}) \in \pi_{\text{R}.A_1, \ldots, \text{R}.A_k, B_1, \ldots, B_m, C_1, \ldots, C_n}(\Theta_{\text{R}.A_1=\text{S}.A_1, \ldots, \text{R}.A_k=\text{S}.A_k}(R \times S)) \\
&\iff (a_1, \ldots, a_{k+m+n}) \in \pi_{\text{R} \ltimes S.A_1, \ldots, \text{R} \ltimes S.A_k, B_1, \ldots, B_m, C_1, \ldots, C_n}(\Theta_{\text{R} \ltimes S.A_1=\text{S}.A_1, \ldots, \text{R} \ltimes S.A_k=\text{S}.A_k}((R \ltimes S) \times S)) \\
&\iff (a_1, \ldots, a_{k+m+n}) \in (R \ltimes S) \bowtie S,
\end{aligned}$$

where the third step follows form the fact that R and $R \ltimes S$ have the same attributes.

(5a) Table 2.9

Table 2.9

Name	Student ID	Study year
S Nkosi	268356	1

(5b) It returns the details of all students enrolled for both Chemistry and Algebra in 2014.

(5c) $\mathit{Clients} \ltimes [\pi_{\text{Owner,Vet Name}}(\mathit{Pets}) \div \pi_{\text{Vet Name}}(\Theta_{\text{Vet Name = Dr Dolittle}}(\mathit{Vets}))]$

(5d) $\pi_{A_1, \ldots, A_{n-m}}(\Theta_{\text{R}.B_1=\text{S}.B_1, \ldots, \text{R}.B_m=\text{S}.B_m}(R \times S))$

3

Propositional Logic

3.1. Propositions, logical connectives, truth tables, tautologies

(1a) Antecedent: "John talks". Consequent: "Everyone else listens".

(1b) Antecedent: "John talks". Consequent: "Everyone else listens".

(1c) Antecedent: "John talks". Consequent: "Everyone else listens".

(1d) Antecedent: "The cube of an integer n is positive". Consequent: "The integer n is positive".

(1e) Antecedent: "The integer n is positive". Consequent: "The cube of n is positive".

(1f) Antecedent: "A function f is differentiable". Consequent: "The function f is continuous".

(1g) Antecedent: "A function f is differentiable". Consequent: "The function f is continuous".

(1h) Antecedent: "A function f is continuous". Consequent: "The function f is differentiable".

(2a) Neither

(2b) Sufficient

(2c) Neither

(2d) Necessary

(2e) Necessary and sufficient

(2f) Sufficient

(2g) Necessary

(2h) Necessary

(2i) Necessary and sufficient

(3a) Since both P and $P \to Q$ are true, Q must be true, by truth table of $\to$.

(3b) Suppose $R \wedge S$ is false. Since $P \wedge S$ is true, P and S are true. Hence, R must be false. Since $P \to Q$ is true, Q is true. Thus, for $Q \to R$ to be true, R must be true, which is a contradiction. Hence, $R \wedge S$ is true.

(3d) Suppose Q is true. Since $\neg P \to \neg Q$ must be true, $\neg P$ must be false, and thus P is true. For $P \wedge \neg R$ to be false, $\neg R$ must be false. However, this is a contradiction with $\neg R$ true. Hence, Q is false.

Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

(4a) The statement is true, since wherever $Q \to (R \wedge S)$ is true and $Q \wedge S$ is false, $R \wedge Q$ is also false:

Q	R	S	Q	$\to$	$(R \wedge S)$	$(Q \wedge S)$	$(R \wedge Q)$
F	F	F	F	T	FFF	FFF	FFF
F	F	T	F	T	FFT	FFT	FFF
F	T	F	F	T	TFF	FFF	TFF
F	T	T	F	T	TTT	FFT	TFF
T	F	F	T	F	FFF	TFF	FFT
T	F	T	T	F	FFT	TTT	FFT
T	T	F	T	F	TFF	TFF	TTT
T	T	T	T	T	TTT	TTT	TTT
				↑		↑	↑

(4c) The statement is true, since wherever $\neg P \to (\neg Q \vee \neg R)$ and $Q \wedge (P \vee R)$ are true, P is also true:

P	Q	R	$\neg P$	$\to$	$(\neg Q \vee \neg R)$	Q	$\wedge$	$(P \vee R)$	P
F	F	F	T	T	TTT	F	F	FFF	F
F	F	T	T	T	TTF	F	F	FTT	F
F	T	F	T	T	FTT	T	F	FFF	F
F	T	T	T	F	FFF	T	T	FTT	F
T	F	F	F	T	TTT	F	F	TTF	T
T	F	T	F	T	TTF	F	F	TTT	T
T	T	F	F	T	FTT	T	T	TTF	T
T	T	T	F	T	FFF	T	T	TTT	T
				↑			↑		↑

(5a) $\neg(p \to \neg p)$ is satisfiable:

p	$\neg$	$(p \to \neg p)$
F	F	FTT
T	T	TFF
	↑	

(5b) $p \vee (p \to \neg p)$ is a tautology:

p	p	$\vee$	$(p \to \neg p)$
F	F	T	FTT
T	T	T	TFF
		↑	

(5c) $p \wedge (q \vee \neg q)$ is satisfiable.

(5d) $\neg((p \wedge \neg p) \to q)$ is a contradiction:

p	q	$\neg$	$((p \wedge \neg p)$	$\to$	$q)$
F	F	F	FFT	T	F
F	T	F	FFT	T	T
T	F	F	TFF	T	F
T	T	F	TFF	T	T
		↑			

(5e) $\neg p \wedge \neg(p \to q)$ is a contradiction.

(5f) $((p \to q) \to p) \to p$ is a tautology:

p	q	$((p \to q)$	$\to$	$p)$	$\to$	p
F	F	F T F	F	F	T	F
F	T	F T T	F	F	T	F
T	F	T F F	T	T	T	T
T	T	T T T	T	T	T	T
					↑	

(5g) $(p \vee \neg q) \to \neg(q \wedge \neg p)$ is a tautology.

(5h) $((p \to q) \wedge (q \to r)) \wedge \neg(\neg p \vee r)$ is a contradiction:

p	q	r	$((p \to q)$	$\wedge$	$(q \to r))$	$\wedge$	$\neg(\neg p \vee r)$
F	F	F	F T F	T	F T F	F	F T T F
F	F	T	F T F	T	F T T	F	F T T T
F	T	F	F T T	F	T F F	F	F T T F
F	T	T	F T T	T	T T T	F	F T T T
T	F	F	T F F	F	F T F	F	T F F F
T	F	T	T F F	F	F T T	F	F F T T
T	T	F	T T T	F	T F F	F	T F F F
T	T	T	T T T	T	T T T	F	F F T T
						↑	

(5i) $\neg(\neg p \leftrightarrow q) \wedge (r \vee \neg q)$ is satisfiable.

(5j) $\neg((p \wedge \neg q) \to r) \leftrightarrow (\neg(q \vee r) \to \neg p)$ is a contradiction.

(6a) P is a truth teller and Q a liar.

(6b) If the answer was yes, the inhabitant he asked is a truth teller and the other inhabitant a liar. If the answer was no, both are truth tellers.

(6c) Both A and B are truth tellers.

(6d) Note that no local can say that he is a liar, so Y's statement must be false, making him a liar. However, this means that Z's statement is true, so he is a truth teller. Since X's answer invariably would be "I'm a truth teller", it is not possible to determine whether X is a truth teller or liar from the information provided.

(6e) The stranger should go with inhabitant E since E is not a man-eater.

(6f) The stranger could ask either inhabitant, "What would your answer be if I asked you if your path leads to the spaceship port?"

3.2. Propositional logical consequence. Valid and invalid propositional inferences

(1) Assume $A_1, A_2, \ldots, A_n \vDash B$. Then, for all assignments of truth values to the variables occurring in $A_1, A_2, \ldots, A_n, B$, if $A_1, A_2, \ldots, A_n$ are true, then B is also true. Hence, for all assignments of truth values to the variables occurring in $A_1, A_2, \ldots, A_n, B$, $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ is true. Thus, $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ is a tautology. For the converse, assume $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ is a tautology. Then, for all assignments of truth values to the variables occurring in $A_1, A_2, \ldots, A_n, B$, $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ is true. Hence, for all assignments of truth values to the variables occurring in $A_1, A_2, \ldots, A_n, B$, if $A_1, A_2, \ldots, A_n$ are true, then B is also true. Thus, by definition, $A_1, A_2, \ldots, A_n \vDash B$.

(3a) The inference rule is sound.

(3b) The inference rule is *not* sound since the third and seventh row contain premises with truth values T but with a truth value F for the conclusion:

p	q	r	$p \to q$	$p \vee \neg r$	$\neg r$	$\neg q \vee r$
F	F	F	F T F	F T T	T	T T F
F	F	T	F T F	F F F	F	T T T
F	T	F	F T T	F T T	T	F F F
F	T	T	F T T	F F F	F	F T T
T	F	F	T F F	T T T	T	T T F
T	F	T	T F F	T T F	F	T T T
T	T	F	T T T	T T T	T	F F F
T	T	T	T T T	T T F	F	F T T
			↑	↑	↑	↑

(3c) The inference rule is sound.

(3d) The inference rule is sound since wherever the premises have truth values, the conclusion also has a truth value T:

p	q	r	$((p \wedge q)$	$\to$	$r)$	$\neg$	$(p \to r)$	$q \to r$
F	F	F	F F F	T	F	F	F T F	F T F
F	F	T	F F F	T	T	F	F T T	F T T
F	T	F	F F T	T	F	F	F T F	T F F
F	T	T	F F T	T	T	F	F T T	T T T
T	F	F	T F F	T	F	T	T F F	F T F
T	F	T	T F F	T	T	F	T T T	F T T
T	T	F	T T T	F	F	T	T F F	T F F
T	T	T	T T T	T	T	F	T T T	T T T
				↑		↑		↑

(4a) The inference rule is

$$\frac{p}{p \vee q}.$$

It is sound.

(4b) Denote "a is greater than -1" by p and "a is greater than -2" by q. Then the inference rule for the argument can be written as

$$\frac{p \to q,\ \neg q}{\neg p}.$$

This inference rule is sound.

(4c) Denote "The triangle ABC has a right angle" by p and "The triangle ABC is equilateral" by q. Then the inference rule for the argument can be written as

$$\frac{p \to \neg q,\ \neg p}{q}.$$

This inference rule is not sound. A falsifying assignment: p : F, q : F.

(4d) Denote "Bill likes logic" by p, "Bill is clever" by q and "Bill is rich" by r. Then the inference rule for the argument can be written as

$$\frac{p \to q,\ q \to r}{p \to r}.$$

This inference rule is sound.

(4e) Denote "n is divisible by 2" by p, "n is divisible by 3" by q and "n is divisible by 6" by r. Then the inference rule for the argument can be written as

$$\frac{(p \wedge q) \to r,\ r \to p,\ \neg q}{\neg r}.$$

The inference rule is *not* sound since the sixth row contains all premises with truth values T, but with a truth value F for the conclusion:

p	q	r	$((p \wedge q)$	$\to$	$r)$	$r \to p$	$\neg q$	$\neg r$
F	F	F	F F F	T	F	F T F	T	T
F	F	T	F F F	T	T	T F F	T	F
F	T	F	F F T	T	F	F T F	F	T
F	T	T	F F T	T	T	T F F	F	F
T	F	F	T F F	T	F	F T T	T	T
T	F	T	T F F	T	T	T T T	T	F
T	T	F	T T T	F	F	F T T	F	T
T	T	T	T T T	T	T	T T T	F	F
				↑		↑	↑	↑

(5a) **Converse:** If a is greater than -2, then a is greater than -1.
Inverse: If a is not greater than -1, then a is not greater than -2.
Contrapositive: If a is not greater than -2, then a is not greater than -1.

(5b) **Converse:** If x is not prime, then x is divisible by 6.
Inverse: If x is not divisible by 6, then x is prime.
Contrapositive: If x is prime, then x is not divisible by 6.

(5c) **Converse:** The square of x is positive only if x is positive.
Inverse: x is not positive only if its square is not positive.
Contrapositive: The square of x is not positive only if x is not positive.

(5d) **Converse:** The triangle ABC's medicentre and orthocentre coincide whenever it is equilateral.
Inverse: The triangle ABC is not equilateral whenever its medicentre and orthocentre do not coincide.
Contrapositive: The triangle ABC's medicentre and orthocentre do not coincide whenever it is not equilateral.

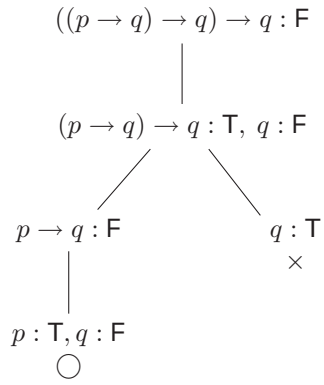
(5e) **Converse:** For the function f to be differentiable it is sufficient that it is continuous.
Inverse: For the function f to be discontinuous it is sufficient that it is not differentiable.
Contrapositive: For the function f to be not differentiable it is sufficient that it is discontinuous.

(5f) **Converse:** For the function f to be discontinuous it is sufficient that it is not differentiable.
Inverse: For the function f to be differentiable it is sufficient that it is continuous.
Contrapositive: For the function f to be continuous it is sufficient that it is differentiable.

(5g) **Converse:** For the integer n to be indivisible by 10 it is necessary that it is prime.
Inverse: For the integer n to be not prime it is necessary that it is divisible by 10.
Contrapositive: For the integer n to be divisible by 10 it is necessary that it is not prime.

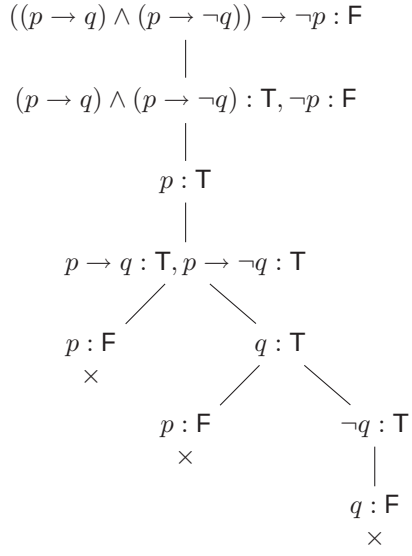
3.3. Semantic tableaux

(1a) The formula is *not* a tautology:

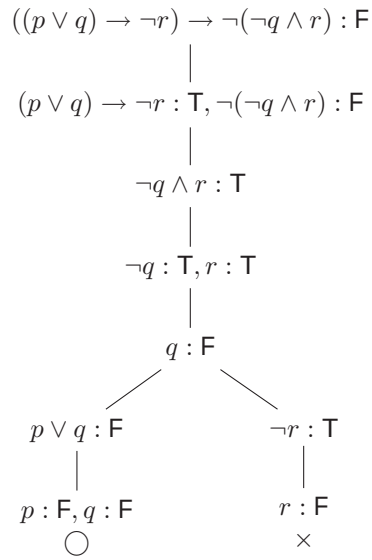


(1b) The formula is a tautology.

(1c) The formula is a tautology:

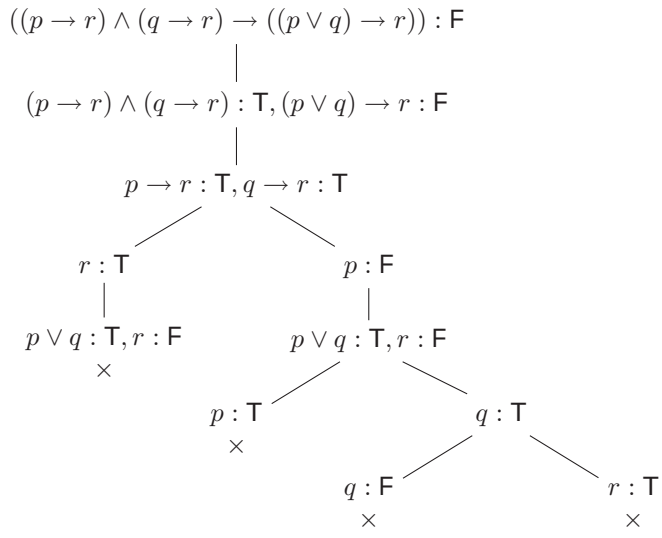


(1d) The formula is *not* a tautology:

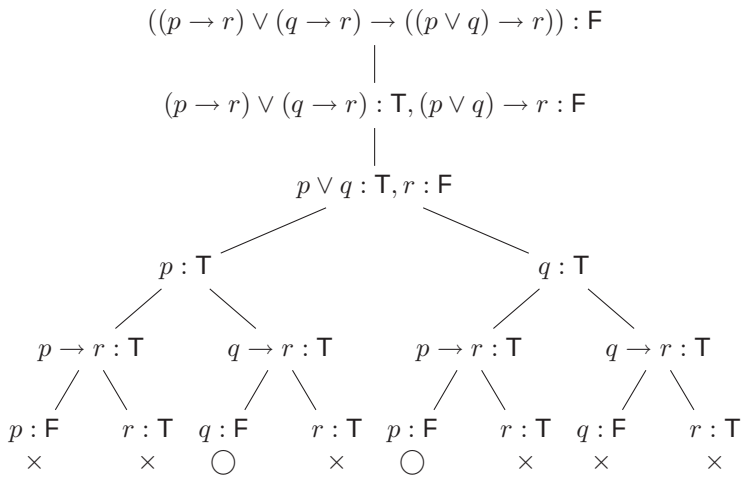


(1e) The formula is a tautology.

(1f) The formula is a tautology:

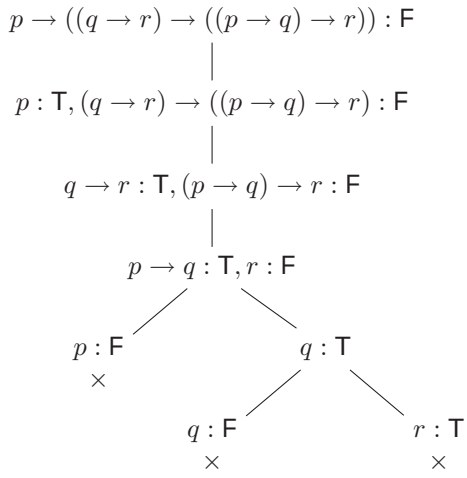


(1g) The formula is *not* a tautology:

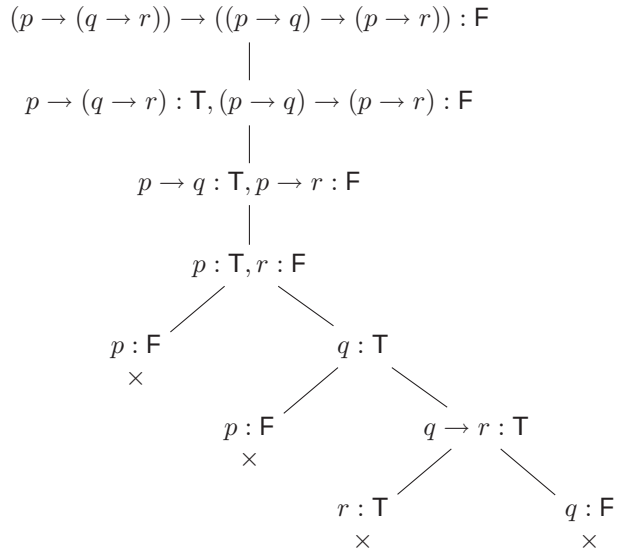


(1h) The formula is a tautology.

(1i) The formula is a tautology:

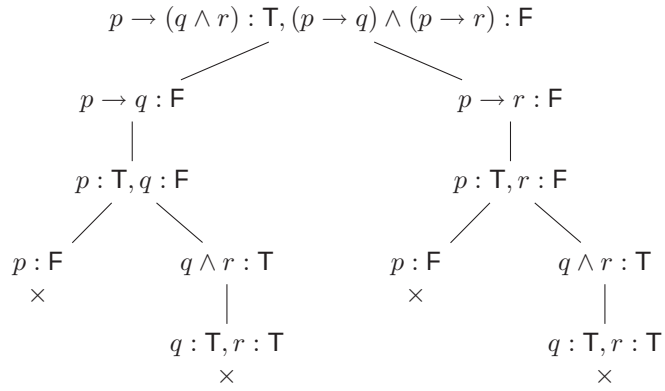


(1j) The formula is a tautology:

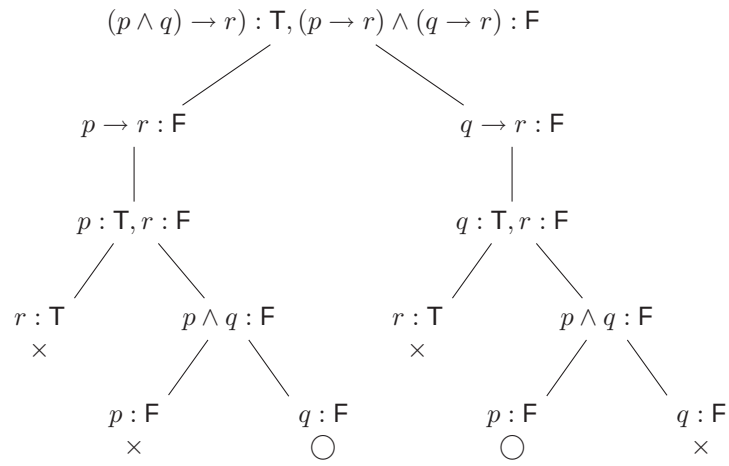


(2a) The logical consequence is valid.

(2b) The logical consequence is valid:

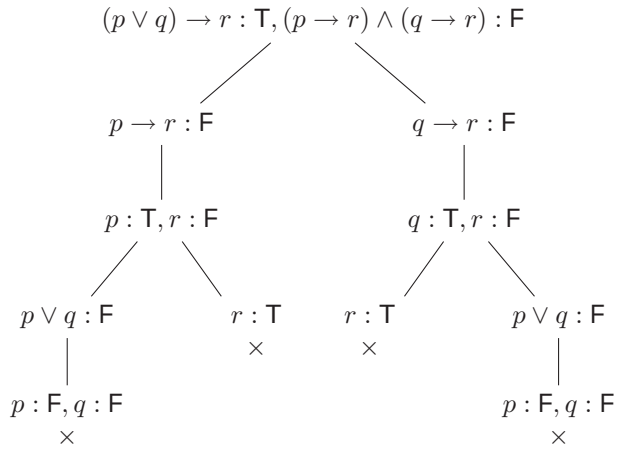


(2c) The logical consequence is not valid:



(2d) The logical consequence is valid.

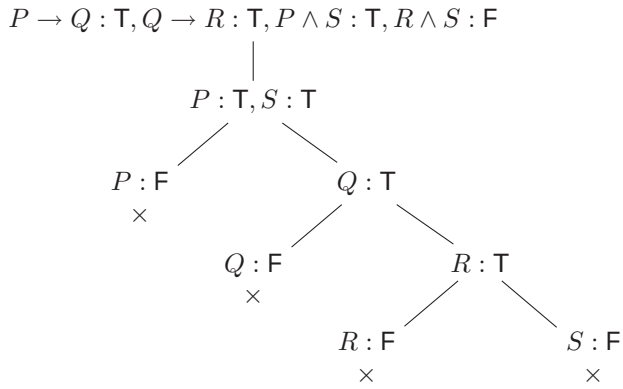
(2e) The logical consequence is valid:



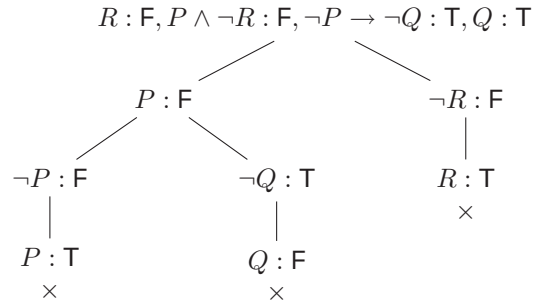
(2f) The logical consequence is valid.

(3) In each of these, we construct the tableau with all premises assigned the required truth values and the conclusion assigned the opposite truth value. If the tableau closes, then such a truth assignment is impossible; hence the stated consequence holds. If the tableau does not close, then the stated consequence does not necessarily hold.

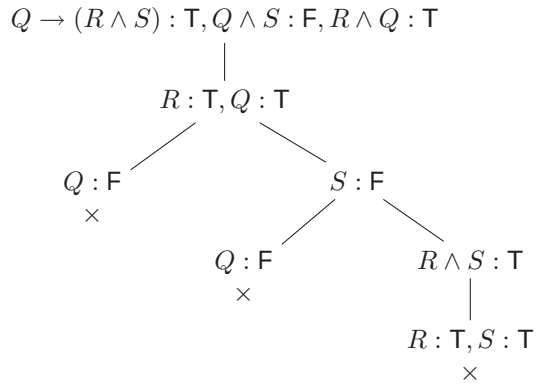
(3a) The tableau closes, so the consequence holds:



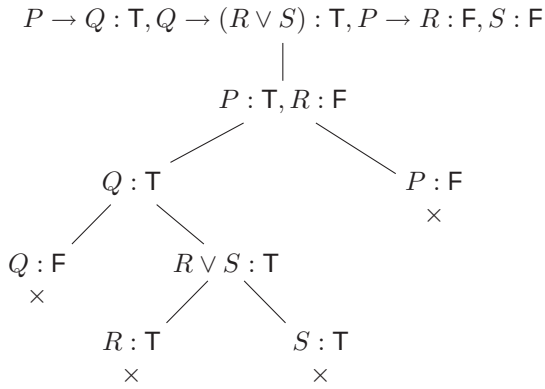
(3b) The tableau closes, so the consequence holds:



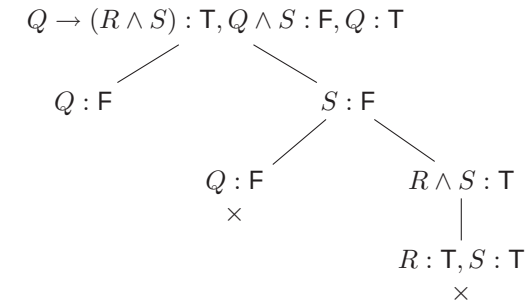
(3c) The tableau closes, so the consequence holds:



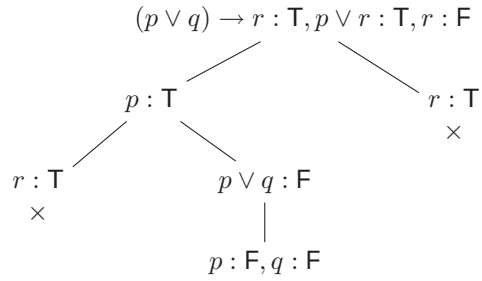
(3d) The tableau closes, so the consequence holds:



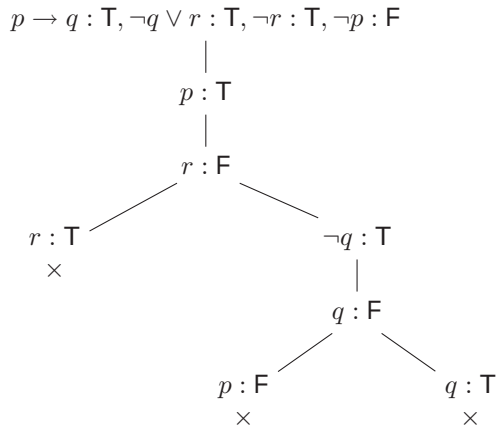
(3e) The tableau closes, so the consequence holds:



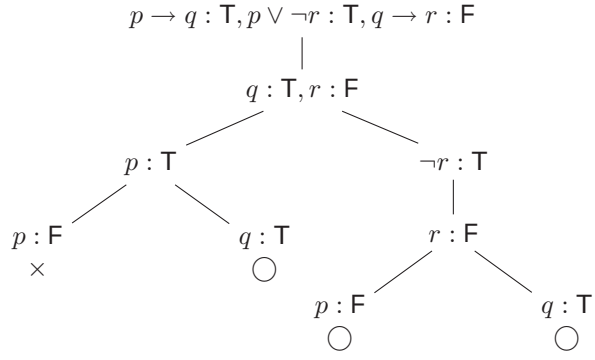
(4b) The inference rule is sound:



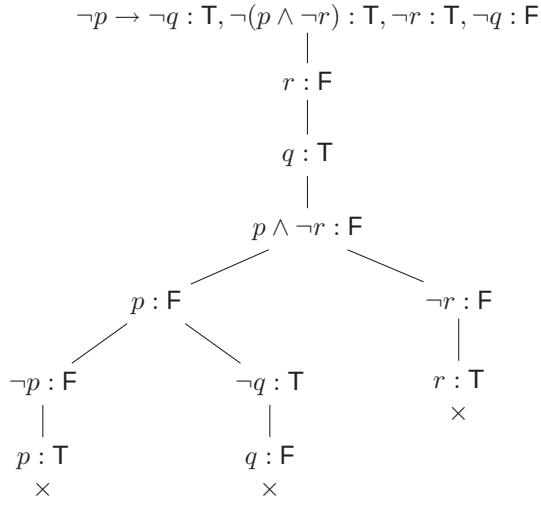
(4c) The inference rule is sound:



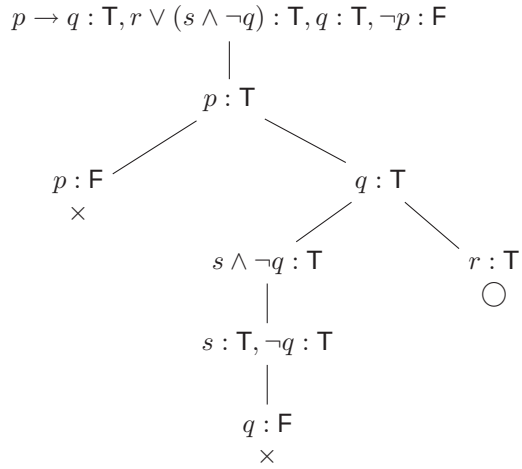
(4d) The inference rule is *not* sound:



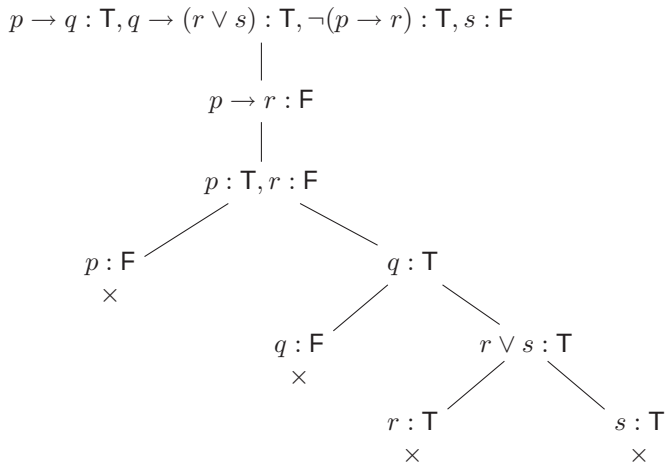
(4e) The inference rule is sound:



(4f) The inference rule is *not* sound:



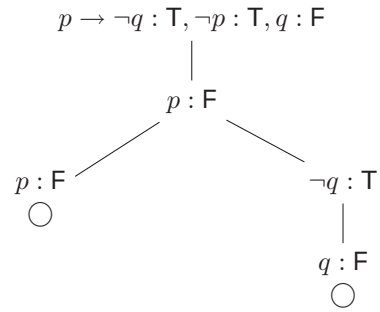
(4g) The inference rule is sound:



(5a) Denote "The triangle *ABC* has a right angle" by p and "The triangle *ABC* is equilateral" by q. Then the propositional argument can be written as

$$\frac{p \to \neg q,\ \neg p}{q}\ .$$

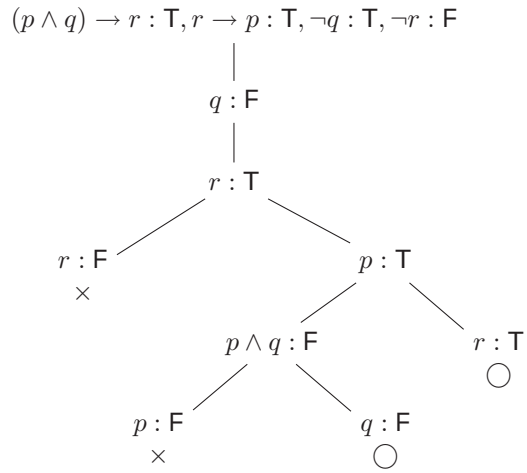
The propositional argument is *not* correct:



(5b) Denote "n is divisible by 2" by p, "n is divisible by 3" by q and "n is divisible by 6" by r. Then the propositional argument can be written as

$$\frac{(p \wedge q) \to r,\ r \to p,\ \neg q}{\neg r}.$$

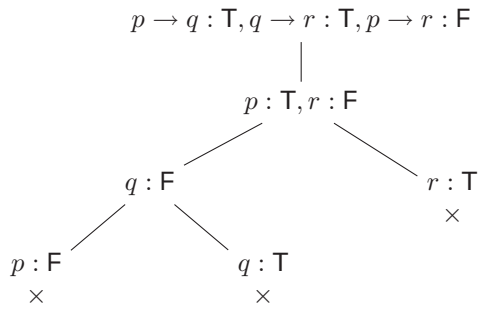
The propositional argument is *not* correct:



(5c) Denote "Bill likes logic" by p, "Bill is clever" by q and "Bill is rich" by r. Then the propositional argument can be written as

$$\frac{p \to q,\ q \to r}{p \to r}.$$

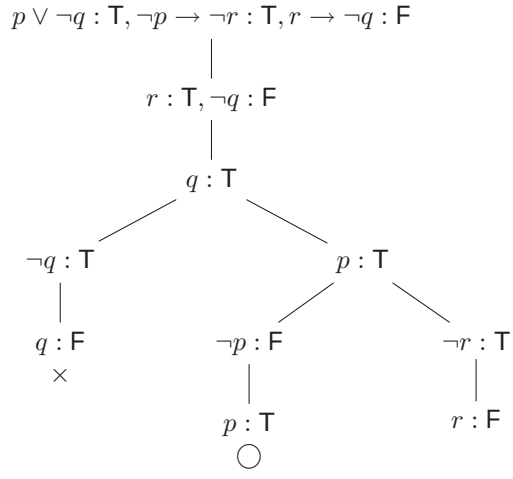
The propositional argument is correct:



(5d) Denote "Socrates is wise" by p, "Socrates is happy" by q and "Socrates is a philosopher" by r. Then the propositional argument can be written as

$$\frac{p \vee \neg q, \neg p \to \neg r}{r \to \neg q}.$$

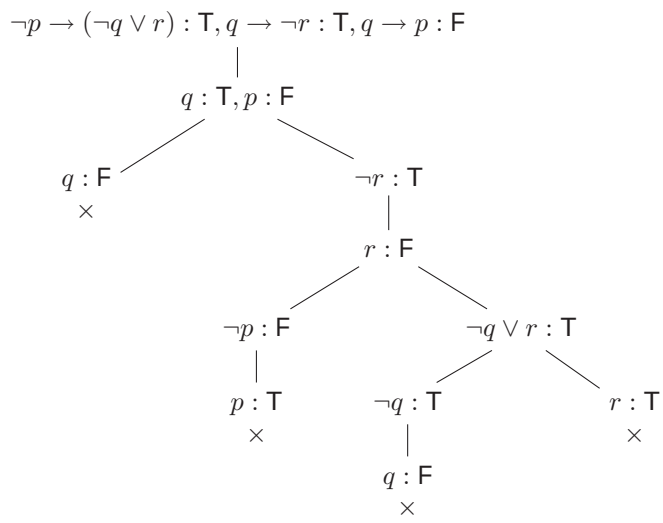
The propositional argument is *not* correct:



(5e) Denote "Christina is a good student" by p, "Christina is clever" by q and "Christina is lazy" by r. Then the propositional argument can be written as

$$\frac{\neg p \to (\neg q \vee r),\ q \to \neg r}{q \to p}.$$

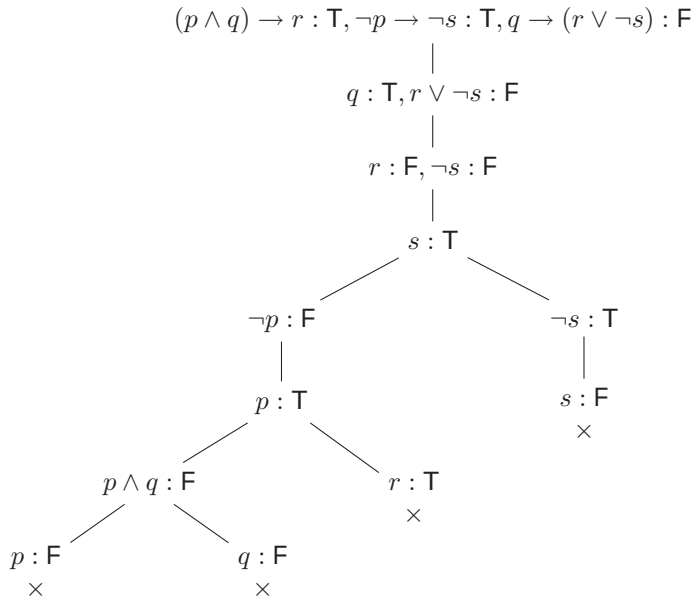
The propositional argument is correct:



(5f) Denote "Victor studies hard" by p, "Victor is clever" by q, "Victor will go to a university" by r and "Victor will get a good job" by s. Then the propositional argument can be written as

$$\frac{(p \wedge q) \to r,\ \neg p \to \neg s}{q \to (r \vee \neg s)}\,.$$

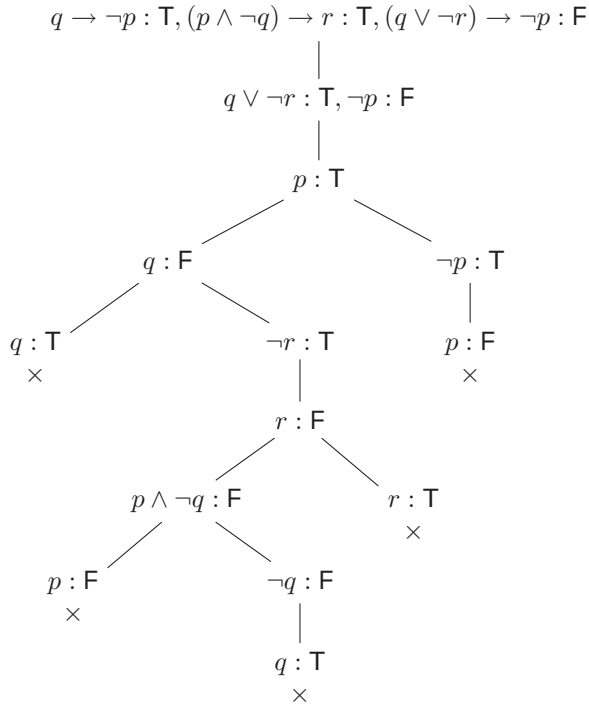
The propositional argument is correct:



(5g) Denote "Johnnie will learn logic" by p, "Johnnie skips lectures" by q and "Johnnie will pass the exam" by r. Then the propositional argument can be written as

$$\frac{q \to \neg p,\ p \wedge \neg q \to r}{q \vee \neg r \to \neg p}.$$

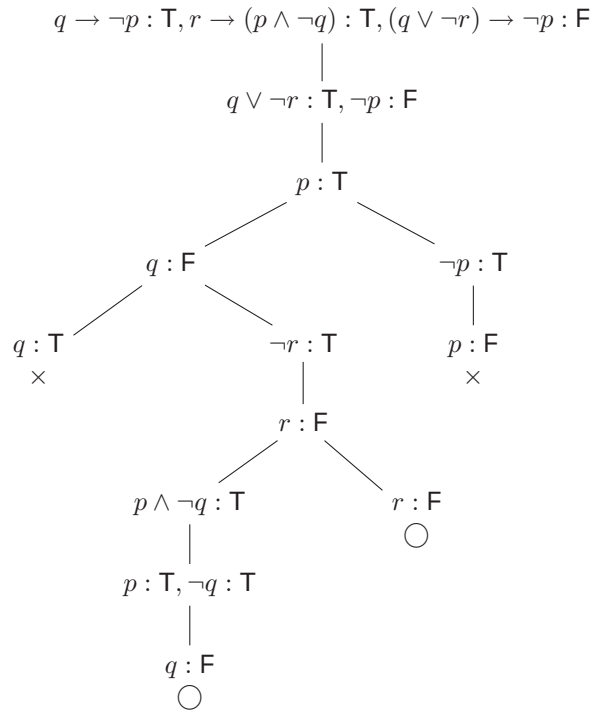
The propositional argument is correct:



(5h) Now the argument can be written as follows:

$$\frac{q \to \neg p,\ r \to p \wedge \neg q}{q \vee \neg r \to \neg p}.$$

The argument is *not* correct:



3.4. Logical equivalences. Negating propositional formulae

(1) Each pair of equivalences are verified quite similarly, so we only prove the first of them.

(1a) Suppose p and $p \wedge p$ are not equivalent. Then there are two cases:

Case 1: $p \wedge p$ ***is true, while*** p ***is false.***
But if p is false, then $p \wedge p$ is false, a contradiction.

Case 2: $p \wedge p$ ***is false, while*** p ***is true.***
But if p is true, then $p \wedge p$ is true, which is a contradiction. Hence, the formulae are equivalent.

(1b) Suppose $p \wedge q$ and $q \wedge p$ are not equivalent. Then there are two cases:

Case 1: $p \wedge q$ ***is true, while*** $q \wedge p$ ***is false.***
But if $p \wedge q$ is true, then both p and q are true, and so $q \wedge p$ is true, a contradiction.

Case 2: $p \wedge q$ ***is false, while*** $q \wedge p$ ***is true.***
But if $q \wedge p$ is true, then both p and q are true, and so $p \wedge q$ is true, a contradiction. Hence, the formulae are equivalent.

(1c) Suppose $p \wedge (q \wedge r)$ and $(p \wedge q) \wedge r$ are not equivalent. Then there are two cases:

Case 1: $p \wedge (q \wedge r)$ ***is true, while*** $(p \wedge q) \wedge r$ ***is false.***
But if $(p \wedge (q \wedge r))$ is true, then p and $q \wedge r$ are true. Hence, p, q, and r are true, and so $(p \wedge q) \wedge r$ is true, which is a contradiction.

Case 2: $p \wedge (q \wedge r)$ ***is false, while*** $(p \wedge q) \wedge r$ ***is true.***
If $(p \wedge (q \wedge r)$ is true, then p and $q \wedge r$ are true. Hence, p, q, and r are true, and so $p \wedge (q \wedge r)$ is true, a contradiction. Hence, the formulae are equivalent.

(1d) There are two cases if the formulae are not equivalent:

Case 1: $p \wedge (p \vee q)$ ***is true, while*** p ***is false.***
If $p \wedge (p \vee q)$ is true, then both p and $p \vee q$ are true, which contradicts the fact that p is false.

Case 2: $p \wedge (p \vee q)$ ***is false, while*** p ***is true.***
Then $p \vee q$ is true, and so, since p is true, $p \wedge (p \vee q)$ is also true, which is a contradiction. Hence, the formulae are equivalent.

(1e) There are two cases if the formulae are not equivalent:

Case 1: $p \wedge (q \vee r)$ ***is true, while*** $(p \wedge q) \vee (p \wedge r)$ ***is false.***
If $(p \wedge q) \vee (p \wedge r)$ is false, then $p \wedge q$ and $p \wedge r$ are false. Hence, p or q is false and p or r is false. In all the cases $p \wedge (q \vee r)$ is false, which is a contradiction.

Case 2: $p \wedge (q \vee r)$ ***is false, while*** $(p \wedge q) \vee (p \wedge r)$ ***is true.***
If $(p \wedge (q \vee r))$ is false, then p is false or $q \vee r$ is false. Hence, p is false or both q and r are false. In both cases $(p \wedge q) \vee (p \wedge r)$ is false, which is a contradiction. Hence, the formulae are equivalent.

(1f) There are two cases if the formulae are not equivalent:

Case 1: $\neg(p \wedge q)$ ***is true, while*** $(\neg p \vee \neg q)$ ***is false.***
If $(\neg p \vee \neg q)$ is false, then $\neg p$ and $\neg q$ are false. Hence, p and q are true, and so $\neg(p \wedge q)$ is false, which is a contradiction.

Case 2: $\neg(p \wedge q)$ ***is false, while*** $(\neg p \vee \neg q)$ ***is true.***
If $\neg(p \wedge q)$ is false, then $p \wedge q$ is true. Hence, p and q are true, and so $(\neg p \vee \neg q)$ is false, a contradiction. Hence, the formulae are equivalent.

(2b) The formulae are equivalent since they have the same truth tables:

p	q	r	$(p \to q)$	$\vee$	$(p \to r)$	p	$\to$	$(q \vee r)$
F	F	F	F T F	T	F T F	F	T	F F F
F	F	T	F T F	T	F T T	F	T	F T T
F	T	F	F T T	T	F T F	F	T	T T F
F	T	T	F T T	T	F T T	F	T	T T T
T	F	F	T F F	F	T F F	T	F	F F F
T	F	T	T F F	T	T T T	T	T	F T T
T	T	F	T T T	T	T F F	T	T	T T F
T	T	T	T T T	T	T T T	T	T	T T T
				↑			↑	

(2f) The formulae are equivalent since they have the same truth tables:

p	q	$\neg$	$(p \leftrightarrow q)$	$\neg p \leftrightarrow q$	$p \leftrightarrow \neg q$
F	F	F	F T F	T F F	F F T
F	T	T	F F T	T T T	F T F
T	F	T	T F F	F T F	T T T
T	T	F	T T T	F F T	T F F
		↑		↑	↑

(2h) The formulae are equivalent since they have the same truth tables:

p	q	r	p	$\leftrightarrow$	$(q \leftrightarrow r)$	$(p \leftrightarrow q)$	$\leftrightarrow$	r
F	F	F	F	F	FTF	FTF	F	F
F	F	T	F	T	FFT	FTF	T	T
F	T	F	F	T	TFF	FFT	T	F
F	T	T	F	F	TTT	FFT	F	T
T	F	F	T	T	FTF	TFF	T	F
T	F	T	T	F	FFT	TFF	F	T
T	T	F	T	F	TFF	TTT	F	F
T	T	T	T	T	TTT	TTT	T	T
				↑			↑	

(3a) The formulae are *not* equivalent since they have different truth tables.

(3b) The formulae are *not* equivalent since they have different truth tables:

p	q	$p \to q$	$\neg p \to \neg q$
F	F	FTF	TTT
F	T	FTT	TFF
T	F	TFF	FTT
T	T	TTT	FTF
		↑	↑

(3c) The formulae are equivalent since they have the same truth tables.

(3d) The formulae are equivalent since they have the same truth tables:

p	q	$\neg$	$(p \to \neg q)$	$p \wedge q$
F	F	F	FTT	FFF
F	T	F	FTF	FFT
T	F	F	TTT	TFF
T	T	T	TFF	TTT
		↑		↑

(3e) The formulae are *not* equivalent since they have different truth tables.

(3f) The formulae are *not* equivalent since they have different truth tables:

p	q	r	$(p \to r)$	$\wedge$	$(q \to r)$	$(p \wedge q)$	$\to$	r
F	F	F	FTF	T	FTF	FFF	T	F
F	F	T	FTT	T	FTT	FFF	T	T
F	T	F	FTF	F	TFF	FFT	T	F
F	T	T	FTT	T	TTT	FFT	T	T
T	F	F	TFF	F	FTF	TFF	T	F
T	F	T	TTT	T	FTT	TFF	T	T
T	T	F	TFF	F	TFF	TTT	F	F
T	T	T	TTT	T	TTT	TTT	T	T
				↑			↑	

(3g) The formulae are *not* equivalent since they have different truth tables.

(3h) The formulae are equivalent since they have the same truth tables:

p	q	r	$(p \to r)$	$\vee$	$(q \to r)$	$(p \wedge q)$	$\to$	r
F	F	F	F T F	T	F T F	F F F	T	F
F	F	T	F T T	T	F T T	F F F	T	T
F	T	F	F T F	T	T F F	F F T	T	F
F	T	T	F T T	T	T T T	F F T	T	T
T	F	F	T F F	T	F T F	T F F	T	F
T	F	T	T T T	T	F T T	T F F	T	T
T	T	F	T F F	F	T F F	T T T	F	F
T	T	T	T T T	T	T T T	T T T	T	T
				↑			↑	

(3i) The formulae are *not* equivalent since they have different truth tables.

(3j) The formulae are equivalent since they have the same truth tables:

p	q	r	p	$\leftrightarrow$	$(q \leftrightarrow r)$	q	$\leftrightarrow$	$(p \leftrightarrow r)$
F	F	F	F	F	F T F	F	F	F T F
F	F	T	F	T	F F T	F	T	F F T
F	T	F	F	T	T F F	T	T	F T F
F	T	T	F	F	T T T	T	F	F F T
T	F	F	T	T	F T F	F	T	T F F
T	F	T	T	F	F F T	F	F	T T T
T	T	F	T	F	T F F	T	F	T F F
T	T	T	T	T	T T T	T	T	T T T
				↑			↑	

(3k) The formulae are equivalent since they have the same truth tables.

(4a) $\neg((p \vee \neg q) \wedge \neg p)$
$\equiv \neg(p \vee \neg q) \vee \neg\neg p$
$\equiv (\neg p \wedge \neg\neg q) \vee p$
$\equiv (\neg p \wedge q) \vee p$

(4b) $\neg((p \to \neg q) \to p)$
$\equiv (p \to \neg q) \wedge \neg p$

(4c) $\neg(p \to (\neg q \to p))$
$\equiv p \wedge \neg(\neg q \to p)$
$\equiv p \wedge (\neg q \wedge \neg p)$

(4d) $\neg((p \leftrightarrow \neg q) \to \neg r)$
$\equiv (p \leftrightarrow \neg q) \wedge \neg\neg r$
$\equiv (p \leftrightarrow \neg q) \wedge r$

(4e) $\neg(p \to (\neg q \leftrightarrow r))$
$\equiv p \wedge \neg(\neg q \leftrightarrow r)$
$\equiv p \wedge ((\neg\neg q \wedge r) \vee (\neg q \wedge \neg r))$
$\equiv p \wedge ((q \wedge r) \vee (\neg q \wedge \neg r))$

3.5. Normal forms. Propositional resolution

(4a) First method:

$$
\begin{aligned}
&\neg(p \leftrightarrow q)\\
&\equiv \neg((p \to q) \wedge (q \to p))\\
&\equiv \neg((\neg p \vee q) \wedge (\neg q \vee p)\\
&\equiv (p \wedge \neg q) \vee (q \wedge \neg p) \textbf{ (DNF)}\\
&\equiv ((p \wedge \neg q) \vee q) \wedge ((p \wedge \neg q) \vee \neg p)\\
&\equiv (p \vee q) \wedge \top \wedge \top \wedge (\neg q \vee \neg p)\\
&\equiv (p \vee q) \wedge (\neg q \vee \neg p) \textbf{ (CNF)}
\end{aligned}
$$

Second method:

p	q	$\neg$	$(p \leftrightarrow q)$
F	F	F	F
F	T	T	F
T	F	T	F
T	T	F	T

DNF: $(\neg p \wedge q) \vee (p \wedge \neg q)$
CNF: $(\neg p \vee \neg q) \wedge (p \vee q)$

(4b) First method:

$$
\begin{aligned}
&((p \to q) \wedge \neg q) \to p\\
&\equiv ((\neg p \vee q) \wedge \neg q) \to p\\
&\equiv \neg((\neg p \vee q) \wedge \neg q) \vee p\\
&\equiv (p \wedge \neg q) \vee q \vee p \textbf{ (DNF)}\\
&\equiv (p \wedge \neg q) \vee (p \vee q)\\
&\equiv (p \vee (p \vee q)) \wedge (\neg q \vee (p \vee q))\\
&\equiv (p \vee q) \wedge \top\\
&\equiv p \vee q \textbf{ (CNF)}
\end{aligned}
$$

Second method:

p	q	$((p \to q)$	$\wedge$	$\neg q)$	$\to$	p
F	F	F T F	T	T	F	F
F	T	F T T	F	F	T	F
T	F	T F F	T	T	T	T
T	T	T T T	F	F	T	T

DNF: $(\neg p \wedge q) \vee (p \wedge \neg q) \vee (p \wedge q)$
CNF: $p \vee q$

(4d) First method:

$$
\begin{aligned}
& p \to (\neg q \leftrightarrow r) \\
& \equiv \neg p \vee ((\neg q \to r) \wedge (r \to \neg q)) \\
& \equiv \neg p \vee ((q \vee r) \wedge (\neg r \vee \neg q)) \ (*) \\
& \equiv \neg p \vee (q \wedge (\neg r \vee \neg q)) \vee (r \wedge (\neg r \vee \neg q)) \\
& \equiv \neg p \vee (q \wedge \neg r) \vee (q \wedge \neg q) \vee (r \wedge \neg r) \vee (r \wedge \neg q) \\
& \equiv \neg p \vee (q \wedge \neg r) \vee (r \wedge \neg q) \ \textbf{(DNF)} \\
& \equiv (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r) \ \textbf{CNF} \text{ (from } *)
\end{aligned}
$$

Second method:

p	q	r	p	$\to$	$(\neg q$	$\leftrightarrow$	$r)$
F	F	F	F	T	T	F	F
F	F	T	F	T	T	T	T
F	T	F	F	T	F	T	F
F	T	T	F	T	F	F	T
T	F	F	T	F	T	F	F
T	F	T	T	T	T	T	T
T	T	F	T	T	F	T	F
T	T	T	T	F	F	F	T

DNF: $(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r)$
CNF: $(\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$

(4e) First method:

$$
\begin{aligned}
& (\neg p \wedge (\neg q \leftrightarrow p)) \to ((q \wedge \neg p) \vee p) \\
& \equiv \neg(\neg p \wedge (\neg q \leftrightarrow p)) \vee (q \wedge \neg p) \vee p \\
& \equiv p \vee \neg((\neg q \to p) \wedge (p \to \neg q)) \vee (q \wedge \neg p) \vee p \\
& \equiv p \vee \neg((q \vee p) \wedge (\neg p \vee \neg q)) \vee (q \wedge \neg p) \\
& \equiv p \vee (\neg q \wedge \neg p) \vee (p \wedge q) \vee (q \wedge \neg p) \ \textbf{(DNF)} \\
& \equiv ((p \vee \neg q) \wedge (p \vee \neg p)) \vee ((p \vee q) \wedge (p \vee \neg p) \wedge (q \vee q) \wedge (q \vee \neg p)) \\
& \equiv (p \vee \neg q) \vee ((p \vee q) \wedge q \wedge (q \vee \neg p)) \\
& \equiv (p \vee \neg q \vee p \vee q) \wedge (p \vee \neg q \vee q) \wedge (p \vee \neg q \vee q \vee \neg p) \\
& \equiv \neg q \vee q \ \textbf{(CNF)}
\end{aligned}
$$

Second method:

p	q	$(\neg p$	$\wedge$	$(\neg q \leftrightarrow p))$	$\to$	$((q \wedge \neg p) \vee p)$				
F	F	T	F	T F F	T	F	F	T	F	F
F	T	T	T	F T F	T	T	T	T	T	F
T	F	F	F	T T T	T	F	F	F	T	T
T	T	F	T	F F T	T	T	F	F	T	T

DNF: $(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge \neg q) \vee (p \wedge q)$
CNF: $p \vee \neg p$

(5a) First, we transform $\neg(((p \to q) \to q) \to q)$ to clausal form:

$$C_1 = \{p, q\} \text{ and } C_2 = \{\neg q\}.$$

Applying resolution, we get $C_3 = Res(C_1, C_2) = \{p\}$. No more clauses are derivable. Therefore, the empty clause cannot be derived, so the formula is *not* a tautology.

(5b) Transform $\neg(((q \to p) \to q) \to q)$ clausal form:

$$C_1 = \{q\}, C_2 = \{\neg p, q\} \text{ and } C_3 = \{\neg q\}.$$

Applying resolution, we get $C_4 = Res(C_1, C_3) = \{\}$. The empty clause has been derived; therefore the formula is a tautology.

(5c) Transform $\neg(((p \to q) \wedge (p \to \neg q)) \to \neg p)$ to clausal form:

$$C_1 = \{\neg p, q\}, C_2 = \{\neg p, \neg q\} \text{ and } C_3 = \{p\}.$$

Finally, applying resolution successively, we get

$$C_4 = Res(C_1, C_2) = \{\neg p\},$$
$$C_5 = Res(C_3, C_4) = \{\}.$$

The empty clause has been derived, therefore the formula is a tautology.

(5d) Transform $\neg(((p \vee q) \to \neg r) \to \neg(\neg q \wedge r))$ to clausal form:

$$C_1 = \{\neg p, \neg r\}, C_2 = \{\neg q, \neg r\}, C_3 = \{\neg q\} \text{ and } C_4 = \{r\}.$$

Applying resolution, we get $C_5 = Res(C_1, C_4) = \{\neg p\}$. No more new clauses are derivable. The empty clause cannot be derived, so the formula is *not* a tautology.

(5e) Transform $\neg(((p \to q) \wedge (p \to r)) \to (p \to (q \wedge r)))$ to clausal form:

$$C_1 = \{\neg p, q\},\ C_2 = \{\neg p, r\},\ C_3 = \{p\} \text{ and } C_4 = \{\neg q, \neg r\}.$$

Finally, applying resolution successively, we get

$$C_5 = Res(C_2, C_4) = \{\neg p, \neg q\},$$
$$C_6 = Res(C_1, C_5) = \{\neg p\},$$
$$C_7 = Res(C_3, C_6) = \{\}.$$

The empty clause has been derived; therefore the formula is a tautology.

(5f) First, transform $\neg(((p \to r) \wedge (q \to r)) \to ((p \wedge q) \to r))$ to clausal form:

$$C_1 = \{\neg p, r\},\ C_2 = \{\neg q, r\},\ C_3 = \{p\},\ C_4 = \{q\} \text{ and } C_5 = \{\neg r\}.$$

Finally, applying resolution successively, we get

$$C_6 = Res(C_1, C_3) = \{r\},$$
$$C_7 = Res(C_5, C_6) = \{\}.$$

The empty clause has been derived; hence the formula is a tautology.

(5g) First, transform $\neg(((p \to r) \vee (q \to r)) \to ((p \vee q) \to r))$ to clausal form:

$$C_1 = \{\neg p, r, \neg q\},\ C_2 = \{\neg r\} \text{ and } C_3 = \{p, q\}.$$

Finally, applying resolution successively, we get

$$C_4 = Res(C_1, C_2) = \{\neg p, \neg q\},$$
$$C_5 = Res_1(C_3, C_4) = \{p, \neg p\},$$
$$C_6 = Res_2(C_3, C_4) = \{q, \neg q\}.$$

No more clauses are derivable. Therefore, the empty clause cannot be derived, so the formula is *not* a tautology.

(5h) Transform $\neg(((p \to r) \wedge (q \to r)) \to ((p \vee q) \to r))$ to clausal form:

$$C_1 = \{\neg p, r\},\ C_2 = \{\neg q, r\},\ C_3 = \{p, q\} \text{ and } C_4 = \{\neg r\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_1, C_3) = \{q, r\}, \\ C_6 &= Res(C_2, C_5) = \{r\}, \\ C_7 &= Res(C_4, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the formula is a tautology.

(5i) First, transform $\neg(p \to ((q \to r) \to ((p \to q) \to r)))$ to clausal form:

$$C_1 = \{p\},\ C_2 = \{\neg q, r\},\ C_3 = \{\neg p, q\} \text{ and } C_4 = \{\neg r\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_1, C_3) = \{q\}, \\ C_6 &= Res(C_2, C_4) = \{\neg q\}, \\ C_7 &= Res(C_5, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the formula is a tautology.

(5j) First, transform $\neg((p \to (q \to r)) \to ((p \to q) \to (p \to r)))$ to clausal form:

$$C_1 = \{\neg p, \neg q, r\},\ C_2 = \{\neg p, q\},\ C_3 = \{p\} \text{ and } C_4 = \{\neg r\}.$$

Finally, applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_1, C_2) = \{\neg p, r\}, \\ C_6 &= Res(C_3, C_5) = \{r\}, \\ C_7 &= Res(C_4, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the formula is a tautology.

(6a) Transform the formulae to clausal form:

$$C_1 = \{p, q\},\ C_2 = \{p, \neg q\} \text{ and } C_3 = \{\neg p\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_4 &= Res(C_1, C_2) = \{p\}, \\ C_5 &= Res(C_3, C_4) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

(6b) Transform the formulae to clausal form:

$$C_1 = \{\neg p, r\},\ C_2 = \{\neg q, r\},\ C_3 = \{p, q\} \text{ and } C_4 = \{\neg r\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_2, C_3) = \{p, r\}, \\ C_6 &= Res(C_1, C_5) = \{r\}, \\ C_7 &= Res(C_4, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

(6c) First, transform the formulae to clausal form:

$$C_1 = \{\neg p, \neg q, r\},\ C_2 = \{q\},\ C_3 = \{p\} \text{ and } C_4 = \{\neg r\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_1, C_4) = \{\neg p, \neg q\}, \\ C_6 &= Res(C_2, C_5) = \{\neg p\}, \\ C_7 &= Res(C_3, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

(6d) Transform the formulae to clausal form:

$$C_1 = \{\neg p, q\},\ C_2 = \{p, \neg r\},\ C_3 = \{\neg r\} \text{ and } C_4 = \{q\}.$$

Finally, applying resolution, we get

$$C_5 = Res(C_1, C_2) = \{q, \neg r\}.$$

No more clauses are derivable. The empty clause cannot be derived, so the consequence does not hold.

(6e) Transform the formulae to clausal form:

$$C_1 = \{\neg p, r\},\ C_2 = \{\neg q, r\},\ C_3 = \{p, q\} \text{ and } C_4 = \{\neg r\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_2, C_3) = \{p, r\}, \\ C_6 &= Res(C_1, C_5) = \{r\}, \\ C_7 &= Res(C_4, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

(6f) Transform the formulae to clausal form:

$$C_1 = \{p, \neg q, \neg r\},\ C_2 = \{r\},\ C_3 = \{\neg p\} \text{ and } C_4 = \{q\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_5 &= Res(C_1, C_2) = \{p, \neg q\}, \\ C_6 &= Res(C_3, C_5) = \{\neg q\}, \\ C_7 &= Res(C_4, C_6) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

(6g) Transform the formulae to clausal form:

$$C_1 = \{\neg p, q\},\ C_2 = \{r, s\},\ C_3 = \{\neg q, r\},\ C_4 = \{\neg r\} \text{ and } C_5 = \{p\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_6 &= Res(C_1, C_5) = \{q\}, \\ C_7 &= Res(C_3, C_4) = \{\neg q\}, \\ C_8 &= Res(C_6, C_7) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

(6h) Transform the formulae to clausal form:

$$C_1 = \{\neg p, q\},\ C_2 = \{\neg q, r, s\},\ C_3 = \{p\},\ C_4 = \{\neg r\} \text{ and } C_5 = \{\neg s\}.$$

Applying resolution successively, we get

$$\begin{aligned} C_6 &= Res(C_1, C_3) = \{q\}, \\ C_7 &= Res(C_2, C_6) = \{r, s\}, \\ C_8 &= Res(C_4, C_7) = \{s\}, \\ C_9 &= Res(C_5, C_8) = \{\}. \end{aligned}$$

The empty clause has been derived, so the consequence holds.

4

First-Order Logic

4.1. Basic concepts of first-order logic

(1) We can view any graph as the structure $\mathcal{G} = (V, R)$ in the language with one binary relational symbol $\{E\}$. The domain of $\mathcal{G}$ is the set of vertices V, and E is interpreted as the edge relation R.
We can view any group as the structure for the language $\mathcal{L}_G$ with nonlogical symbols $\{\cdot, ', e\}$, where $\cdot$ is a binary functional symbol (multiplication), $'$ is a unary functional symbol (the inverse operation) and e is a constant symbol. The domain of $\mathcal{G}$ is the set of group elements and the interpretations of $\cdot$, $'$, e satisfy the defining axioms of a group. We can likewise view any ring as a structure for the language $\mathcal{L}_R$ with nonlogical symbols $\{\cdot, +, 0\}$, where $\cdot$ and $+$ are both binary functional symbols (multiplication and addition) and 0 is a constant symbol, such that their interpretations in the set of ring elements satisfy the defining axioms of a ring.
A vector space over a field of scalars S can be formalized as a first-order structure for the language $\mathcal{L}_V$ with nonlogical symbols $\{+, \mathbf{0}\} \cup \{c_s \mid s \in S\}$, where $+$ is a binary functional symbol (vector addition), $\mathbf{0}$ is a constant symbol and each c_s, where $s \in S$, is a unary functional symbol (multiplication by the scalar s). The domain of a vector space is a set of vectors V and the interpretations of $+$, $\{c_s \mid s \in S\}$, $\mathbf{0}$ in V satisfy the defining axioms of a vector space.

(3a) Yes, $x \times y$.

(3b) No, $\times$ is a binary function, not ternary.

(3c) No, should be written $+(x, y)$ or $x + y$.

(3d) No, there is a missing right parenthesis.

(3e) Yes, $(x \times (\mathbf{3} + y)) + ((\mathbf{3} + y) \times x)$.

(3f) No, s is a unary function, not a binary one.

(3g) No, the second occurrence of s does not have an argument.

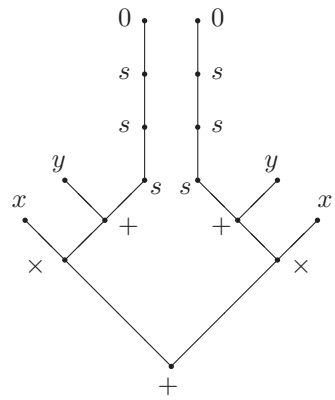
(3h) Yes, $s((\mathbf{2} \times x) \times (\mathbf{3} + y))$.

(3i) Yes, $s(\mathbf{2} \times x) \times s(s(\mathbf{3}) + y)$.

(3j) No, the first occurrence of s has 2 arguments.

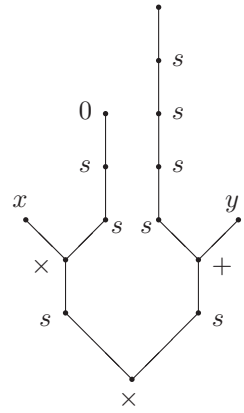
Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

(4e) The parsing tree of $+(\times(x, +(\mathbf{3}, y)), \times(+(\mathbf{3}, y), x))$ looks as follows:



The set of subterms is $\{x, y, \mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, +(\mathbf{3}, y), \times(x, +(\mathbf{3}, y)), \times(+(\mathbf{3}, y), x), +(\times(x, +(\mathbf{3}, y)), \times(+(\mathbf{3}, y), x))\}$.

(4i) The parsing tree of $\times(s(\times(\mathbf{2}, x)), s(+(s(\mathbf{3}), y)))$ looks as follows:



The set of subterms is $\{x, y, \mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, s(\mathbf{3}), \times(\mathbf{2}, x), s(\times(\mathbf{2}, x)), +(s(\mathbf{3}), y), s(+(s(\mathbf{3}), y)), \times(s(\times(\mathbf{2}, x)), s(+(s(\mathbf{3}), y)))\}$.

(6a) Yes

(6b) No, x is a variable, not a formula.

(6c) Yes

(6d) No, $=$ is not a formula, but a predicate symbol.

(6e) No, $\mathbf{0}$ is not a formula, but a constant.

(6f) Yes

(6g) No, $\mathbf{0.5}$ does not belong to the language.

(6h) No, x is a variable, not a formula.

(6i) No, $x + y$ and $y + x$ are terms, not formulae.

(6j) Yes

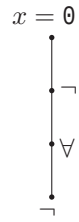
(6k) No, $x + \mathbf{0}$ is a term, not a formula.

(6l) Yes (though, formally, $x < \mathbf{0}$ should be in parentheses)

(6m) Yes

(6n) No, there is no connective between $y < y$ and $\neg\forall x(x < x)$.

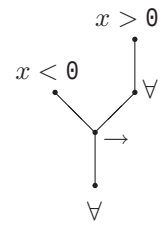
(7f) The parsing tree of $\neg\forall x(\neg x = \mathbf{0})$ looks as follows:



The main connective is $\neg$ and the set of subformulae is

$$\{x = \mathbf{0}, \neg(x = \mathbf{0}), \forall x(\neg x = \mathbf{0}), \neg\forall x(\neg x = \mathbf{0})\}.$$

(7j) The parsing tree of $\forall x((x < \mathbf{0}) \to \forall x(x > \mathbf{0}))$ looks as follows:



The main connective is $\forall$ and the set of subformulae is

$$\{x < \mathbf{0}, x > \mathbf{0}, \forall x(x > \mathbf{0}), x < \mathbf{0} \to \forall x(x > \mathbf{0}), \forall x(x < \mathbf{0} \to \forall x(x > \mathbf{0}))\}.$$

(10a) $\times(x, s(s(\mathbf{2})))$ equals 12, while $\times(s(s(x)), \mathbf{2})$ equals 10, so the formula is false.

(10b) The terms $+(\mathbf{5}, \times(x, +(\mathbf{3}, y)))$ and $s(\times(\mathbf{3}, \times(\mathbf{2}, x)))$ have values 4 and 4, respectively. Consequently, the formula is false.

(10c) The formula is false for each of these values of x, as the values of terms on the left and on the right are always equal, due to the algebraic identity $x^3 + 1 = (x + 1)(x^2 - x + 1)$.

(11a) $(\neg\neg(f(x) = y) \to (\exists x(x > y) \vee \neg(\neg(f(x) = y) \wedge \exists x(x > y))))$

(11b) $(\neg\neg(x = y) \to (\neg(x = y) \vee \neg(\neg(x = y) \wedge \neg(x = y))))$

(12) No, because $(x = y)$ is substituted for the first occurrence of p and $(y = x)$ is substituted for the second occurrence of p.

(13a) False
(13b) True
(13c) True
(13d) True
(13e) False
(13f) True
(13g) True
(13h) True
(13i) True
(13j) True
(13k) True
(13l) True
(13m) True
(13n) True
(13o) True
(13p) True
(13q) True

(14a) Every woman is the mother of all her children. True.

(14b) Everybody who is a father is not a mother. True.

(14c) There is no man that does not know any of his children. False.

(14d) Everybody has a parent-in-law. False.

(14e) Every mother likes all children. False.

(14f) There is a woman that does not like any men that like her. True (most probably).

(14g) There is no child that likes some mother that does not like her child. False (most probably).

(15a) There is a real number which, when added to any real number, produces that number. True, take $x = 0$.

(15b) There is a real number which, when added to any real number, produces a number greater than that number. True, take $x = 1$.

(15c) There is a real number which, when added to any real number, produces a sum greater than it. False, take $y = 0$.

(15d) For every real number x, there is another real number y, such that the sum of x and y is the same as the difference between x and y. True, take $y = 0$.

(15e) For every real number x, there is another real number y, such that their sum is greater than y. False, take $x = 0$.

(15f) For every real number x, there is another real number y, such that their sum is greater than x. True, take $x = 1$.

(15g) There is a real number which, when multiplied by any real number, produces that number. True, take $x = 1$.

(15h) There is a real number which, when multiplied by any real number, produces a number greater than that number. False. (Hint: if $x > 0$ is chosen, take $y < 0$ and vice versa.)

(15i) For every real number x, there is another real number y, such that the product of x and y is greater than y. False, take $x = 0$.

(15j) For every real number x, there is another real number y, such that the product of x and y is greater than x. False, take $x = 0$.

(15k) Every square of an integer is positive. False, take $x = 0$.

(15l) Not every real number is greater than some integer. False.

(15m) For every integer there is a greater integer. True.

(15n) There is a integer that is not less than some real number. True.

(15o) There is no real number greater than all integers. True.

(15p) Between any two different real numbers, there is another real number. True.

(15q) Between any two different real numbers, there is an integer. False, take $x = 0$ and $y = 1$.

4.2. The formal semantics of first-order logic

(1a) False

(1b) False

(1c) True

(1d) True

(1e) True

(1f) True

(1g) True

(1h) True

(1i) True

(2a) Not every real number is different from 0. True.

(2b) Every real number is less than or equal to its cube. False, take $x = -2$.

(2c) Every real number equal to its square is positive. False, take $x = 0$.

(2d) There is a negative real number equal to its square. False, the square of any real number is always non-negative.

(2e) There exists a real number which, if equal to its square, is negative. True, take any x such that $x \neq x^2$; then the antecedent is false, so the implication is true.

(2f) Any positive real number is less than its square. False, take $x = 1$.

(2g) Every real number is either zero or it is not equal to twice itself. True.

(2h) The square of any real number greater than 1 and equal to its square is less than 1. True, because the antecedent is always false.

(2i) For every pair of real numbers, one of them is less than the other. False, take $x = y$.

(2j) Every real number is greater than the square of some real number. False, take $x = -1$.

(2k) For every real number, there is a real number that is either positive or whose square is less than that number. True.

(2l) Every non-negative number is the square of a positive number. False, take $x = 0$.

(2m) For every real number x there is some real number y such that x is greater than the square of y if x is greater than y. True, given x, take $y = x$.

(2n) Every real number x is greater than the square of some real number y if x is different from y. True, take $y = x$.

(2o) There is real number greater than all real numbers. False.

(2p) There is a real number such that adding any real number to it does not change it. False.

(2q) There is a real number x which added to any real number does not change it. True, take $x = 0$.

(2r) There is a number such that every number is either less than it or less than its additive inverse. False.

(2s) There is a number x that is greater than or not greater than any given number y. True.

(2t) There is a number such that the square of every number greater than it is also greater than it. True, take, for example, $x = 1$.

(2u) There is a number such that the square of every number less than it is also less than it. False.

(2v) There exist two real numbers whose sum is equal to their product. True, take $x = y = 0$.

(2w) For any real number, there is some real number such that their product is the same as the product of this number and any real number. True, given x, take $y = 0$.

(2x) There is a real number such that adding any number to it yields a number that has a multiplicative inverse. False, given x, take $y = -x$.

(2y) Between any two distinct real numbers, there is another real number. True.

(2z) Any real number is greater than some real number greater than every real number. True, given x, take $z = x$.

4.3. The language of first-order logic: a deeper look

(1a) $\forall x(\mathsf{I}(x) \rightarrow x^2 > \mathbf{0})$

(1b) $\forall x(\neg\mathsf{I}(x) \rightarrow x^2 > \mathbf{0})$

(1c) $\exists x\neg\mathsf{I}(x)$

(1d) $\forall x(\mathsf{I}(x) \to \exists y(\mathsf{I}(y) \wedge (x = y + y \vee x = y + y + 1)))$

(1e) $\neg\exists x(\mathsf{I}(x) \wedge \exists y(\mathsf{I}(y) \wedge x = y + y) \wedge \exists y(\mathsf{I}(y) \wedge x = y + y + 1))$

(1f) $\forall x(\mathsf{I}(x) \to \exists y(\mathsf{I}(y) \wedge x < y))$

(1g) $\forall x((\mathsf{I}(x) \wedge x > \mathbf{0}) \to \exists y(y < \mathbf{0} \wedge x = y^2))$

(1h) $\neg\forall x\exists y(\mathsf{I}(y) \wedge x > y)$

(1i) $\exists x(\mathsf{I}(x) \wedge \neg\forall y(x < y))$

(1j) $\neg\exists x\forall y(\mathsf{I}(y) \to x > y)$

(1k) $\forall x(\neg x = \mathbf{0} \to \exists y(x \times y = \mathbf{1}))$

(1l) $\exists x\forall y(xy = y)$

(1m) $\forall x\forall y(x < y \to \exists z(\mathsf{I}(z) \wedge x < z \wedge z < y))$

(2a) $\forall x\mathsf{T}(x) \vee \forall x\mathsf{L}(x)$

(2b) $\forall x(\mathsf{T}(x) \vee \mathsf{L}(x))$

(2c) $T(\mathsf{John}) \to \forall x\mathsf{L}(x)$

(2d) $\exists x\mathsf{T}(x) \to \forall y\mathsf{L}(y)$

(2e) $\forall x(\mathsf{T}(x) \to \forall y(\neg y = x \to \mathsf{L}(y)))$

(2f) $\forall x\mathsf{T}(x) \to \neg\exists y\mathsf{L}(y)$

(3a) $\exists x(\mathsf{M}(x) \wedge \forall y(\mathsf{W}(y) \to \mathsf{L}(x, y)))$

(3b) $\forall x(\mathsf{W}(x) \to \forall y((\mathsf{M}(y) \wedge \mathsf{L}(y, x)) \to \mathsf{L}(x, y)))$

(3c) $\forall x(\mathsf{M}(x) \to \exists y(\mathsf{W}(y) \wedge \mathsf{L}(x, y) \wedge \neg\mathsf{L}(y, x)))$

(3d) $\exists x(\mathsf{W}(x) \wedge \neg\exists y(\mathsf{M}(y) \wedge \mathsf{L}(x, y) \wedge \mathsf{L}(y, x)))$

(3e) $\exists x(\mathsf{M}(x) \wedge \forall y(\mathsf{W}(y) \to (\mathsf{L}(x, y) \to \neg\mathsf{L}(y, x))))$

(3f) $\neg\exists x(\mathsf{W}(x) \wedge \exists y(\mathsf{M}(y) \wedge \mathsf{L}(x, y) \wedge \forall z(\mathsf{W}(z) \to \mathsf{L}(y, z))))$

(3g) $\forall x(\mathsf{W}(x) \to \forall y(\mathsf{C}(y, x) \to \mathsf{L}(x, y)))$

(3h) $\forall x\exists y(\mathsf{C}(x, y) \wedge y = \mathsf{m}(x) \to \mathsf{L}(x, y))$

(3i) $\forall x\exists y\exists z(\mathsf{C}(y, z) \wedge \mathsf{L}(x, y))$

(3j) $\forall x(\exists y(x = \mathsf{m}(y)) \to \forall z\exists v(\mathsf{C}(z, v) \to \mathsf{L}(x, z)))$

(3k) $\forall x(\exists y\mathsf{C}(x, y) \to \exists z\mathsf{L}(z, x))$

(3l) $\exists x(\mathsf{W}(x) \wedge \forall y\exists z(\mathsf{C}(y, z) \to \mathsf{L}(x, y)))$

(4a) $\lambda_n = \exists x_1 \cdots \exists x_n(\wedge_{1 \le i \ne j \le n} \neg x_i = x_j)$

(4b) $\mu_n = \forall x_1 \cdots \forall x_{n+1}(\vee_{1 \le i \ne j \le n+1} x_i = x_j)$

(4c) $\sigma_n = \lambda_n \wedge \mu_n$

(5) $\forall x\exists y(R(x, y) \wedge \forall z(R(x, z) \to y = z))$

(6a) x is bound by $\exists$, the second occurrence of y is bound by the second occurrence of $\forall$ and the first and second occurrences of z are bound by the first occurrence of $\forall$. The first occurrence of y is free.
The scope of $\exists$ is the whole formula, the scope of the first occurrence of $\forall$ is $\forall z(Q(z, y) \vee \neg\forall y(Q(y, z) \to P(x)))$ and the scope of the second occurrence of $\forall$ is $\forall y(Q(y, z) \to P(x))$.

(6e) The first occurrence of x is bound by $\exists$, the second occurrence of x is free, y is free, the first occurrence of z is bound by the first occurrence of $\forall$ and the second occurrence of z is free.

The scope of $\exists$ is $\exists x \forall z(Q(z,y) \vee \neg \forall y(Q(x,z))$, the scope of the first occurrence of $\forall$ is $\forall z(Q(z,y) \vee \neg \forall y(Q(x,z))$ and the scope of the second occurrence of $\forall$ is $\forall y Q(x,z)$.

(6i) The first and second occurrences of x are bound by $\exists$, the second occurrence of x is bound by the second occurrence of $\forall$, the third occurrence of x is free, y is bound by the first occurrence of $\forall$ and z is free.
The scope of $\exists$ is $\exists x(\forall y(Q(x,y) \vee \neg \forall x Q(x,z)))$, the scope of the first occurrence of $\forall$ is $\forall y(Q(x,y) \vee \neg \forall x Q(x,z))$ and the scope of the second occurrence of $\forall$ is $\forall x Q(x,z)$.

(7a) $\exists x \forall z(Q(z,y) \vee \neg \forall w(Q(w,z) \rightarrow P(x)))$

(7b) $\exists x \forall z(Q(z,y) \vee \neg \forall w(Q(z,z) \rightarrow P(x)))$

(7c) $\exists x(\forall z Q(z,y) \vee \neg \forall w(Q(y,w) \rightarrow P(x)))$

(7d) $\exists u(\forall w Q(w,y) \vee \neg \forall v Q(v,z)) \rightarrow P(x)$

(7e) $\exists u \forall z(Q(z,y) \vee \neg \forall w Q(u,z)) \rightarrow P(x)$

(7f) $\exists u \forall z Q(z,y) \vee \neg(\forall w Q(w,x) \rightarrow P(x))$

(7g) $\exists x(\forall z Q(z,y) \vee \neg(\forall w Q(y,w) \rightarrow P(x)))$

(7h) $\exists x(\forall w(Q(w,y) \vee \neg \forall z(Q(y,z) \rightarrow P(x))))$

(7i) $\exists u(\forall y(Q(u,y) \vee \neg \forall v Q(v,z))) \rightarrow P(x)$

(8a) $f(x)$ is not free for substitution for z.

(8b) $f(z)$ is not free for substitution for y.

(8c) $\exists x(\forall z P(f(y)) \vee \neg \forall y(Q(y,z) \rightarrow P(x)))$

(8d) $\forall x((\neg \forall y Q(x,y) \vee P(f(y)) \rightarrow \forall y \neg \exists z \exists x Q(z,y))$

(8e) $g(x, f(z))$ is not free for substitution for z.

(8f) $\forall y(\neg(\forall x \exists z(\neg P(z) \wedge \exists y Q(z,x))) \wedge \neg \forall x Q(x,y) \vee P(f(x)))$

(8g) $f(y)$ is not free for substitution for z.

(8h) $(\forall y \exists z \neg P(z) \wedge \forall x Q(g(f(z),y),x)) \rightarrow (\neg \exists y Q(x,y) \vee P(g(f(z),y)))$

(8i) $g(f(z),y)$ is not free for substitution for x.

(9a) $P(x) := \exists y \exists z(y \times z = x \rightarrow (y = s(0) \wedge z = x) \vee (y = x \wedge z = s(0)))$

(9b) $\forall x \exists y(x < y \wedge P(y))$

(9c) $\forall x(\mathbf{2} < x \wedge \exists y(\mathbf{2} \times y = x) \rightarrow \exists z \exists v(P(z) \wedge P(v) \wedge z + v = x))$

(9d) $\forall x \exists y \exists z(P(y) \wedge P(z) \wedge x < y \wedge z = y + \mathbf{2})$

(9e) $\forall x \exists y(P(y) \wedge \neg(y \times y > x) \wedge \exists u(u \times y = x))$

(9f) $\neg \exists z(P(z) \wedge \exists u(z \times u = x) \wedge \exists v(z \times v = y))$

4.4. Truth, logical validity, equivalence and consequence in first-order logic

(1) All sentences not mentioned below are valid.

(1b) Invalid, consider the structure $\mathcal{H}$ with P taken as the predicate M.

(1e) Invalid, consider the structure $\mathcal{H}$ with P taken as the predicate W.

(1j) Invalid, consider the structure $\mathcal{H}$ with P taken as the predicate M.

(1k) Invalid, consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(1m) Invalid, consider the structure $\mathcal{N}$ with Q taken as the predicate $<$. If $x = 0$, the antecedent is true, while the consequent is false.

(1o) Invalid, consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(2) All equivalences follow from the fact that, due to Proposition 4.3.2, if x does not occur free in Q, then $S, v \vDash Q$ iff $S, v' \vDash Q$ for every x-variant v' of v iff $S, v \vDash \forall x Q$.

(3a) The equivalence holds.

(3b) The equivalence does not hold. Consider the structure $\mathcal{H}$ with P and Q taken respectively as the predicates M and W.

(3c) The equivalence does not hold. Consider the structure $\mathcal{H}$ with P and Q taken respectively as the predicates M and W. Then the left-hand side is false while the right-hand side is true.

(3d) The equivalence does not hold. Consider the structure $\mathcal{H}$ with P and Q taken respectively as the predicates M and W.

(3e) The equivalence holds.

(3f) The equivalence does not hold. Consider the structure $\mathcal{N}$ with $P(x)$ interpreted as "x is prime" and $Q(x)$ to mean "$x < x$".

(3g) The equivalence does not hold. Consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(3h) The equivalence does not hold. Consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(3i) The equivalence does not hold. Consider the structure $\mathcal{Z}$ with $Q(x, y)$ taken to mean "$x \leq y$".

(3j) The equivalence holds.

(3k) The equivalence holds since the implication on the right-hand side is equivalent to the contrapositive of the implication on the left-hand side.

(4b) $\neg\forall x((x = x^2 \wedge x > \mathbf{1}) \rightarrow x^2 < \mathbf{1})$
$\equiv \neg\forall x(\neg(x = x^2 \wedge x > \mathbf{1}) \vee x^2 < \mathbf{1})$
$\equiv \exists x(x = x^2 \wedge x > \mathbf{1} \wedge \neg x^2 < \mathbf{1})$

(4d) $\neg\forall x(x = \mathbf{0} \vee \exists y \neg(xy = x))$
$\equiv \exists x(\neg x = \mathbf{0} \wedge \neg\exists y \neg(xy = x))$
$\equiv \exists x(\neg x = \mathbf{0} \wedge \forall y(xy = x))$

(4g) $\neg\exists x(P(x) \rightarrow \forall y P(y))$
$\equiv \neg\exists x(\neg P(x) \vee \forall y P(y))$
$\equiv \forall x(P(x) \wedge \neg\forall y P(y))$
$\equiv \forall x(P(x) \wedge \exists y \neg P(y))$

(4h) $\neg(\forall x(P(x) \rightarrow Q(x)) \rightarrow (\forall x P(x) \rightarrow \forall x Q(x)))$
$\equiv \forall x(P(x) \rightarrow Q(x)) \wedge \neg(\neg\forall x P(x) \vee \forall x Q(x))$
$\equiv \forall x(P(x) \rightarrow Q(x)) \wedge (\forall x P(x) \wedge \exists x \neg Q(x))$

(4i) $\neg((\exists x P(x) \rightarrow \exists x Q(x)) \rightarrow \exists x(P(x) \rightarrow Q(x)))$
$\equiv \neg(\neg(\exists x P(x) \rightarrow \exists x Q(x)) \vee \exists x(\neg P(x) \vee Q(x)))$
$\equiv (\exists x P(x) \rightarrow \exists x Q(x)) \wedge \forall x(P(x) \wedge \neg Q(x))$

(5a) Suppose $\forall x A(x) \not\vDash \neg\exists x \neg A(x)$. Then there is a structure $\mathcal{S}$ and an assignment v such that $\mathcal{S}, v \vDash \forall x A(x)$ but $\mathcal{S}, v \not\vDash \neg\exists x \neg A(x)$. $\mathcal{S}, v \vDash \forall x A(x)$ implies $\mathcal{S}, v[x := s] \vDash A(x)$ for all $s \in \mathcal{S}$. From $\mathcal{S}, v \not\vDash \neg\exists x \neg A(x)$, we have $\mathcal{S}, v \vDash \exists x \neg A(x)$, which means that there is an $s' \in \mathcal{S}$ such that $\mathcal{S}, v[x := s'] \vDash \neg A(x)$. Hence, $\mathcal{S}, v[x := s'] \not\vDash A(x)$, contradicting the fact that $\mathcal{S}, v[x := s] \vDash A(x)$ for all $s \in \mathcal{S}$.

(5b) Likewise.

(5c) Suppose $\exists x A(x) \not\models \neg\forall x \neg A(x)$. Then there is a structure $\mathcal{S}$ and an assignment v such that $\mathcal{S}, v \vDash \exists x A(x)$ but $\mathcal{S}, v \not\vDash \neg\forall x \neg A(x)$. From $\mathcal{S}, v \vDash \exists x A(x)$ it follows that there is $s' \in \mathcal{S}$ such that $\mathcal{S}, v[x := s'] \vDash A(x)$. Besides, $\mathcal{S}, v \not\vDash \neg\forall x \neg A(x)$ implies that $\mathcal{S}, v \vDash \forall x \neg A(x)$. Hence, $\mathcal{S}, v[x := s] \vDash \neg A(x)$ for all $s \in \mathcal{S}$, and so $\mathcal{S}, v[x := s] \not\vDash A(x)$ for all $s \in \mathcal{S}$, contradicting the fact that $\mathcal{S}, v[x := s'] \vDash A(x)$.

(5d) Likewise.

(5e) Suppose $\exists x \exists y A(x, y) \not\models \exists y \exists x A(x, y)$. Then there is a structure $\mathcal{S}$ and an assignment v such that $\mathcal{S}, v \vDash \exists x \exists y A(x, y)$ but $\mathcal{S}, v \not\vDash \exists y \exists x A(x, y)$. $\mathcal{S}, v \vDash \exists x \exists y A(x, y)$ implies that there are $s', s'' \in \mathcal{S}$ such that $\mathcal{S}, v[x := s'][y := s''] \vDash A(x, y)$. From $\mathcal{S}, v \not\vDash \exists y \exists x A(x, y)$, we have $\mathcal{S}, v[x := s][y := t] \not\vDash A(x, y)$ for all $s, t \in \mathcal{S}$. This means that $\mathcal{S}, v[x := s'][y := s''] \not\vDash A(x, y)$, which is a contradiction.

(6) The first four logical consequences follow from the equivalences in Exercise 2. The rest follows from fact that, due to Proposition 4.3.2, if x does not occur free in Q, then $Q \equiv \forall x Q \equiv \exists x Q$.

(7a) For the sake of a contradiction, suppose $\forall x A(x), \forall x B(x) \not\models \forall x (A(x) \wedge B(x))$. Then there exist a structure $\mathcal{S}$ and an assignment v in $\mathcal{S}$ such that $\mathcal{S}, v \vDash \forall x A(x)$ and $\mathcal{S}, v \vDash \forall x B(x)$ but $\mathcal{S}, v \not\vDash \forall x (A(x) \wedge B(x))$. We thus have $\mathcal{S}, v[x := s] \vDash A(x)$ and $\mathcal{S}, v[x := s] \vDash B(x)$ for all $s \in \mathcal{S}$, while $\mathcal{S}, v[x := c] \not\vDash A(x) \wedge B(x)$ for some $c \in \mathcal{S}$. Hence, $\mathcal{S}, v[x := c] \not\vDash A(x)$ or $\mathcal{S}, v[x := c] \not\vDash B(x)$ for some $c \in \mathcal{S}$, which contradicts the fact that $A(x)$ and $B(x)$ are true for all s in $\mathcal{S}$.

(7b) Likewise.

(7c) Likewise.

(7d) Consider the structure $\mathcal{H}$ with A and B taken respectively as the predicates M and W.

(7e) Likewise.

(7f) For the sake of a contradiction, suppose $\forall x (A(x) \to B(x)) \not\models \forall x A(x) \to \forall x B(x)$. Then there exist a structure $\mathcal{S}$ and an assignment v in $\mathcal{S}$ such that $\mathcal{S}, v \vDash \forall x (A(x) \to B(x))$, while $\mathcal{S}, v \not\vDash \forall x A(x) \to \forall x B(x)$. Hence, $\mathcal{S}, v \vDash \forall x A(x)$ but $\mathcal{S}, v \not\vDash \forall x B(x)$. This means that $\mathcal{S}, v[x := s] \vDash A(x) \to B(x)$ and $\mathcal{S}, v[x := s] \vDash A(x)$ for all $s \in \mathcal{S}$, while $\mathcal{S}, v[x := c] \not\vDash B(x)$ for some $c \in \mathcal{S}$. We thus know that $\mathcal{S}, v[x := c] \not\vDash A(x) \to B(x)$, which contradicts the fact that $A(x) \to B(x)$ is true for all $s \in \mathcal{S}$.

(7g) Likewise.

(7h) Consider the structure $\mathcal{H}$ with A and B taken respectively as the predicates M and W.

(7i) For the sake of a contradiction, suppose $\exists x (A(x) \vee B(x)) \not\models \exists x A(x) \vee \exists x B(x)$. Then there exist a structure $\mathcal{S}$ and an assignment v in $\mathcal{S}$ such that $\mathcal{S}, v \vDash \exists x (A(x) \vee B(x))$, while $\mathcal{S}, v \not\vDash \exists x A(x) \vee \exists x B(x)$. Hence, $\mathcal{S}, v \not\vDash \exists x A(x)$ and $\mathcal{S}, v \not\vDash \exists x B(x)$. This means that there is some $c \in \mathcal{S}$ such that $\mathcal{S}, v[x := c] \vDash A(x)$ or $\mathcal{S}, v[x := c] \vDash B(x)$, while $\mathcal{S}, v[x := s] \not\vDash A(x)$ and $\mathcal{S}, v[x := s] \not\vDash B(x)$ for all $s \in \mathcal{S}$, which is a contradiction.

(7j) Likewise.

(7k) Consider the structure $\mathcal{N}$ with $A(x)$ meaning "x is prime" and $B(x)$ meaning "x is negative".

(7l) For the sake of a contradiction, suppose $\exists x A(x) \to \exists x B(x) \not\models \exists x (A(x) \to B(x))$. Then there exist a structure $\mathcal{S}$ and an assignment v such that $\mathcal{S}, v \vDash \exists x A(x) \to \exists x B(x)$, while $\mathcal{S}, v \not\vDash \exists x (A(x) \to B(x))$. Hence, $\mathcal{S}, v \not\vDash \exists x A(x)$ or $\mathcal{S}, v \vDash \exists x B(x)$, and so $\mathcal{S}, v[x := s] \not\vDash A(x)$ for all $s \in \mathcal{S}$ or $\mathcal{S}, v[x := c] \vDash B(x)$ for some $c \in \mathcal{S}$. On the other hand, from $\mathcal{S}, v \not\vDash \exists x (A(x) \to B(x))$, we have $\mathcal{S}, v[x := s] \not\vDash A(x) \to B(x)$ for all $s \in \mathcal{S}$, which means that $\mathcal{S}, v[x := s] \vDash A(x)$ and $\mathcal{S}, v[x := s] \not\vDash B(x)$ for all s, a contradiction.

(8) Using predicates $L(x)$ for "x is a lawyer" and $G(x)$ for "x is greedy", we can formalize A and B as follows:

$$\text{A} : \neg\forall x (L(x) \to G(x)) \text{ and}$$

$$\text{B} : \exists x L(x) \wedge \neg\forall x G(x).$$

First, we show that $\neg\forall x (L(x) \to G(x)) \vDash \exists x L(x) \wedge \neg\forall x G(x)$.

Suppose $\neg\forall x(L(x) \to G(x)) \not\models \exists x L(x) \wedge \neg\forall x G(x)$. Then there is a structure $\mathcal{S}$ and an assignment v on $\mathcal{S}$ such that $\mathcal{S}, v \models \neg\forall x(L(x) \to G(x))$, while $\mathcal{S}, v \not\models \exists x L(x) \wedge \neg\forall x G(x)$. However, then $\mathcal{S}, v \not\models \forall x(L(x) \to G(x))$, while $\mathcal{S}, v \not\models \exists x L(x)$ or $\mathcal{S}, v \models \forall x G(x)$. $\mathcal{S}, v \not\models \forall x(L(x) \to G(x))$ implies there is some c in $\mathcal{S}$ such that $\mathcal{S}, v[x := c] \not\models L(x) \to G(x)$. This means that $\mathcal{S}, v[x := c] \models L(x)$ but $\mathcal{S}, v[x := c] \not\models G(x)$. Hence, $\mathcal{S}, v \models \exists x L(x)$ and $\mathcal{S}, v \not\models \forall x G(x)$, which is a contradiction. On the other hand, $\exists x L(x) \wedge \neg\forall x G(x) \not\models \neg\forall x(L(x) \to G(x))$. To see this, consider for instance the structure $\mathcal{N}$ with $L(x)$ taken to mean "x is divisible by 6" and $G(x)$ to mean "x is divisible by 3".

(9) Using predicates $H(x)$ for "x is happy" and $D(x)$ for "x is drunk", we can formalize A and B as follows:

$$\text{A} : \neg\exists x(H(x) \to D(x)) \text{ and}$$
$$\text{B} : \exists x H(x) \wedge \exists x \neg D(x).$$

First, we show that $\neg\exists x(H(x) \to D(x)) \models \exists x H(x) \wedge \exists x \neg D(x)$. Suppose $\neg\exists x(H(x) \to D(x)) \not\models \exists x H(x) \wedge \exists x \neg D(x)$. Then there is a structure $\mathcal{S}$ and an assignment v on $\mathcal{S}$ such that $\mathcal{S}, v \models \neg\exists x(H(x) \to D(x))$, while $\mathcal{S}, v \not\models \exists x H(x) \wedge \exists x \neg D(x)$. However, then $\mathcal{S}, v \not\models \exists x(H(x) \to D(x))$, while $\mathcal{S}, v \not\models \exists x H(x)$ or $\mathcal{S}, v \not\models \exists x \neg D(x)$. $\mathcal{S}, v \not\models \exists x(H(x) \to D(x))$ implies $\mathcal{S}, v[x := s] \not\models H(x) \to D(x)$ for all s in $\mathcal{S}$. This means that $\mathcal{S}, v[x := s] \models H(x)$ and $\mathcal{S}, v[x := s] \models \neg D(x)$ for all s in $\mathcal{S}$. Hence, $\mathcal{S}, v \models \exists x H(x)$ and $\mathcal{S}, v \models \exists x \neg D(x)$, a contradiction. On the other hand, $\exists x H(x) \wedge \exists x \neg D(x) \not\models \neg\exists x(H(x) \to D(x))$. To see this, consider for instance the structure $\mathcal{N}$ and take $H(x)$ to mean "x is divisible by 2" and $D(x)$ to mean "x is divisible by 3".

(10a) Using predicates $L(x)$ for "x is a logician", $C(x)$ for "x is clever", and $R(x)$ for "x is rich", we can formalize the argument as follows:

$$\frac{\forall x(L(x) \to C(x)), \forall x(C(x) \to R(x))}{\forall x(L(x) \to R(x))}.$$

The argument is correct. To see this, suppose $\forall x(L(x) \to C(x)), \forall x(C(x) \to R(x)) \not\models \forall x(L(x) \to R(x))$. Then there is a structure $\mathcal{S}$ and an assignment v on $\mathcal{S}$ such that $\mathcal{S}, v \models \forall x(L(x) \to C(x))$ and $\mathcal{S}, v \models \forall x(C(x) \to R(x))$ but $\mathcal{S}, v \not\models \forall x(L(x) \to R(x))$. Now, $\mathcal{S}, v \not\models \forall x(L(x) \to R(x))$ implies that $\mathcal{S}, v[x := c] \not\models L(x) \to R(x)$ for some c in $\mathcal{S}$, and so $\mathcal{S}, v[x := c] \models L(x)$ while $\mathcal{S}, v[x := c] \not\models R(x)$. On the other hand, since $\mathcal{S}, v \models \forall x(L(x) \to C(x))$, $\mathcal{S}, v[x := c] \models L(x) \to C(x)$, which means $\mathcal{S}, v[x := c] \not\models L(x)$ or $\mathcal{S}, v[x := c] \models C(x)$. If $\mathcal{S}, v[x := c] \not\models L(x)$, we have a contradiction with $\mathcal{S}, v[x := c] \models L(x)$. If $\mathcal{S}, v[x := c] \models C(x)$, note that $\mathcal{S}, v \models \forall x(C(x) \to R(x))$ implies $\mathcal{S}, v[x := c] \not\models C(x)$ or $\mathcal{S}, v[x := c] \models R(x)$, again a contradiction.

(10b) Using predicates $N(x)$ for "x is a natural number", $I(x)$ for "x is an integer" and $O(x)$ for "x is odd", we can formalize the argument as follows:

$$\frac{\forall x(N(x) \to I(x)), \exists x(I(x) \wedge O(x))}{\exists x(N(x) \wedge O(x))}.$$

The argument is not logically correct. To see this, consider for instance the structure $\mathcal{N}$ and take $N(x)$ to mean "x is negative", $I(x)$ to mean "x is positive" and $O(x)$ to mean "x is odd".

(10c) Using predicates $P(x)$ for "x is a penguin", $B(x)$ for "x is a bird" and $W(x)$ for "x is white", we can formalize the argument as follows:

$$\frac{\forall x(P(x) \to B(x)), \exists x(P(x) \wedge W(x))}{\exists x(B(x) \wedge W(x) \wedge P(x))}.$$

The argument is correct. To see this, suppose $\forall x(P(x) \to B(x)), \exists x(P(x) \wedge W(x)) \not\models \exists x(B(x \wedge W(x) \wedge P(x))$. Then there is some structure $\mathcal{S}$ and an assignment on $\mathcal{S}$ such that $\mathcal{S}, v \models \forall x(P(x) \to B(x))$ and $\mathcal{S}, v \models \exists x(P(x) \wedge W(x))$ but $\mathcal{S}, v \not\models \exists x(B(x) \wedge W(x) \wedge P(x))$. Now, $\mathcal{S}, v \models \exists x(P(x) \wedge W(x))$ implies that $\mathcal{S}, v[x := c] \models P(x) \wedge W(x)$ for some c in $\mathcal{S}$. Hence, $\mathcal{S}, v[x := c] \models P(x)$ and $\mathcal{S}, v[x := c] \models W(x)$. However, since $\mathcal{S}, v \models \forall x(P(x) \to B(x))$, $\mathcal{S}, v[x := c] \not\models P(x)$ or $\mathcal{S}, v[x := c] \models B(x)$. Furthermore, $\mathcal{S}, v \not\models \exists x(B(x) \wedge W(x) \wedge P(x))$ implies that $\mathcal{S}, v[x := c] \not\models B(x)$ or $\mathcal{S}, v[x := c] \not\models W(x)$ or $\mathcal{S}, v[x := c] \not\models P(x)$. It is not difficult to see that in each of these cases we get a contradiction.

(10d) Using predicates $P(x)$ for "x is a plonk", $Y(x)$ for "x is yellow" and $Q(x)$ for "x is a qlink", we can formalize the argument as follows:

$$\frac{\neg\exists x(P(x) \wedge Y(x) \wedge Q(x)),\ \exists x(P(x) \vee \neg Q(x))}{\exists x(\neg Y(x) \wedge Q(x))}$$

The argument is not logically correct. To see this, consider for instance the structure $\mathcal{N}$ and take $P(x)$ to mean "x is negative", $Y(x)$ to mean "x is positive" and $Q(x)$ to mean "x is odd".

4.5. Semantic tableaux for first-order logic

(1a) $\vDash \forall x P(x) \to \forall y P(y)$ since the tableau closes:

$$\begin{array}{c} \forall x P(x) \to \forall y P(y) : \mathsf{F} \\ | \\ \forall x P(x) : \mathsf{T}^1, \forall y P(y) : \mathsf{F} \\ | \\ P(c) : \mathsf{F} \\ | \\ P(c) : \mathsf{T} \\ \times \end{array}$$

(1d) $\neg\exists x \neg A(x) \vDash \forall x A(x)$ since the tableau closes:

$$\begin{array}{c} \neg\exists x \neg A(x) : \mathsf{T}, \forall x A(x) : \mathsf{F} \\ | \\ A(c) : \mathsf{F} \\ | \\ \exists x \neg A(x) : \mathsf{F} \\ | \\ \neg A(c) : \mathsf{F} \\ | \\ A(c) : \mathsf{T} \\ \times \end{array}$$

(1g) $\exists x \exists y Q(x, y) \vDash \exists y \exists x Q(x, y)$ since the tableau closes:

$$\exists x \exists y Q(x, y) : \mathsf{T}, \exists y \exists x Q(x, y) : \mathsf{F}$$
$$\exists y Q(c_1, y) : \mathsf{T}$$
$$Q(c_1, c_2) : \mathsf{T}$$
$$\exists x Q(x, c_2) : \mathsf{F}$$
$$Q(c_1, c_2) : \mathsf{F}$$
$$\times$$

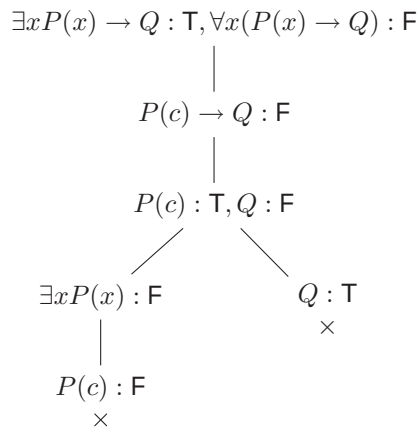
(2a) $\forall x(P(x) \vee Q) \vDash \forall x P(x) \vee Q$ since the tableau closes:

$$\forall x(P(x) \vee Q) : \mathsf{T}, \forall x P(x) \vee Q : \mathsf{F}$$
$$\forall x P(x) : \mathsf{F}, Q : \mathsf{F}$$
$$P(c) : \mathsf{F}$$
$$P(c) \vee Q : \mathsf{T}$$
$$P(c) : \mathsf{T} \qquad\qquad Q : \mathsf{T}$$
$$\times \qquad\qquad \times$$

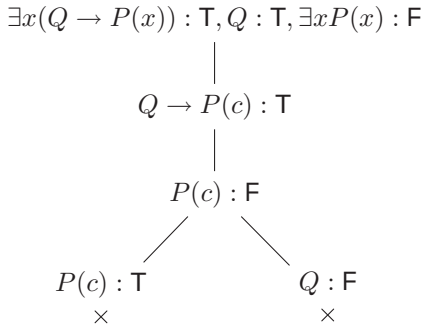
(2d) $\exists x P(x) \wedge Q \vDash \exists x(P(x) \wedge Q)$ since the tableau closes:

$$\exists x P(x) \wedge Q : \mathsf{T}, \exists x(P(x) \wedge Q) : \mathsf{F}$$
$$\exists x P(x) : \mathsf{T}, Q : \mathsf{T}$$
$$P(c) : \mathsf{T}$$
$$P(c) \wedge Q : \mathsf{F}$$
$$P(c) : \mathsf{F} \qquad\qquad Q : \mathsf{F}$$
$$\times \qquad\qquad \times$$

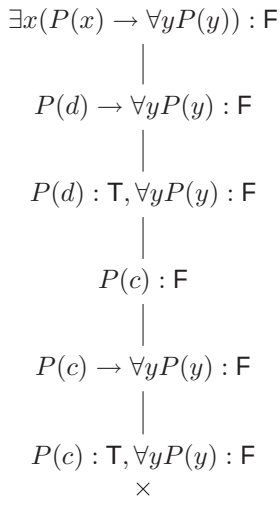
(2f) $\exists x P(x) \to Q \vDash \forall x(P(x) \to Q)$ since the tableau closes:



(2h) $\exists x(Q \to P(x)), Q \vDash \exists x P(x)$ since the tableau closes:



(3a) $\vDash \exists x(P(x) \to \forall y P(y))$ since the tableau closes:



(3b) The tableau closes, hence the formula is valid.

(3c) $\not\models \forall x\exists y Q(x,y) \to \forall y\exists x Q(x,y)$ since the tableau does not terminate:

$$\begin{array}{c}
\forall x\exists y Q(x,y) \to \forall y\exists x Q(x,y) : \mathsf{F} \\
\vert \\
\forall x\exists y Q(x,y) : \mathsf{T}, \forall y\exists x Q(x,y) : \mathsf{F} \\
\vert \\
\exists x Q(x,c_1) : \mathsf{F} \\
\vert \\
Q(c_1,c_1) : \mathsf{F} \\
\vert \\
\exists y Q(c_1,y) : \mathsf{T} \\
\vert \\
Q(c_1,c_2) : \mathsf{T} \\
\vert \\
Q(c_2,c_1) : \mathsf{F} \\
\vert \\
\exists y Q(c_2,y) : \mathsf{T} \\
\vert \\
Q(c_2,c_3) : \mathsf{T} \\
\vdots
\end{array}$$

Countermodel: consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(3d) The tableau closes, hence the formula is valid.

(3e) $\not\models \forall x\exists y Q(x,y) \to \exists y\forall x Q(x,y))$ since the tableau does not terminate.
Countermodel: consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(3f) $\not\models \forall x\exists y Q(x,y) \to \exists x Q(x,x))$ since the tableau does not terminate.
Countermodel: consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

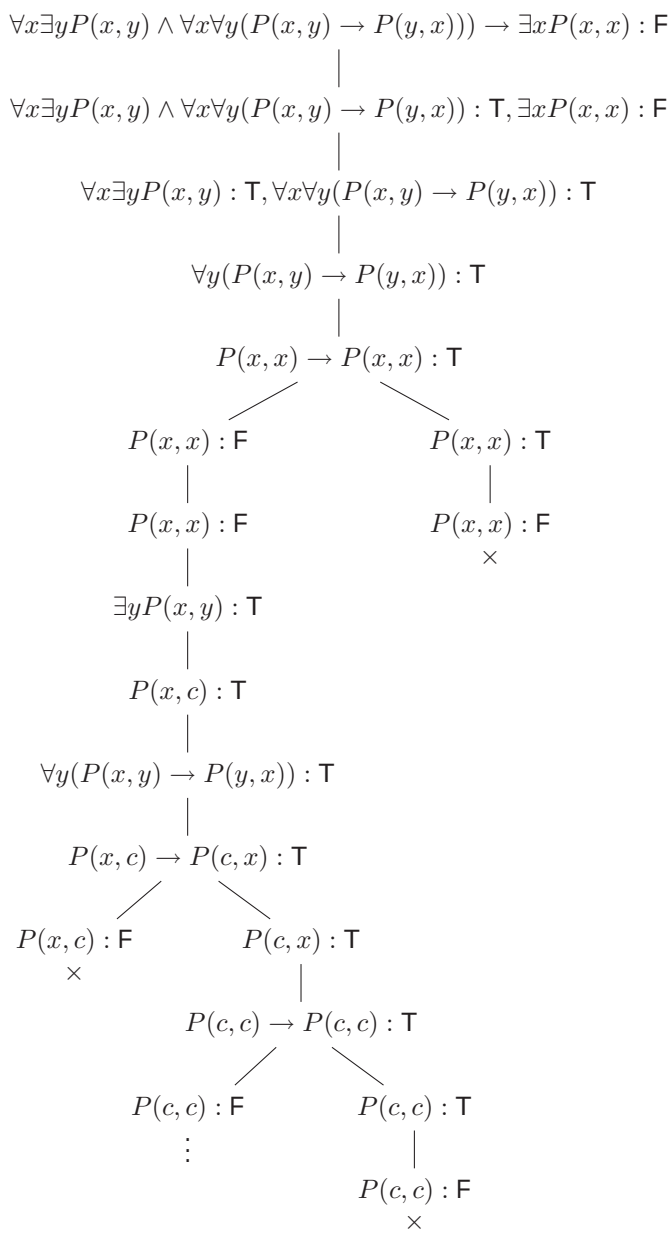
(3g) The tableau closes, hence the formula is valid.

(3h) $\not\models \forall x(\exists y Q(x,y) \to \exists y Q(y,x))$ since the tableau does not terminate.
Countermodel: consider the structure $\mathcal{N}$ with Q taken as the predicate $<$.

(3i) $\vDash \exists x \neg \exists y P(x, y) \rightarrow \forall y \neg \forall x P(x, y)$ since the tableau closes:

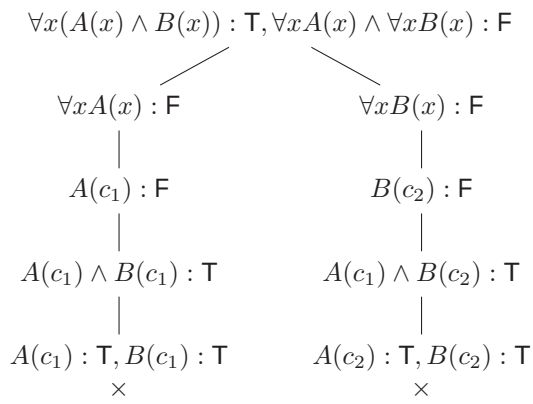
$$\exists x \neg \exists y P(x, y) \rightarrow \forall y \neg \forall x Q(x, y) : \mathsf{F}$$
$$\exists x \neg \exists y P(x, y) : \mathsf{T}, \forall y \neg \forall x P(x, y) : \mathsf{F}$$
$$\neg \exists y P(c_1, y) : \mathsf{T}$$
$$\exists y P(c_1, y) : \mathsf{F}$$
$$P(c_1, c_1) : \mathsf{F}$$
$$\neg \forall x P(x, c_2) : \mathsf{F}$$
$$\forall x P(x, c_2) : \mathsf{T}$$
$$P(c_1, c_2) : \mathsf{T}$$
$$P(c_1, c_2) : \mathsf{F}$$
$$\times$$

(3j) $\not\models \forall x \exists y P(x,y) \wedge \forall x \forall y (P(x,y) \rightarrow P(y,x))) \rightarrow \exists x P(x,x)$ since the tableau does not terminate:



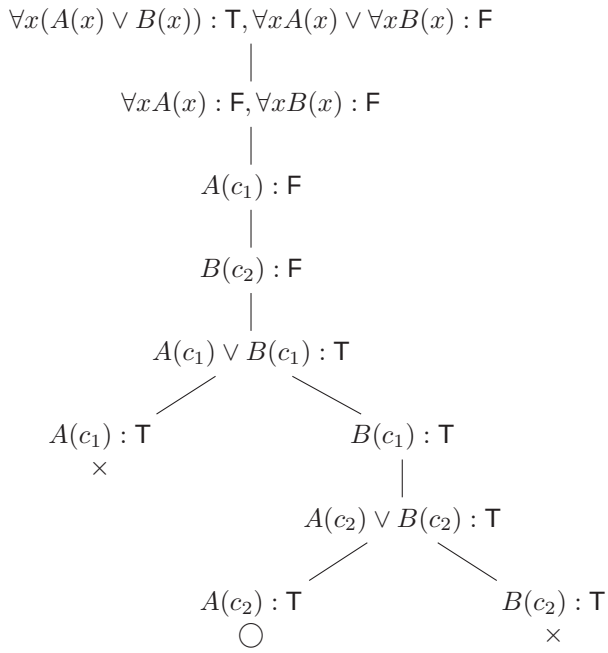
(4a) The tableau closes, hence the logical consequence holds.

(4b) $\forall x(A(x) \wedge B(x)) \vDash \forall x A(x) \wedge \forall x B(x)$ since the tableau closes:



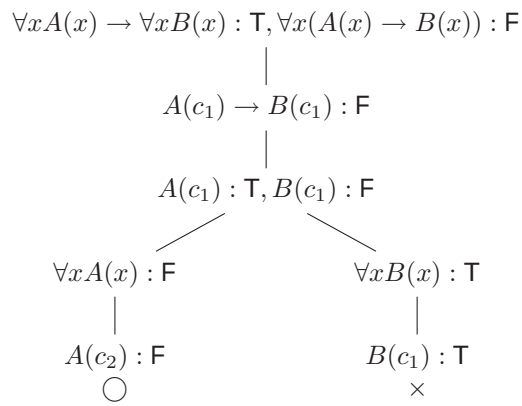
(4c) The tableau closes, hence the logical consequence holds.

(4d) $\forall x(A(x) \vee B(x)) \nvDash \forall x A(x) \vee \forall x B(x)$ since the tableau does not close:



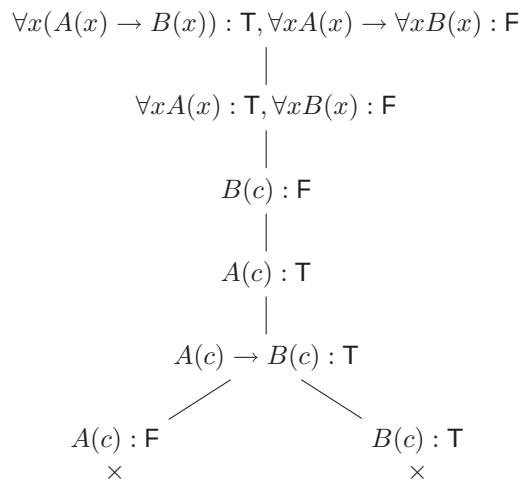
Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$ where c_1 is interpreted as a_1, c_2 is interpreted as a_2, A is interpreted as $\{a_1\}$ and B is interpreted as $\{a_2\}$.

(4e) $\forall x A(x) \to \forall x B(x) \not\models \forall x(A(x) \to B(x))$ since the tableau does not close:



Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$ where c_1 is interpreted as a_1, c_2 is interpreted as a_2, A is interpreted as $\{a_1\}$ and B is interpreted as $\{a_2\}$.

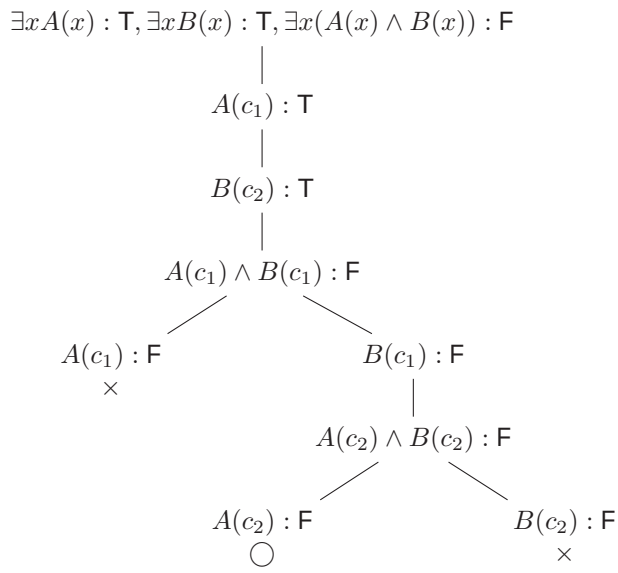
(4f) $\forall x(A(x) \to B(x)) \models \forall x A(x) \to \forall x B(x)$ since the tableau closes:



(4g) $\forall x(A(x) \to B(x)) \models \exists x A(x) \to \exists x B(x)$ since the tableau closes.

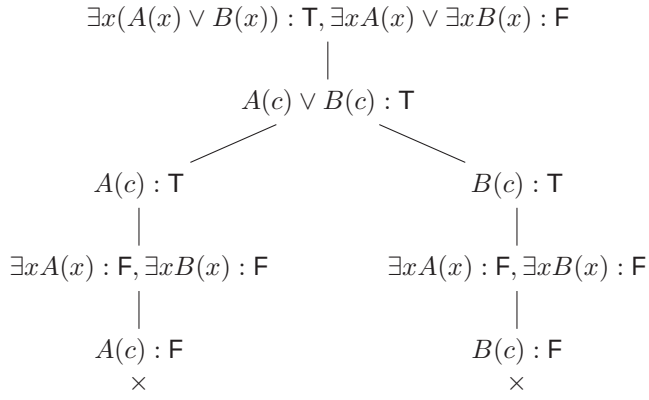
(4h) $\exists x(A(x) \wedge B(x)) \models \exists x A(x) \wedge \exists x B(x)$ since the tableau closes.

(4i) $\exists x A(x), \exists x B(x) \not\models \exists x(A(x) \wedge B(x))$ since the tableau does not close:



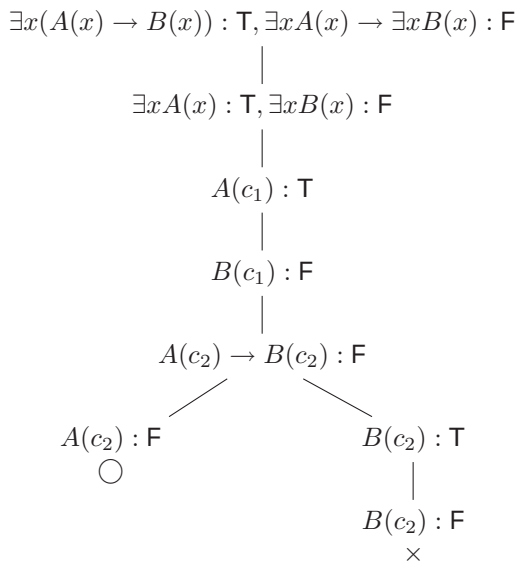
Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$, where c_1 is interpreted as a_1, c_2 is interpreted as a_2, A is interpreted as $\{a_1\}$ and B is interpreted as $\{a_2\}$.

(4j) $\exists x(A(x) \vee B(x)) \vDash \exists x A(x) \vee \exists x B(x)$ since the tableau closes:



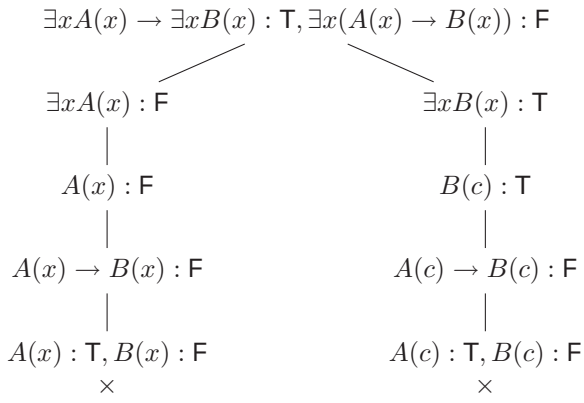
(4k) $\exists x A(x) \vee \exists x B(x) \vDash \exists x(A(x) \vee B(x))$ since the tableau closes.

(4l) $\exists x(A(x) \to B(x)) \not\models \exists x A(x) \to \exists x B(x)$ since the tableau does not close:



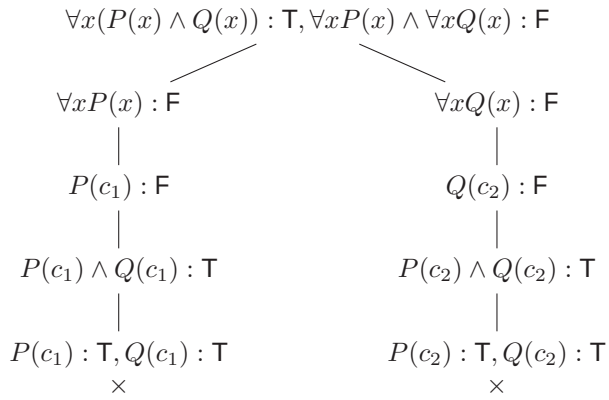
Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$, where c_1 is interpreted as a_1, c_2 is interpreted as a_2, A is interpreted as $\{a_1\}$ and B is interpreted as $\emptyset$.

(4m) $\exists x A(x) \to \exists x B(x) \models \exists x(A(x) \to B(x))$ since the tableau closes:

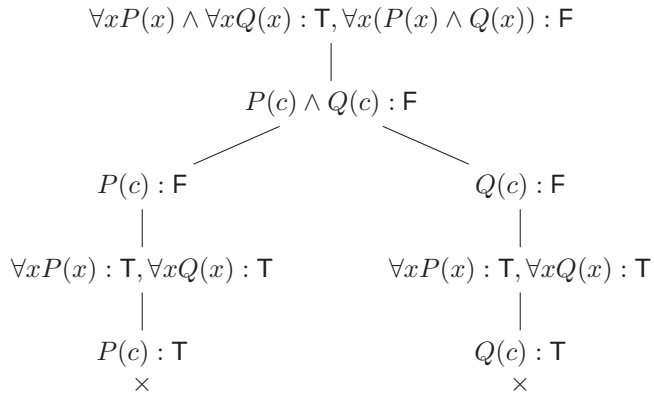


(5a) Checking the validity of both consequences:

$\forall x(P(x) \wedge Q(x)) \vDash \forall x P(x) \wedge \forall x Q(x)$:

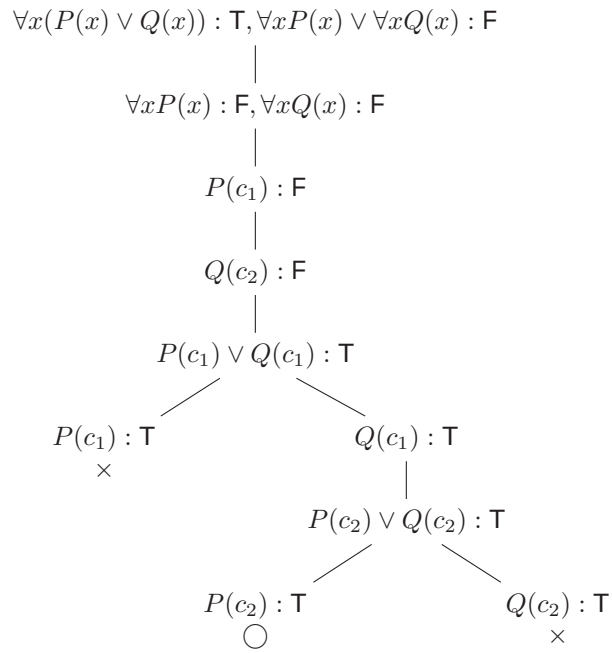


$\forall x P(x) \wedge \forall x Q(x) \vDash \forall x(P(x) \wedge Q(x))$:



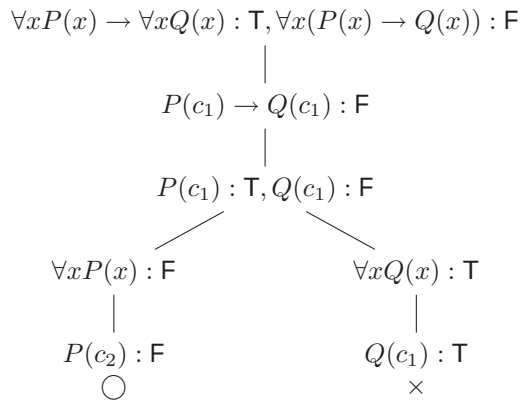
Hence, $\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$.

(5b) $\forall x(P(x) \vee Q(x)) \not\equiv \forall x P(x) \vee \forall x Q(x)$ because $\forall x(P(x) \vee Q(x)) \not\models \forall x P(x) \vee \forall x Q(x)$:



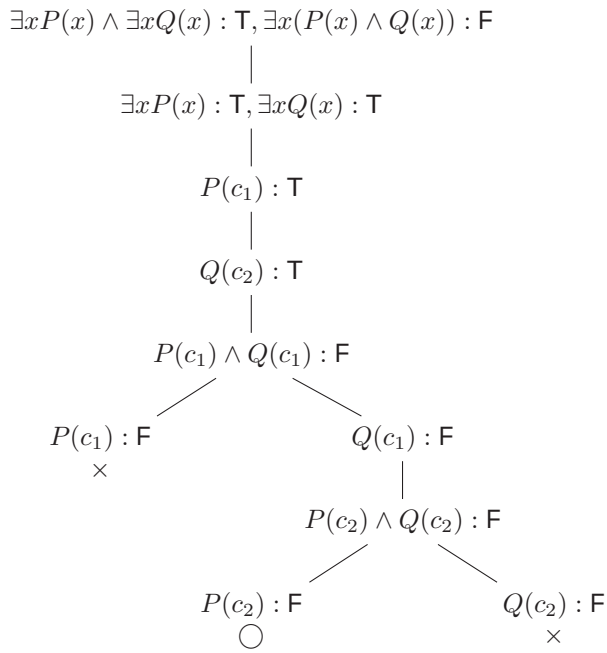
Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$, where c_1 is interpreted as a_1, c_2 is interpreted as a_2, P is interpreted as $\{a_2\}$ and Q is interpreted as $\{a_1\}$.

(5c) $\forall x P(x) \to \forall x Q(x) \not\equiv \forall x(P(x) \to Q(x))$ because $\forall x P(x) \to \forall x Q(x) \not\models \forall x(P(x) \to Q(x))$:



Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$ where c_1 is interpreted as a_1, c_2 is interpreted as a_2, P is interpreted as $\{a_1\}$ and Q is interpreted as $\varnothing$.

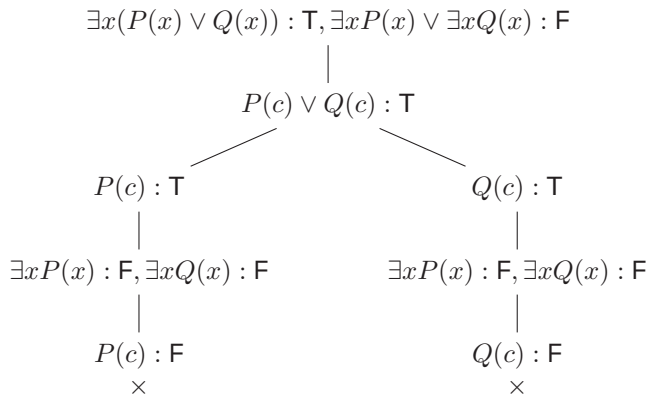
(5d) $\exists x P(x) \wedge \exists x Q(x) \not\equiv \exists x(P(x) \wedge Q(x))$ since $\exists x P(x) \wedge \exists x Q(x) \not\models \exists x(P(x) \wedge Q(x))$:



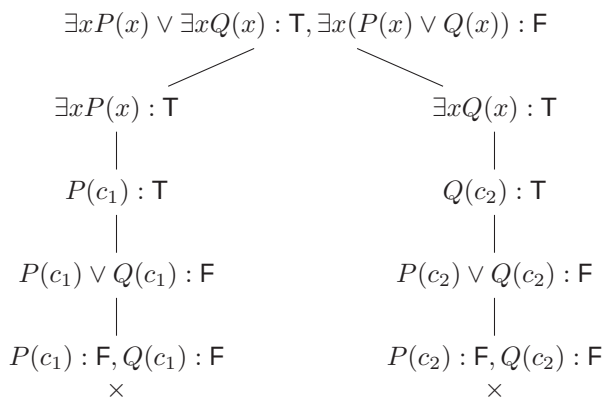
Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$, where c_1 is interpreted as a_1, c_2 is interpreted as a_2, P is interpreted as $\{a_1\}$ and Q is interpreted as $\{a_2\}$.

(5e) Checking the validity of both consequences:

$\exists x(P(x) \vee Q(x)) \models \exists x P(x) \vee \exists x Q(x)$:

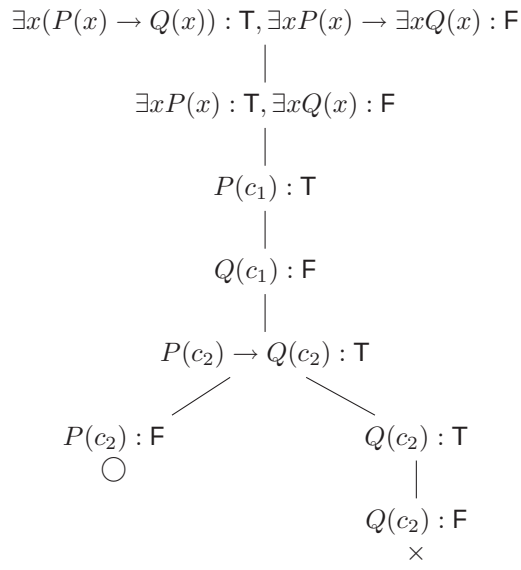


$\exists x P(x) \vee \exists x Q(x) \vDash \exists x(P(x) \vee Q(x))$:



Therefore, $\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$.

(5f) $\exists x(P(x) \to Q(x)) \not\equiv \exists x P(x) \to \exists x Q(x)$ because $\exists x(P(x) \to Q(x)) \nvDash \exists x P(x) \to \exists x Q(x)$:

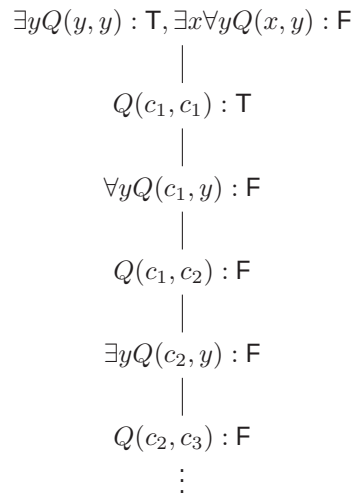


Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$, where c_1 is interpreted as a_1, c_2 is interpreted as a_2, P is interpreted as $\{a_1\}$ and Q is interpreted as $\varnothing$.

(5g) $\forall x Q(x, x) \not\equiv \forall x \exists y Q(x, y)$ because $\forall x \exists y Q(x, y) \nvDash \forall x Q(x, x)$. A countermodel: the structure $\mathcal{N}$ with Q taken as the predicate $<$.

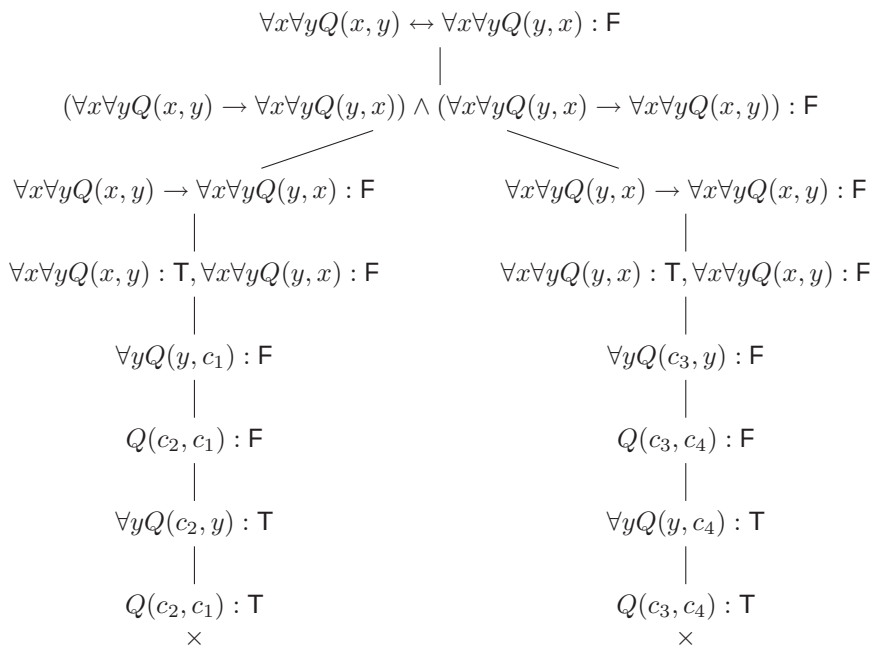
(5h) $\forall x \exists y Q(x, y) \not\equiv \exists x Q(x, x)$ since $\exists x Q(x, x) \nvDash \forall x \exists y Q(x, y)$. A countermodel: a structure with domain $\{a_1, a_2\}$, where Q is interpreted as $\{(a_1, a_1)\}$.

(5i) $\exists x \forall y Q(x, y) \not\equiv \exists y Q(y, y)$ since $\exists y Q(y, y) \not\models \exists x \forall y Q(x, y)$:



Countermodel: consider the structure $\mathcal{N}$ with Q taken as $=$.

(5j) Checking the validity of $\forall x \forall y Q(x, y) \leftrightarrow \forall x \forall y Q(y, x)$:



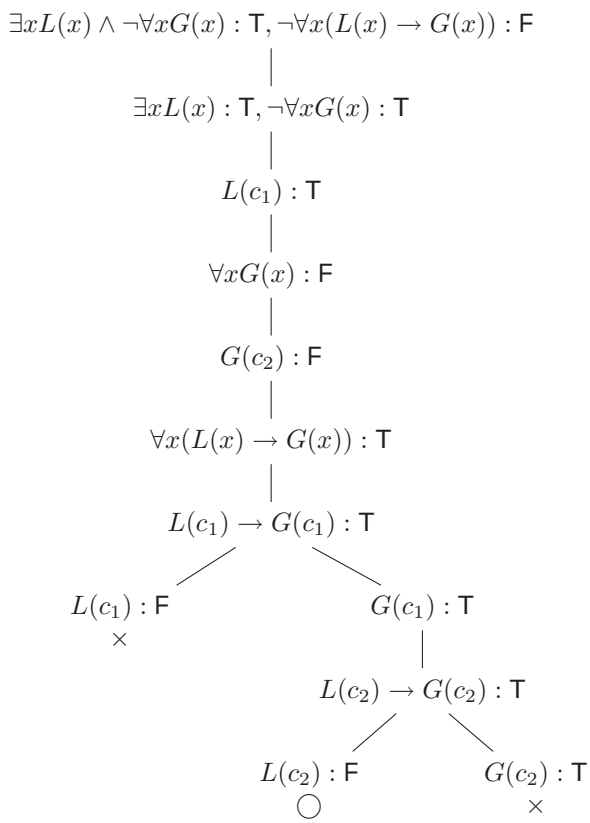
The tableau closes; hence $\forall x \forall y Q(x, y) \equiv \forall x \forall y Q(y, x)$.

(5k) The tableaux for both logical consequences close; hence the equivalence holds.

(6a) Using predicates $L(x)$ for "x is a lawyer" and $G(x)$ for "x is greedy", we can formalize A and B as follows:

$$\text{A} : \neg\forall x(L(x) \to G(x)) \text{ and}$$
$$\text{B} : \exists x L(x) \wedge \neg\forall x G(x).$$

Checking the validity of both consequences: the tableau for $\neg\forall x(L(x) \to G(x)) \vDash \exists x L(x) \wedge \neg\forall x G(x)$ closes; hence it holds. However, $\exists x L(x) \wedge \neg\forall x G(x) \nvDash \neg\forall x(L(x) \to G(x))$:



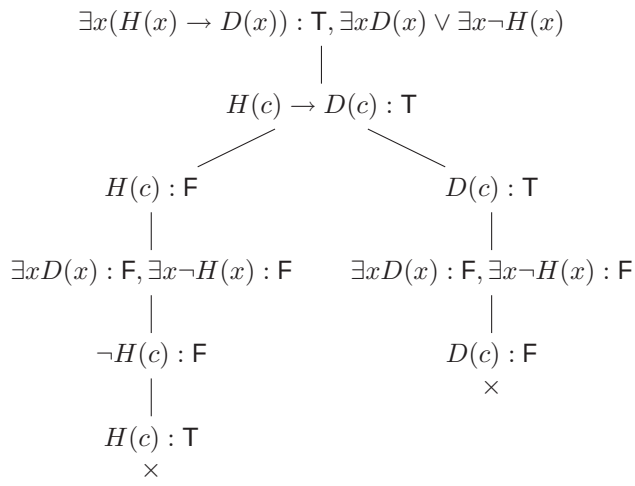
Countermodel extracted from the tableau: a structure with domain $\{a_1, a_2\}$, where c_1 is interpreted as a_1, c_2 is interpreted as a_2 and both L and G are interpreted as $\{a_1\}$. Therefore, $A \not\equiv B$.

(6b) Using predicates $H(x)$ for "x is happy" and $D(x)$ for "x is drunk", we can formalize A and B as follows:

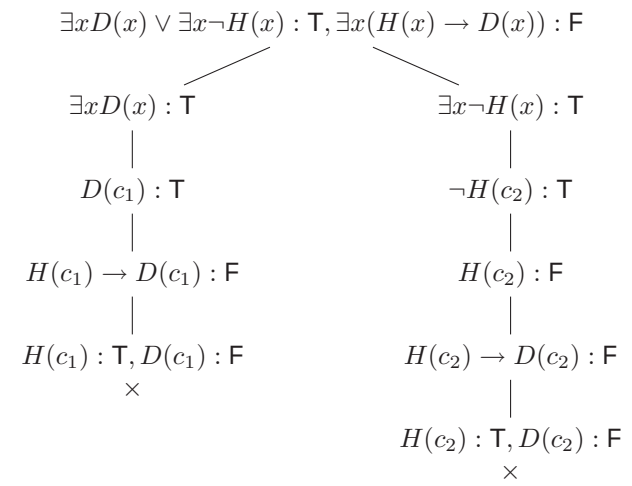
$$\text{A} : \exists x(H(x) \to D(x)) \text{ and}$$
$$\text{B} : \exists x D(x) \vee \exists x \neg H(x).$$

Checking the validity of both logical consequences:

$\exists x(H(x) \to D(x)) \vDash \exists x D(x) \vee \exists x \neg H(x)$:



$\exists x D(x) \vee \exists x \neg H(x) \vDash \exists x(H(x) \to D(x))$:



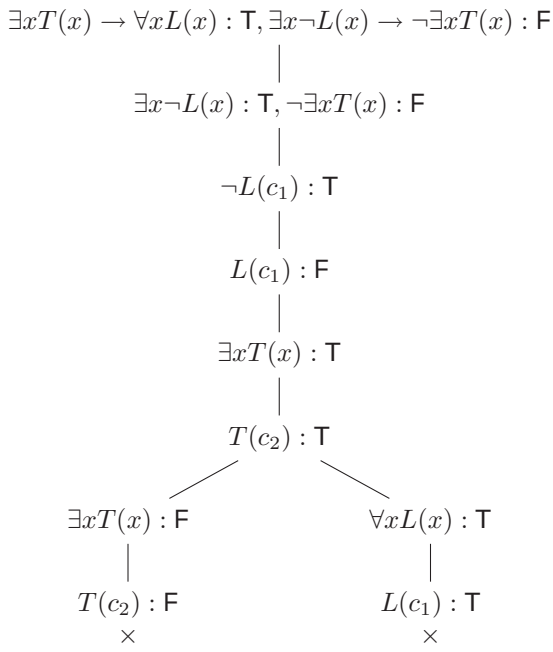
Both tableaux close; hence $A \equiv B$.

(6c) Using predicates $T(x)$ for "x is talking" and $L(x)$ for "x is listening", we can formalize A and B as follows:

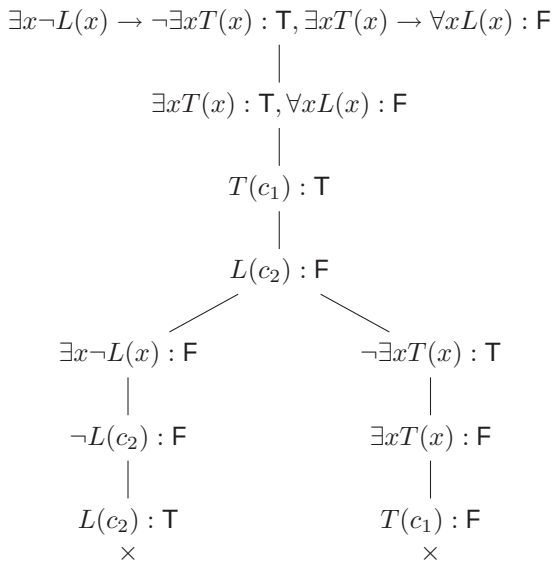
$$\text{A} : \exists x T(x) \to \forall x L(x) \text{ and}$$
$$\text{B} : \exists x \neg L(x) \to \neg \exists x T(x).$$

Checking the validity of both logical consequences:

$\exists x T(x) \to \forall x L(x) \vDash \exists x \neg L(x) \to \neg \exists x T(x)$:



$\exists x \neg L(x) \to \neg \exists x T(x) \vDash \exists x T(x) \to \forall x L(x)$:

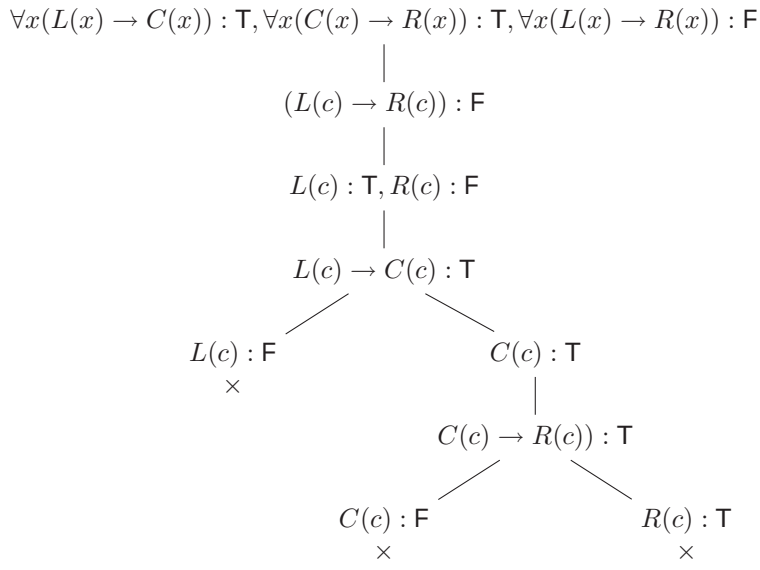


Both tableaux close; hence $A \equiv B$.

(7a) Using predicates $L(x)$ for "x is a logician", $C(x)$ for "x is clever" and $R(x)$ for "x is rich", we can formalize the argument as follows:

$$\frac{\forall x(L(x) \to C(x)), \forall x(C(x) \to R(x))}{\forall x(L(x) \to R(x))}.$$

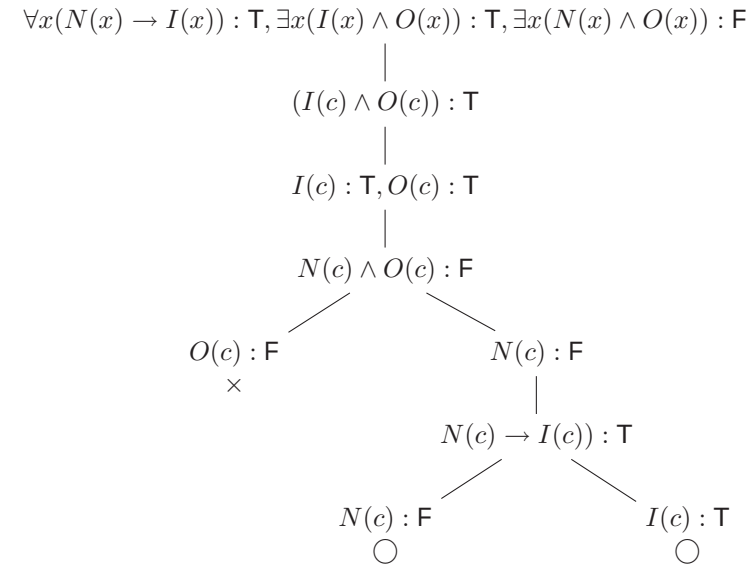
The argument is valid:



(7b) Using predicates $N(x)$ for "x is a natural number", $I(x)$ for "x is an integer" and $O(x)$ for "x is odd", we can formalize the argument as follows:

$$\frac{\forall x(N(x) \to I(x)), \exists x(I(x) \wedge O(x))}{\exists x(N(x) \wedge O(x))}.$$

The argument is not valid:

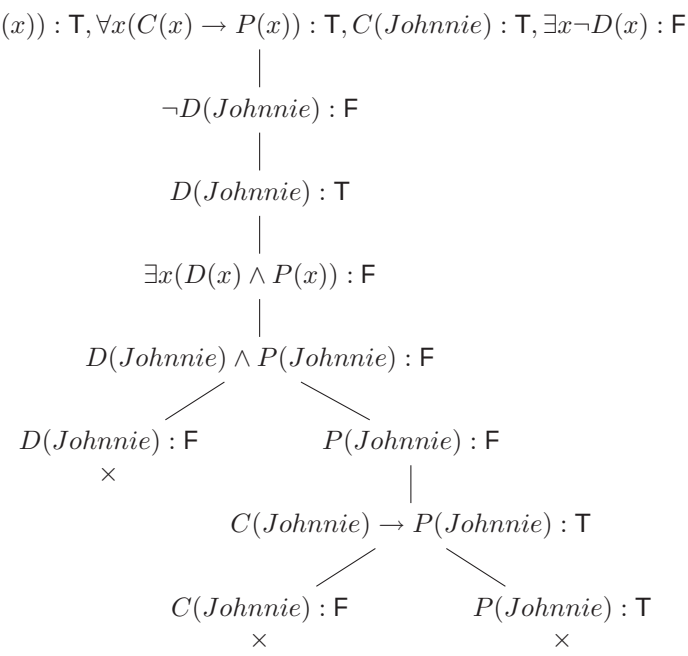


A countermodel extracted from the tableau: a structure with domain $\{a\}$, where c is interpreted as a, both I and O are interpreted as $\{a\}$ and N is interpreted as the empty set. Another countermodel: keep the original interpretation of N and I and change the interpretation of O to mean "x is negative".

(7c) Using predicates $P(x)$ for "x is a pedestrian", $C(x)$ for "x is a child" and $D(x)$ for "x is a driver", we can formalize the argument as follows:

$$\frac{\neg\exists x(D(x) \wedge P(x)),\ \forall x(C(x) \rightarrow P(x)),\ C(Johnnie)}{\exists x \neg D(x)}.$$

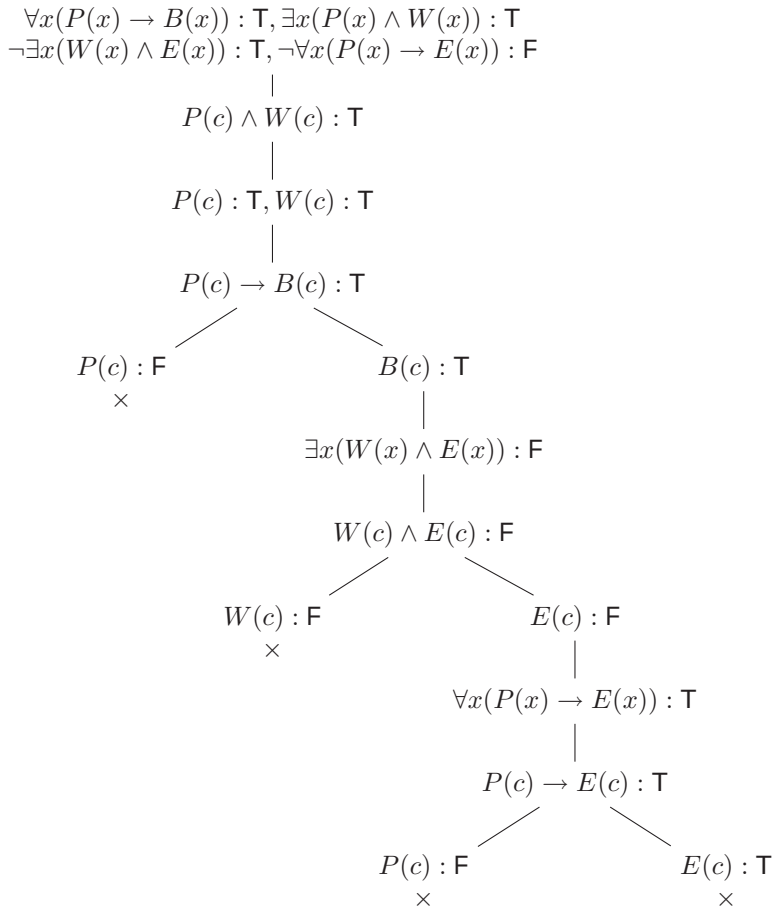
The argument is valid:



(7d) Using predicates $P(x)$ for "x is a penguin", $B(x)$ for "x is a bird", $W(x)$ for "x is white" and $E(x)$ for "x eats butterflies", we can formalize the argument as follows:

$$\frac{\forall x(P(x) \to B(x)),\ \exists x(P(x) \wedge W(x)),\ \neg\exists x(W(x) \wedge E(x))}{\neg\forall x(P(x) \to E(x))}.$$

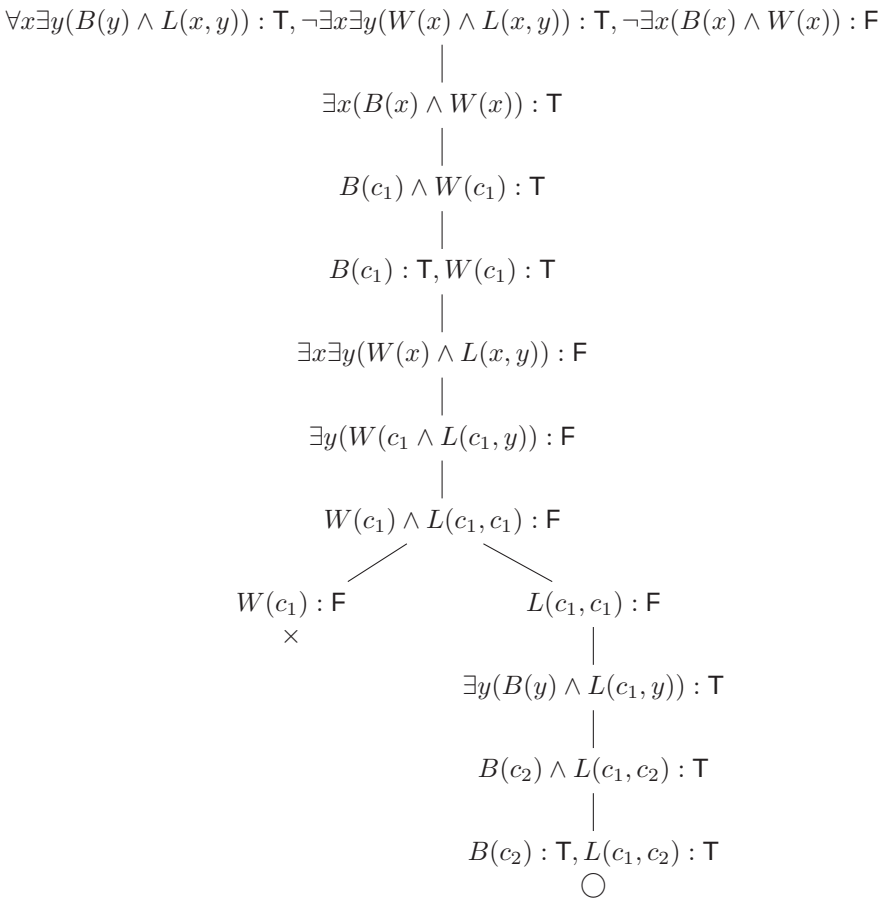
The argument is valid:



(7e) Using predicates $B(x)$ for "x is black gmuck", $W(x)$ for "x is white gmuck" and $L(x, y)$ for "x likes y", we can formalize the argument as follows:

$$\frac{\forall x \exists y(B(y) \wedge L(x, y)), \neg\exists x \exists y(W(x) \wedge L(x, y))}{\neg\exists x(B(x) \wedge W(x))}.$$

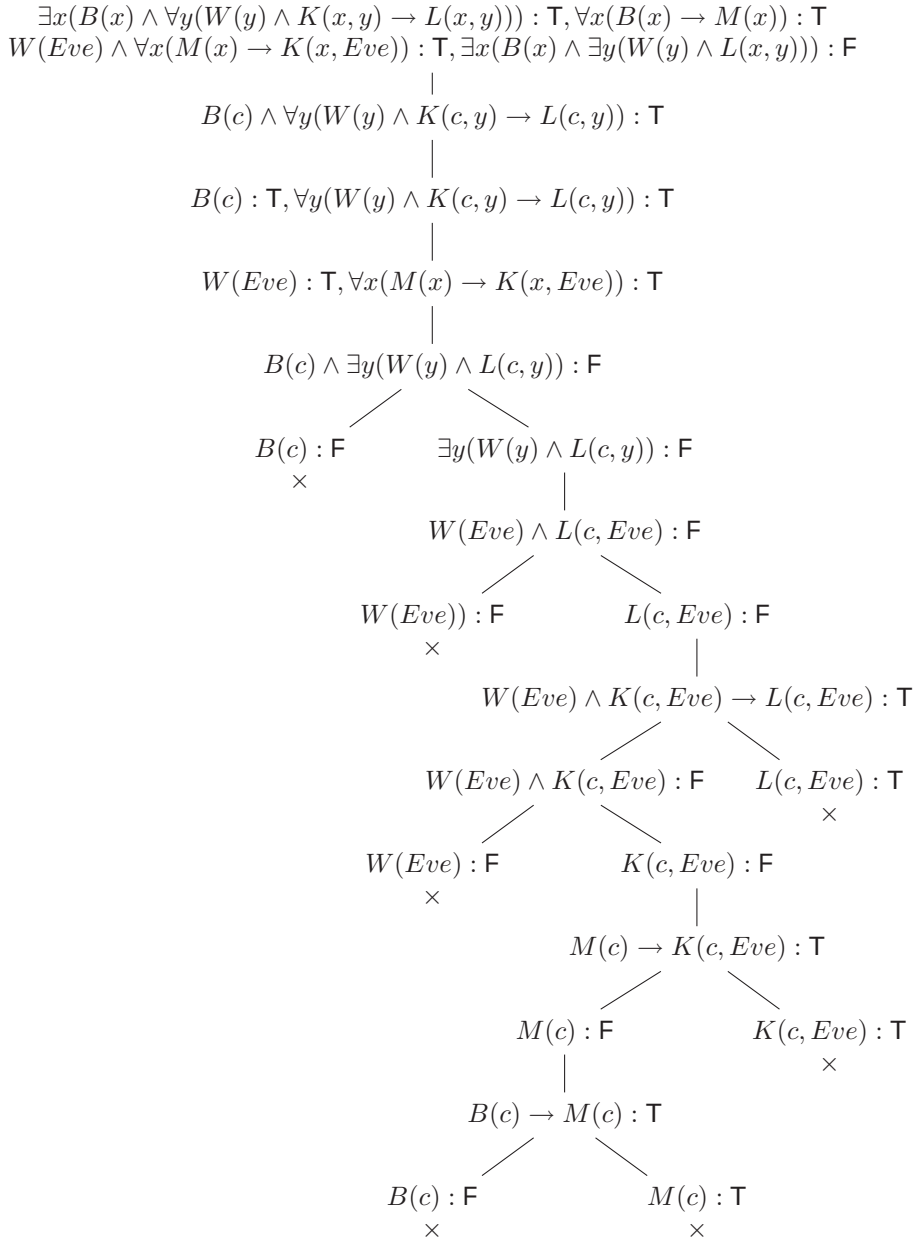
The argument is not valid:



(7f) Using predicates $B(x)$ for "x is a bachelor", $M(x)$ for "x is a man", $W(x)$ for "x is a woman", $K(x, y)$ for "x knows y" and $L(x, y)$ for "x loves y", we can formalize the argument as follows:

$$\frac{\begin{array}{l}\exists x(B(x) \wedge \forall y(W(y) \wedge K(x,y) \rightarrow L(x,y))) \\ \forall x(B(x) \rightarrow M(x)) \\ W(Eve) \wedge \forall x(M(x) \rightarrow K(x, Eve))\end{array}}{\exists x(B(x) \wedge \exists y(W(y) \wedge L(x,y)))}$$

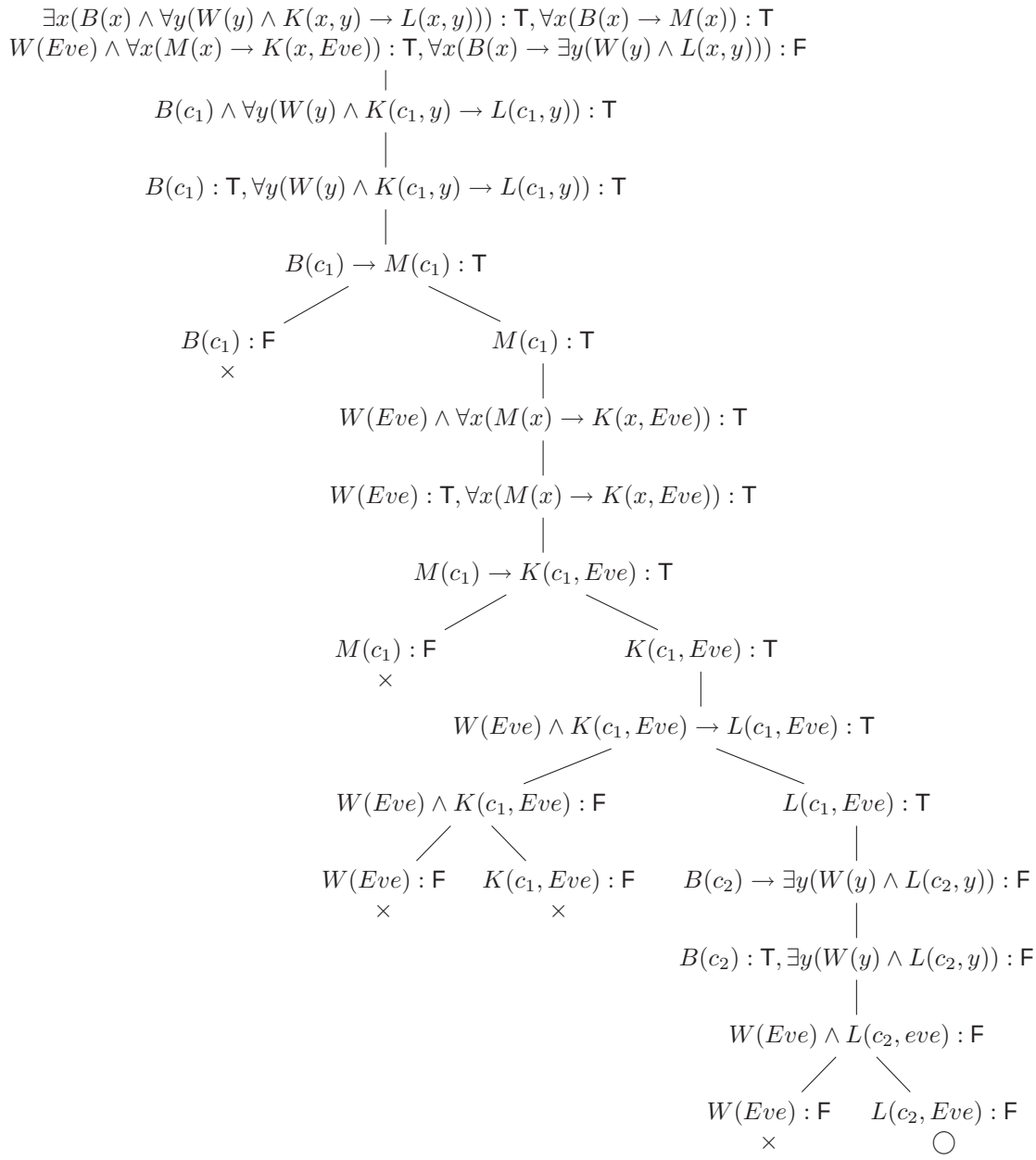
The argument is logically valid:



(7g) In this case, we can formalize the argument as follows:

$$\frac{\begin{array}{l}\exists x(B(x) \wedge \forall y(W(y) \wedge K(x,y) \rightarrow L(x,y))) \\ \forall x(B(x) \rightarrow M(x)) \\ W(Eve) \wedge \forall x(M(x) \rightarrow K(x,Eve))\end{array}}{\forall x(B(x) \rightarrow \exists y(W(y) \wedge L(x,y)))}$$

The argument is *not* valid:



4.6. Prenex and clausal normal forms

(1a) $\forall x((\exists y P(y) \wedge \forall z Q(z,x)) \rightarrow \exists y Q(x,y))$
$\equiv \forall x(\neg(\exists y P(y) \wedge \forall z Q(z,x)) \vee \exists y Q(x,y))$
$\equiv \forall x((\neg\exists y P(y) \vee \neg\forall z Q(z,x)) \vee \exists y Q(x,y))$
$\equiv \forall x(\forall y \neg P(y) \vee \exists z \neg Q(z,x) \vee \exists y Q(x,y))$
$\equiv \forall x(\forall y \neg P(y) \vee \exists z \neg Q(z,x) \vee \exists w Q(x,w))$
$\equiv \forall x \exists z \exists w \forall y(\neg P(y) \vee \neg Q(z,x) \vee Q(x,w))$ (PCNF and PDNF)

Skolemization: $\forall x \forall y(\neg P(y) \vee \neg Q(f(x),x) \vee Q(x,g(x)))$

Clausal form: $\{\neg P(y), \neg Q(f(x),x), Q(x,g(x))\}$

(1b) $\exists z(\exists x Q(x,z) \rightarrow (\exists x P(x) \vee \neg\exists z P(z)))$
$\equiv \exists z(\neg\exists x Q(x,z) \vee (\exists x P(x) \vee \forall z \neg P(z)))$
$\equiv \exists z(\forall x \neg Q(x,z) \vee \exists x P(x) \vee \forall z \neg P(z))$
$\equiv \exists z(\forall x \neg Q(x,z) \vee \exists y P(y) \vee \forall w \neg P(w))$
$\equiv \exists z \exists y \forall x \forall w(\neg Q(x,z) \vee P(y) \vee \neg P(w))$ (PCNF and PDNF)

Skolemization: $\forall x \forall w(\neg Q(x,c) \vee P(d) \vee \neg P(w))$

Clausal form: $\{\neg Q(x,c), P(d), \neg P(w)\}$

(1c) $\forall y \neg(P(y) \leftrightarrow \exists x Q(y,x))$
$\equiv \forall y \neg((\neg P(y) \vee \exists x Q(y,x)) \wedge (\neg\exists x Q(y,x) \vee P(y)))$
$\equiv \forall y((P(y) \wedge \forall x \neg Q(y,x)) \vee (\exists x Q(y,x) \wedge \neg P(y)))$
$\equiv \forall y((P(y) \wedge \forall x \neg Q(y,x)) \vee (\exists z Q(y,z) \wedge \neg P(y)))$
$\equiv \forall y \exists z \forall x((P(y) \vee \neg Q(y,x)) \vee (Q(y,z) \wedge \neg P(y)))$ (PDNF)
$\equiv \forall y \exists z \forall x((P(y) \vee (Q(y,z) \wedge \neg P(y))) \wedge (\neg Q(y,x) \vee (Q(y,z) \wedge \neg P(y))))$
$\equiv \forall y \exists z \forall x((P(y) \vee Q(y,z)) \wedge (\neg Q(y,x) \vee Q(y,z)) \wedge (\neg Q(y,x) \vee \neg P(y)))$ (PCNF)

Skolemization: $\forall y \forall x((P(y) \vee Q(y,f(y))) \wedge (\neg Q(y,x) \vee Q(y,f(y))) \wedge (\neg Q(y,x) \vee \neg P(y)))$

Clausal form: $\{\{P(y), Q(y,f(y))\}, \{\neg Q(y,x), Q(y,f(y))\}, \{\neg Q(y,x), \neg P(y)\}\}$

(1d) $\forall z(\exists y P(y) \leftrightarrow Q(z,y))$
$\equiv \forall z((\exists y P(y) \rightarrow Q(z,y)) \wedge (Q(z,y) \rightarrow \exists y P(y)))$
$\equiv \forall z((\neg\exists y P(y) \vee Q(z,y)) \wedge (\neg Q(z,y) \vee \exists y P(y)))$
$\equiv \forall z((\forall y \neg P(y) \vee Q(z,y)) \wedge (\neg Q(z,y) \vee \exists y P(y)))$
$\equiv \forall z((\forall u \neg P(u) \vee Q(z,y)) \wedge (\neg Q(z,y) \vee \exists v P(v)))$
$\equiv \forall z \exists v \forall u((\neg P(u) \vee Q(z,y)) \wedge (\neg Q(z,y) \vee P(v)))$ (PCNF)
$\equiv \forall z \exists v \forall u((\neg P(u) \wedge \neg Q(z,y)) \vee (\neg P(u) \wedge P(v)) \vee (Q(z,y) \wedge \neg Q(z,y)) \vee (Q(z,y) \wedge P(v)))$
$\equiv \forall z \exists v \forall u((\neg P(u) \wedge \neg Q(z,y)) \vee (\neg P(u) \wedge P(v)) \vee (Q(z,y) \wedge P(v)))$ (PDNF)

Skolemization: $\forall z \forall u((\neg P(u) \vee Q(z,y)) \wedge (\neg Q(z,y) \vee P(f(z))))$

Clausal form: $\{\{\neg P(u), Q(z,y)\}, \{\neg Q(z,y), P(f(z))\}\}$

(1e) $(\exists x P(x) \rightarrow \neg\exists x Q(x)) \rightarrow \forall x(P(x) \rightarrow \neg Q(x))$
$\equiv \neg(\exists x P(x) \rightarrow \neg\exists x Q(x)) \vee \forall x(P(x) \rightarrow \neg Q(x))$
$\equiv (\exists x P(x) \wedge \exists x Q(x)) \vee \forall x(\neg P(x) \vee \neg Q(x))$
$\equiv (\exists x P(x) \wedge \exists y Q(y)) \vee \forall z(\neg P(z) \vee \neg Q(z))$
$\equiv \exists x \exists y \forall z((P(x) \wedge Q(y)) \vee (\neg P(z) \vee \neg Q(z))$ (PDNF)
$\equiv \exists x \exists y \forall z((P(x) \vee \neg P(z) \vee \neg Q(z)) \wedge (Q(y) \vee \neg P(z) \vee \neg Q(z)))$ (PCNF)

Skolemization: $\forall z((P(c_1) \vee \neg P(z) \vee \neg Q(z)) \wedge (Q(c_2) \vee \neg P(z) \vee \neg Q(z)))$

Clausal form: $\{\{P(c_1), \neg P(z), \neg Q(z)\}, \{(Q(c_2), \neg P(z), \neg Q(z)\}\}$

(1f) $\forall x(\neg\forall y Q(x,y) \wedge P(z)) \rightarrow \exists z(\forall y Q(z,y) \wedge \neg P(x))$
$\equiv \neg\forall x(\neg\forall y Q(x,y) \wedge P(z)) \vee \exists z(\forall y Q(z,y) \wedge \neg P(x))$
$\equiv \exists x(\forall y Q(x,y) \vee \neg P(z)) \vee \exists z(\forall y Q(z,y) \wedge \neg P(x))$
$\equiv \exists u(\forall y Q(u,y) \vee \neg P(z)) \vee \exists w(\forall v Q(w,v) \wedge \neg P(x))$
$\equiv \exists u \exists w \forall y \forall v((Q(u,y) \vee \neg P(z)) \vee (Q(w,v) \wedge \neg P(x)))$ (PDNF)
$\equiv \exists u \exists w \forall y \forall v((Q(u,y) \vee \neg P(z) \vee Q(w,v)) \wedge (Q(u,y) \vee \neg P(z) \vee \neg P(x)))$ (PCNF)
Skolemization: $\forall y \forall u((Q(c_1,y) \vee \neg P(z) \vee Q(c_2,v)) \wedge (Q(c_1,y) \vee \neg P(z) \vee \neg P(x))$
Clausal form: $\{\{Q(c_1,y), \neg P(z), Q(c_2,v)\}, \{Q(c_1,y), \neg P(z), \neg P(x)\}\}$

(1j) $\neg(\forall y(\neg\exists z Q(y,z) \rightarrow P(z)) \rightarrow \exists z((P(z) \rightarrow Q(z,y)) \wedge \neg\exists x R(x,y,z)))$
$\equiv \forall y(\neg\exists z Q(y,z) \rightarrow P(z)) \wedge \forall z((P(z) \wedge \neg Q(z,y)) \vee \exists x R(x,y,z))$
$\equiv \forall y(\exists z Q(y,z) \vee P(z)) \wedge \forall z((P(z) \wedge \neg Q(z,y)) \vee \exists x R(x,y,z))$
$\equiv \forall v(\exists w Q(v,w) \vee P(z)) \wedge \forall u((P(u) \wedge \neg Q(u,y)) \vee \exists x R(x,y,u))$
$\equiv \forall v \exists w \forall u \exists x((Q(v,w) \vee P(z)) \wedge ((P(u) \wedge \neg Q(u,y)) \vee R(x,y,u)))$ $(*)$
$\equiv \forall v \exists w \forall u \exists x(((Q(v,w) \vee P(z)) \wedge (P(u) \wedge \neg Q(u,y))) \vee ((Q(v,w) \vee P(z)) \wedge R(x,y,u)))$
$\equiv \forall v \exists w \forall u \exists x((Q(v,w) \wedge P(u) \wedge \neg Q(u,y)) \vee (P(z) \wedge P(u) \wedge \neg Q(u,y)) \vee (Q(v,w) \wedge R(x,y,u)) \vee (P(z) \wedge R(x,y,u)))$ (PDNF)
$\equiv \forall v \exists w \forall u \exists x((Q(v,w) \vee P(z)) \wedge (P(u) \vee R(x,y,u)) \wedge (\neg Q(u,y) \vee R(x,y,u)))$ (PCNF from $(*)$)
Skolemization: $\forall v \forall u((Q(v,f(v)) \vee P(z)) \wedge (P(u) \vee R(g(v,u),y,u)) \wedge (\neg Q(u,y) \vee R(g(v,u),y,u)))$
Clausal form: $\{\{Q(v,f(v)), P(z)\}, \{P(u), R(g(v,u),y,u)\}, \{\neg Q(u,y), R(g(v,u),y,u)\}\}$

4.7. Resolution in first-order logic

(1a) First, we transform $\neg(\forall x P(x) \rightarrow \forall y P(y))$ to clausal form:

$$C_1 = \{P(x)\} \text{ and } C_2 = \{\neg P(c))\}$$

for some Skolem constant c. Unify $P(c)$ and $P(x)$ with $\mathsf{MGU}[c/x]$, and then resolve to obtain $\{\}$.

(1c) First, we transform $\neg\exists x(P(x) \rightarrow \forall y P(y))$ to clausal form:

$$C_1 = \{P(x)\} \text{ and } C_2 = \{\neg P(f(y))\}$$

for some Skolem function f. Unify $P(x)$ and $P(f(y))$ with $\mathsf{MGU}[f(y)/x]$, and then resolve to obtain $\{\}$.

(1e) First, we transform $\neg\forall x A(x)$ and $\neg\exists x \neg A(x)$ to clausal form:

$$C_1 = \{\neg A(c)\} \text{ and } C_2 = \{A(x)\}$$

for some Skolem constant c. Unify $A(x)$ and $A(c)$ with $\mathsf{MGU}[c/x]$, and then resolve to obtain $\{\}$.

(1h) First, we transform $\exists x \exists y A(x,y)$ and $\neg\exists y \exists x A(x,y)$ to clausal form:

$$C_1 = \{A(c_1,c_2)\} \text{ and } C_2 = \{\neg A(x,y)\}$$

for Skolem constants c_1 and c_2. Unify $A(c_1,c_2)$ and $A(x,y)$ with $\mathsf{MGU}[c_1/x, c_2/y]$, and then resolve to obtain $\{\}$.

(2a) First, we transform $\forall x(P(x) \vee Q)$ and $\neg(\forall x P(x) \vee Q)$ to clausal form:

$$C_1 = \{P(x), Q\}, C_2 = \{\neg P(c)\} \text{ and } C_3 = \{\neg Q\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$C_4 = Res(C_1, C_2) = \{Q\}$ $\mathsf{MGU}[c/x]$,
$C_5 = Res(C_3, C_4) = \{\}$.

The empty clause is derived; hence the logical consequence holds.

(2c) First, we transform $\exists x(P(x) \wedge Q)$ and $\neg(\exists x P(x) \wedge Q)$ to clausal form:

$$C_1 = \{P(c)\}, C_2 = \{Q\}, \text{ and } C_3 = \{\neg P(x), \neg Q\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_3) = \{\neg Q\} \qquad \mathsf{MGU}[c/x],$$
$$C_5 = Res(C_2, C_4) = \{\}.$$

The empty clause is derived; hence the logical consequence holds.

(2e) First, we transform $\forall x(Q \rightarrow P(x))$, Q and $\neg\forall x P(x)$ to clausal form:

$$C_1 = \{\neg Q, P(x)\}, C_2 = \{Q\} \text{ and } C_3 = \{\neg P(c)\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_3) = \{\neg Q\} \qquad \mathsf{MGU}[c/x],$$
$$C_5 = Res(C_2, C_4) = \{\}.$$

The empty clause is derived; hence the logical consequence holds.

(2h) First, we transform $\exists x(Q \rightarrow P(x))$, Q and $\neg\exists x P(x)$ to clausal form:

$$C_1 = \{\neg Q, P(c)\}, C_2 = \{Q\} \text{ and } C_3 = \{\neg P(x)\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_3) = \{\neg Q\} \qquad \mathsf{MGU}[c/x],$$
$$C_5 = Res(C_2, C_4) = \{\}.$$

The empty clause is derived; hence the logical consequence holds.

(3a) First, we transform $\forall x A(x)$, $\forall x B(x)$ and $\neg\forall x(A(x) \wedge B(x))$ to clausal form:

$$C_1 = \{A(x)\}, C_2 = \{B(x)\} \text{ and } C_3 = \{\neg A(c), \neg B(c)\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_2) = \{\neg B(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_5 = Res(C_2, C_4) = \{\} \qquad \mathsf{MGU}[c/x].$$

The empty clause is derived; hence the logical consequence holds.

(3b) The empty clause can be derived, hence the logical consequence holds.

(3c) The empty clause can be derived, hence the logical consequence holds.

(3d) First, we transform $\forall x(A(x) \vee B(x))$ and $\neg(\forall x A(x) \vee \forall x B(x))$ to clausal form:

$$C_1 = \{A(x), B(x)\}, C_2 = \{\neg A(c_1)\} \text{ and } C_3 = \{\neg B(c_2)\}$$

for Skolem constants c_1 and c_2. The only possible resolutions on this set of clauses are: unify $A(x)$ and $A(c_1)$ and resolve C_1 and C_2 to obtain $C_4 = \{B(c_1)\}$. Likewise, unify $B(x)$ and $B(c_2)$ and resolve C_1 and C_3 to obtain $C_5 = \{A(c_2)\}$. The empty clause cannot be derived; hence $\forall x(A(x) \vee B(x)) \not\models \forall x A(x) \vee \forall x B(x)$. Countermodel: for instance, consider the structure $\mathcal{H}$ with A and B taken respectively as the predicates M and W.

(3e) The empty clause cannot be derived; hence the logical consequence does not hold.
Countermodel: for instance, consider the structure $\mathcal{H}$ with A and B taken respectively as the predicates M and W.

(3f) First, we transform $\neg(\forall x A(x) \to \forall x B(x))$ and $\forall x(A(x) \to B(x))$ to clausal form:

$$C_1 = \{\neg A(x), B(x)\}, C_2 = \{A(x)\} \text{ and } C_3 = \{\neg B(c)\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_3) = \{\neg A(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_5 = Res(C_2, C_4) = \{\} \qquad \mathsf{MGU}[c/x].$$

The empty clause is derived; hence the logical consequence holds.

(3g) The empty clause can be derived; hence the logical consequence holds.

(3h) The empty clause cannot be derived; hence the logical consequence does not hold.
Countermodel: for instance, consider the structure $\mathcal{H}$ with A and B taken respectively as the predicates M and W.

(3i) First, we transform $\neg(\exists x A(x) \vee \exists x B(x))$ and $\exists x(A(x) \vee B(x))$ to clausal form:

$$C_1 = \{A(c), B(c)\}, C_2 = \{\neg A(x)\} \text{ and } C_3 = \{\neg B(y)\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_2) = \{B(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_5 = Res(C_3, C_4) = \{\} \qquad \mathsf{MGU}[c/y].$$

The empty clause is derived; hence the logical consequence holds.

(3j) The empty clause can be derived; hence the logical consequence holds.

(3k) First, we transform $\exists x(A(x) \to B(x))$ and $\neg(\exists x A(x) \to \exists x B(x))$ to clausal form:

$$C_1 = \{\neg A(c_1), B(c_1)\}, C_2 = \{A(c_2)\} \text{ and } C_3 = \{\neg B(y)\}$$

for Skolem constants c_1 and c_2. The only possible resolution on this set of clauses is to unify $B(y)$ and $B(c_1)$ and resolve C_1 and C_3 to obtain $C_4 = \{\neg A(c_1)\}$. The empty clause cannot be derived; hence $\exists x(A(x) \to B(x)) \not\models \exists x A(x) \to \exists x B(x)$.
Countermodel: for instance, consider the structure $\mathcal{N}$ with $A(x)$ meaning "x is prime" and $B(x)$ to be always false.

(3l) First, we transform $\exists x A(x) \to \exists x B(x)$ and $\neg\exists x(A(x) \to B(x))$ to clausal form:

$$C_1 = \{\neg A(x), B(f(x))\}, C_2 = \{A(z)\} \text{ and } C_3 = \{\neg B(z)\}$$

for some Skolem function f. Now, applying the resolution rule successively, we get

$$C_4 = Res(C_1, C_2) = \{B(f(x))\} \qquad \mathsf{MGU}[x/z],$$
$$C_5 = Res(C_3, C_4) = \{\} \qquad \mathsf{MGU}[f(x)/z].$$

The empty clause is derived; hence the logical consequence holds.

(4a) Using predicates $L(x)$ for "x is a logician", $C(x)$ for "x is clever" and $R(x)$ for "x is rich", we can formalize the argument as follows:

$$\frac{\forall x(L(x) \to C(x)), \forall x(C(x) \to R(x))}{\forall x(L(x) \to R(x))}.$$

We now transform the formulae $\forall x(L(x) \to C(x))$, $\forall x(C(x) \to R(x))$ and $\neg\forall x(L(x) \to R(x))$ to clausal form:

$$C_1 = \{\neg L(x), C(x)\}, C_2 = \{\neg C(x), R(x)\}, C_3 = \{L(c)\} \text{ and } C_4 = \{\neg R(c)\}$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_5 = Res(C_1, C_3) = \{C(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_6 = Res(C_2, C_4) = \{\neg C(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_7 = Res(C_5, C_6) = \{\}.$$

The empty clause is derived; hence the argument is valid.

(4b) Using predicates $N(x)$ for "x is a natural number", $I(x)$ for "x is an integer" and $O(x)$ for "x is odd", we can formalize the argument as follows:

$$\frac{\forall x(N(x) \rightarrow I(x)), \exists x(I(x) \wedge O(x))}{\exists x(N(x) \wedge O(x))}.$$

Then we transform the formulae $\forall x(N(x) \rightarrow I(x))$, $\exists x(I(x) \wedge O(x))$ and $\neg\exists x(N(x) \wedge O(x))$ to clausal form:

$$C_1 = \{\neg N(x), I(x)\}, C_2 = \{I(c)\}, C_3 = \{O(c)\} \text{ and } C_4 = \{\neg N(y), \neg O(y)\}$$

for some Skolem constant c. Applying the resolution rule we get

$$C_5 = Res(C_1, C_2) = \{\neg N(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_6 = Res(C_3, C_4) = \{\neg N(c)\} \qquad \mathsf{MGU}[c/y].$$

No more resolvents can be obtained; hence the empty clause cannot be derived, so the argument is not valid.

(4c) Using predicates $P(x)$ for "x is a penguin", $B(x)$ for "x is a bird", $W(x)$ for "x is white" and $E(x)$ for "x eats some fish", we can formalize the argument as follows:

$$\frac{\forall x(P(x) \rightarrow B(x)), \exists x(P(x) \wedge W(x)), \forall x(P(x) \rightarrow E(x))}{\exists x(W(x) \wedge B(x) \wedge E(x))}.$$

Now we transform the formulae $\forall x(P(x) \rightarrow B(x))$, $\exists x(P(x) \wedge W(x))$, $\forall x(P(x) \rightarrow E(x))$ and $\neg\exists x(W(x) \wedge B(x) \wedge E(x))$ to clausal form:

$$C_1 = \{\neg P(x), B(x)\}, \qquad C_2 = \{P(c)\},$$
$$C_3 = \{W(c)\}, \qquad C_4 = \{\neg P(x), E(x)\},$$
$$C_5 = \{\neg W(x), \neg B(x), \neg E(x)\}.$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_6 = Res(C_3, C_5) = \{\neg B(c), \neg E(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_7 = Res(C_4, C_6) = \{\neg P(c), \neg B(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_8 = Res(C_1, C_7) = \{\neg P(c)\} \qquad \mathsf{MGU}[c/x],$$
$$C_9 = Res(C_2, C_8) = \{\}.$$

The empty clause is derived; hence the argument is valid.

(4d) Using predicates $Y(x)$ for "x is yellow", $P(x)$ for "x is a plonk" and $Q(x)$ for "x is a qlink", we can formalize the argument as follows:

$$\frac{\neg\exists x(Y(x) \wedge P(x) \wedge Q(x)), \exists x(P(x) \vee \neg Q(x))}{\exists x\neg(Y(x) \wedge Q(x))}.$$

We next transform the formulae $\neg\exists x(Y(x) \wedge P(x) \wedge Q(x))$, $\exists x(P(x) \vee \neg Q(x))$ and $\neg\exists x\neg(Y(x) \wedge Q(x))$ to clausal form:

$$C_1 = \{\neg Y(x), \neg P(x), \neg Q(x)\}, \qquad C_2 = \{P(c), \neg Q(c)\},$$
$$C_3 = \{Y(x)\}, \qquad C_4 = \{Q(x)\}.$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$\begin{aligned} C_5 &= Res(C_1, C_2) = \{\neg Y(c), \neg Q(c)\} && \text{MGU}[c/x], \\ C_6 &= Res(C_3, C_5) = \{\neg Q(c)\} && \text{MGU}[c/x], \\ C_7 &= Res(C_4, C_6) = \{\}. && \text{MGU}[c/x]. \end{aligned}$$

The empty clause is derived; hence the argument is valid.

(5) The argument can be written as follows:

$$\begin{array}{l} \forall x(\mathbf{F}(x) \rightarrow \mathbf{E}(x)) \\ \forall x(\mathbf{H}(x) \rightarrow \neg\exists y(\mathbf{E}(y) \wedge \mathbf{L}(x, y))) \\ \exists x((\mathbf{G}(x) \vee \mathbf{F}(x)) \wedge \mathbf{L}(Kermit, x)) \\ \forall x(\exists y(\mathbf{G}(y) \wedge \mathbf{L}(x, y)) \rightarrow \neg\exists z(\mathbf{T}(z) \wedge \mathbf{L}(x, z))) \\ \hline \exists x(\mathbf{T}(x) \wedge \mathbf{L}(Kermit, x)) \rightarrow \neg\mathbf{H}(Kermit) \end{array}$$

From all premises and the negated conclusion we obtain the following clauses:

$$\begin{aligned} C_1 &= \{\neg\mathbf{F}(x), \mathbf{E}(x)\}, & C_2 &= \{\neg\mathbf{H}(x), \neg\mathbf{E}(x), \neg\mathbf{L}(x, y)\}, \\ C_3 &= \{\mathbf{G}(c_1), \mathbf{F}(c_1)\}, & C_4 &= \{\mathbf{L}(Kermit, c_1)\}, \\ C_5 &= \{\neg\mathbf{G}(y), \neg\mathbf{L}(x, y), \neg\mathbf{T}(z), \neg\mathbf{L}(x, z)\}, & C_6 &= \{\mathbf{T}(c_2)\}, \\ C_7 &= \{\mathbf{L}(Kermit, c_2)\}, & C_8 &= \{\mathbf{H}(Kermit)\}, \end{aligned}$$

for Skolem constants c_1 and c_2. Now, applying resolution successively, we get

$$\begin{aligned} C_9 &= Res(C_5, C_7) = \{\neg\mathbf{G}(y), \neg\mathbf{L}(Kermit, y), \neg\mathbf{T}(c_2)\} && \text{MGU}[Kermit/x, c_2/z], \\ C_{10} &= Res(C_6, C_9) = \{\neg\mathbf{G}(y), \neg\mathbf{L}(Kermit, y)\} \\ C_{11} &= Res(C_3, C_{10}) = \{\mathbf{F}(c_1), \neg\mathbf{L}(Kermit, c_1)\} && \text{MGU}[c_1/y], \\ C_{12} &= Res(C_1, C_{11}) = \{\mathbf{E}(c_1), \neg\mathbf{L}(Kermit, c_1)\} && \text{MGU}[c_1/x], \\ C_{13} &= Res(C_2, C_{12}) = \{\neg\mathbf{H}(x), \neg\mathbf{L}(x, c_1), \neg\mathbf{L}(Kermit, c_1)\} && \text{MGU}[c_1, y], \\ C_{14} &= Res(C_8, C_{13}) = \{\neg\mathbf{L}(Kermit, c_1)\} && \text{MGU}[Kermit/x], \\ C_{15} &= Res(C_4, C_{14}) = \{\}. \end{aligned}$$

The empty clause is derived; hence the argument is valid.

(6a) Using predicates $T(x)$ for "x is a troll", $G(x)$ for "x is a goblin", $E(x)$ for "x is an elf", $D(x)$ for "x is a dragon", $U(x)$ for "x is ugly" and $F(x)$ for "x can fly", we can formalize the argument as follows:

$$\begin{array}{l} \forall x(T(x) \rightarrow ((E(x) \wedge \neg G(x)) \vee (G(x) \wedge \neg E(x)))) \\ \forall y(T(y) \wedge F(y) \rightarrow E(y)) \\ \forall x(D(x) \rightarrow F(x)) \\ \forall x(G(x) \wedge U(x) \rightarrow T(x)) \\ \exists x(G(x) \wedge U(x)) \\ \hline \exists x(U(x) \wedge \neg D(x)) \end{array}$$

From all premises and the negated conclusion we obtain the following clauses:

$$C_1 = \{\neg T(x), E(x), G(x)\}, \qquad C_2 = \{\neg T(x), \neg E(x), \neg G(x)\},$$
$$C_3 = \{\neg T(y), \neg F(y), E(y)\}, \qquad C_4 = \{\neg D(u), F(u)\},$$
$$C_5 = \{\neg G(v), \neg U(v), T(v)\}, \qquad C_6 = \{G(c)\},$$
$$C_7 = \{U(c)\}, \qquad C_8 = \{\neg U(w), D(w)\},$$

for some Skolem constant c. Now, applying the resolution rule successively, we get

$$C_9 = Res(C_3, C_4) = \{\neg T(y), E(y), \neg D(y)\} \quad \mathsf{MGU}[y/u],$$
$$C_{10} = Res(C_8, C_9) = \{\neg T(y), E(y), \neg U(y)\} \quad \mathsf{MGU}[y/w],$$
$$C_{11} = Res(C_2, C_{10}) = \{\neg T(y), \neg U(y), \neg G(y)\} \quad \mathsf{MGU}[y/x],$$
$$C_{12} = Res(C_5, C_{11}) = \{\neg G(y), \neg U(y)\} \quad \mathsf{MGU}[y/v],$$
$$C_{13} = Res(C_6, C_{12}) = \{\neg U(c)\} \quad \mathsf{MGU}[c/y],$$
$$C_{14} = Res(C_7, C_{13}) = \{\}.$$

The empty clause is derived; hence the argument is valid.

(6b) Using predicates $B(x)$ for "x is a bachelor", $M(x)$ for "x is a man", $W(x)$ for "x is a woman", $K(x, y)$ for "x knows y" and $L(x, y)$ for "x loves y", we can formalize the argument as follows:

$$\frac{\begin{array}{l}\exists x(B(x) \wedge \forall y(W(y) \wedge K(x, y) \rightarrow L(x, y)))\\ \forall x(B(x) \rightarrow M(x))\\ W(Eve) \wedge \forall x(M(x) \rightarrow K(x, Eve))\end{array}}{\exists x(B(x) \wedge \exists y(W(y) \wedge L(x, y)))}$$

We then obtain the following clausal form:

$$C_1 = \{B(c)\}, \qquad C_2 = \{\neg W(y), \neg K(c, y), L(c, y)\},$$
$$C_3 = \{\neg B(z), M(z)\}, \qquad C_4 = \{W(Eve)\},$$
$$C_5 = \{\neg M(w), K(w, Eve)\}, \qquad C_6 = \{\neg B(u), \neg W(v), \neg L(u, v)\},$$

for some Skolem constant c. Now, applying resolution successively, we get

$$C_7 = Res(C_2, C_6) = \{\neg B(c), \neg W(y), \neg K(c, y)\} \quad \mathsf{MGU}[c/u, y/v],$$
$$C_8 = Res(C_5, C_7) = \{\neg B(c), \neg M(c), \neg W(Eve)\} \quad \mathsf{MGU}[c/w, Eve/y],$$
$$C_9 = Res(C_3, C_8) = \{\neg B(c), \neg W(Eve)\} \quad \mathsf{MGU}[c/z],$$
$$C_{10} = Res(C_1, C_9) = \{\neg W(Eve)\}$$
$$C_{11} = Res(C_4, C_{10}) = \{\}.$$

The empty clause is derived; hence the argument is valid.

(6c) In this case, the argument can be formalized as follows:

$$\frac{\begin{array}{l}\exists x(B(x) \wedge \forall y(W(y) \wedge K(x, y) \rightarrow L(x, y)))\\ \forall x(B(x) \rightarrow M(x))\\ W(Eve) \wedge \forall x(M(x) \rightarrow K(x, Eve))\end{array}}{\forall x(B(x) \rightarrow \exists y(W(y) \wedge L(x, y)))}$$

We then obtain the following clausal form:

$$C_1 = \{B(c_1)\}, \qquad C_2 = \{\neg W(y), \neg K(c_1, y), L(c_1, y)\},$$
$$C_3 = \{\neg B(z), M(z)\}, \qquad C_4 = \{W(Eve)\},$$
$$C_5 = \{\neg M(w), K(w, Eve)\}, \qquad C_6 = \{B(c_2)\},$$
$$C_7 = \{\neg W(y), \neg L(c_2, y)\},$$

for some Skolem constants c_1 and c_2. Now, the empty clause cannot be derived.

4.8. Applications of first-order logic to mathematical reasoning and proofs

(2a) We use a direct proof. Let a and b be integers and assume that their sum is even. Then there is an integer k such that $a + b = 2k$. Now subtract $2b$ on both sides to get $a - b = 2k - 2b = 2(k - b)$; hence $a - b$ is also even.

(2b) Here we combine direct reasoning with reasoning by contradiction. Let $a, b, x \in \mathbb{R}$ and assume $a < b$ and $(x - a)(x - b) < 0$. From $(x - a)(x - b) < 0$ we have that either $x - a < 0$ and $x - b > 0$ or $x - a > 0$ and $x - b < 0$; hence either $x < a$ and $b < x$ or $a < x$ and $x < b$. The first case leads to a contradiction with $a < b$ because $x < a$ and $b < x$ imply $b < a$ by transitivity of $<$ and $b < a$ does not imply $a < b$ by irreflexivity of $<$. The second case implies the claim $a < x < b$.

(2c) Here we use a direct proof. Let $a, b \in \mathbb{Q}$ such that $a < b$. Then $b - a > 0$. Now, by the Archimedean property, there is an integer m such that $\frac{1}{b-a} < m$. Hence, $1 < m(b - a)$, so $ma + 1 < mb$. Now, let n be the largest integer such that $n \leq ma$. (Why does n exist?) Then $n + 1 > ma$. On the other hand, $n + 1 \leq ma + 1 < mb$. Hence, $ma < n + 1 < mb$; therefore $a < \frac{n+1}{m} < b$.

(2d) We use a proof by contraposition. Let $m, n \in \mathbb{Z}$ and suppose mn is even; yet it is not the case that m is even or n is even. Therefore, both m and n are not even and hence they are odd. Then there are integers a and b such that $m = 2a + 1$ and $n = 2b + 1$. Therefore,

$$mn = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1,$$

which means that mn is odd and hence not even—a contradiction.

(2e) We use a direct reasoning here. First, note that $n^2 + n = n(n + 1)$. There are two cases: n even or n odd. If n is even, then $n(n + 1)$ is even. If n is odd, then $n + 1$ is even, and hence $n(n + 1)$ is even.

(2f) We use a direct proof here. Let $a, b \in \mathbb{Z}$ and assume ab is odd. This is only possible if both a and b are odd. Hence, $a = 2m + 1$ and $b = 2n + 1$ for some integers m and n. Then we obtain $a + b = 2m + 1 + 2n + 1 = 2m + 2n + 2 = 2(m + n + 1)$; hence $a + b$ is even.

(2g) We give a proof by contradiction. Suppose there are positive integers m and n such that $\frac{1}{m} + \frac{1}{n} > 2$. However, since m and n are positive integers we have that $m \geq 1$ and $n \geq 1$. Therefore $\frac{1}{m} \leq 1$ and $\frac{1}{n} \leq 1$, and hence $\frac{1}{m} + \frac{1}{n} \leq 2$—a contradiction.

(2h) We give a proof by contradiction. Suppose $\sqrt[3]{3}$ is not irrational. Then it is rational, which means that $\sqrt[3]{3} = \frac{m}{n}$ for some relatively prime integers m and n. Hence, $3 = \frac{m^3}{n^3}$ and so $3n^3 = m^3$. This means that 3 divides m^3. However, since 3 is prime, it follows from the properties of divisibility and prime numbers (see Theorem 5.4.6 in the textbook) that 3 divides m. Then $m = 3a$ for some integer a and hence $3n^3 = (3a)^3 = 27a^3$, so $n^3 = 9a^3$. By the same argument, we now show that 3 divides n—a contradiction with the assumption that m and n are relatively prime.

(2i) We use a simple proof by contraposition. Suppose that it is not the case that x is irrational or y is irrational. Then both x and y are rational; hence their sum is also rational.

5

Number Theory

5.1. The Principle of Mathematical Induction revisited

(1) For $n = 0$, $2^0 = 1$ and $2^{0+1} - 1 = 2 - 1 = 1$. The inductive hypothesis is that

$$2^0 + 2^1 + \cdots + 2^k = 2^{k+1} - 1$$

for some $k \geq 0$. Then, for $n = k + 1$ we have

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{(k+1)+1} - 1. \end{aligned}$$

(1a) For $n = 1$, both sides equal 1. The inductive hypothesis is that

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

for some $k \geq 1$. Then, for $n = k + 1$ we have

$$\begin{aligned} 1 + 3 + 5 + \cdots + 2k - 1 + 2(k+1) - 1 &= k^2 + 2k + 2 - 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2. \end{aligned}$$

(1c) For $n = 1$, we have $1^2 = 1$ and $\frac{(1+1)(2+1)}{6} = \frac{6}{6} = 1$. The inductive hypothesis is that

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

for some $k \geq 1$. Then, for $n = k + 1$, we have

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

Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

$$
\begin{aligned}
&= \frac{(k+1)(k(2k+1)+6(k+1))}{6} \\
&= \frac{(k+1)(2k^2+k+6k+6)}{6} \\
&= \frac{(k+1)(2k^2+7k+6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.
\end{aligned}
$$

(1d) For $n = 1$, we have $1^3 = 1$ and $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$. The inductive hypothesis is that

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

for some $k \geq 1$. Then, for $n = k+1$ we have

$$
\begin{aligned}
1^3 + 2^3 + 3^3 + \cdots + k^3 + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\
&= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\
&= \frac{(k+1)^2(k^2+4(k+1))}{4} \\
&= \frac{(k+1)^2(k^2+4k+4)}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4}.
\end{aligned}
$$

(1e) For $n = 1$, we have $1 \times (1+2) = 3$ and $\frac{(1+1)(2+7)}{6} = \frac{18}{6} = 3$. The inductive hypothesis is that

$$1 \times 3 + 2 \times 4 + \cdots + k \times (k+2) = \frac{k(k+1)(2k+7)}{6}$$

for some $k \geq 1$. Now, for $n = k+1$,

$$
\begin{aligned}
&1 \times 3 + 2 \times 4 + \cdots + k \times (k+2) + (k+1) \times (k+3) \\
&= \frac{k(k+1)(2k+7)}{6} + (k+1)(k+3) \\
&= \frac{k(k+1)(2k+7) + 6(k+1)(k+3)}{6} \\
&= \frac{(k+1)(k(2k+7)+6(k+3))}{6} \\
&= \frac{(k+1)(2k^2+7k+6k+18)}{6} \\
&= \frac{(k+1)(2k^2+13k+18)}{6} \\
&= \frac{(k+1)(k+2)(2k+9)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+7)}{6}.
\end{aligned}
$$

(1f) For $n = 1$ we have $\frac{1}{1\times 3} = \frac{1}{3}$ and $\frac{3+5}{4(1+1)(1+2)} = \frac{8}{24} = \frac{1}{3}$. The inductive hypothesis is

$$\frac{1}{1\times 3} + \frac{1}{2\times 4} + \cdots + \frac{1}{k\times(k+2)} = \frac{k(3k+5)}{4(k+1)(k+2)}$$

for some $k \geq 1$. Then for $n = k + 1$ we have

$$\begin{aligned}
&\frac{1}{1\times 3} + \frac{1}{2\times 4} + \cdots + \frac{1}{k\times(k+2)} + \frac{1}{(k+1)(k+3)} \\
&= \frac{k(3k+5)}{4(k+1)(k+2)} + \frac{1}{(k+1)(k+3)} \\
&= \frac{k(3k+5)(k+3) + 4(k+2)}{4(k+1)(k+2)(k+3)} \\
&= \frac{3k^3 + 14k^2 + 19k + 8}{4(k+1)(k+2)(k+3)} \\
&= \frac{(k+1)(3k^2 + 11k + 8)}{4(k+1)(k+2)(k+3)} \\
&= \frac{(k+1)(3k+8)(k+1)}{4(k+1)(k+2)(k+3)} \\
&= \frac{(k+1)(3(k+1)+5)}{4((k+1)+1)((k+1)+2)}.
\end{aligned}$$

(2) For $n = 0$, we have $(1+x)^0 = 1$ and $1 + 0x = 1$, so $(1+x)^0 \geq 1 + 0x$. The inductive hypothesis is that $(1+x)^k \geq 1 + kx$ for some $k \geq 0$. Note that $1 + x \geq 0$. Then, for $n = k + 1$ we have

$$\begin{aligned}
(1+x)^{k+1} &= (1+x)^k(1+x) \\
&\geq (1+kx)(1+x) \\
&= 1 + kx + x + kx^2 \\
&\geq 1 + kx + x \\
&= 1 + x(k+1).
\end{aligned}$$

(3a) We will prove by induction that

$$1\times 2 + 2\times 3 + 3\times 4 + \cdots + n\times(n+1) = \frac{n(n+1)(2n+4)}{6}.$$

First, when $n = 1$ we have $1 \times 2 = 2$ and $\frac{1(1+1)(2+4)}{6} = \frac{12}{6} = 2$. The inductive hypothesis is that

$$1\times 2 + 2\times 3 + 3\times 4 + \cdots + k\times(k+1) = \frac{k(k+1)(2k+4)}{6}$$

for some $k \geq 1$. Now, for $n = k + 1$ we have

$$\begin{aligned}
&1\times 2 + 2\times 3 + 3\times 4 + \cdots + k\times(k+1) + (k+1)\times(k+2) \\
&= \frac{k(k+1)(2k+4)}{6} + (k+1)\times(k+2) \\
&= \frac{k(k+1)(2k+4) + 6(k+1)(k+2)}{6} \\
&= \frac{(k+1)(2k^2 + 10k + 12)}{6} \\
&= \frac{(k+1)(k+2)(2k+6)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+4)}{6}.
\end{aligned}$$

(3b) We will prove by induction that

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

When $n=1$ we have $\frac{1}{1\times 2}=\frac{1}{2}$ and $\frac{1}{1+1}=\frac{1}{2}$. The inductive hypothesis is that

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

for some $k\geq 1$. Then for $n=k+1$ we have

$$\begin{aligned}
&\frac{1}{1\times 2}+\frac{1}{2\times 3}+\cdots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}\\
&=\frac{k}{k+1}+\frac{1}{(k+1)(k+2)}\\
&=\frac{k(k+2)+1}{(k+1)(k+2)}\\
&=\frac{k^2+2k+1}{(k+1)(k+2)}\\
&=\frac{(k+1)^2}{(k+1)(k+2)}\\
&=\frac{k+1}{k+2}.
\end{aligned}$$

(4) Suppose there are natural numbers greater than or equal to n_0, for which P does not hold. The set of such numbers has a least element m. First, m must be greater than n_0, since P does hold for n_0. Since m is the least natural number for which P does not hold, P must hold for all natural numbers less than m. Hence, by assumption, P must hold for m, which is a contradiction.

(5) The assumption that the property P holds for n_0 can be omitted because it follows vacuously from the inductive assumption of Theorem 5.1.2 and the fact that there are no natural numbers greater than or equal to n_0 and less than k when $k=n_0$.

(6) First, assume the PCMI holds. Now suppose that some property P holds for some natural number $n_0\geq 0$ and whenever P holds for some natural number $m\geq n_0$, it holds for $m+1$. Then, moreover, if P holds for all natural numbers less that $m+1$ and greater than or equal n_0, then it also holds for $m+1$. Therefore, by PMCI, P holds for every natural number greater than or equal to n_0. Thus, we have proved the PMI.

Conversely, assume that the PMI holds. We will prove the PCMI as follows. Suppose that the property P holds for some natural number n_0, and for any natural number $k\geq n_0$, whenever P holds for all natural numbers greater than or equal to n_0 and less than k, then P holds for k. We consider the property P^* where $P^*(n)$ means that $P(n)$ holds for all natural numbers greater than or equal to n_0 and less than n. We will prove using the PMI that $P^*(n)$ holds for all natural numbers greater than or equal to n_0, which, by the assumption above, will imply that $P(n)$ holds for all natural numbers greater than or equal to n_0. Indeed, $P^*(n_0)$ holds vacuously, because there are no natural numbers greater than or equal to n_0 and less than n_0. Now suppose that $P^*(k)$ holds for some $k\geq n_0$. To show that $P^*(k+1)$ also holds, it suffices to note first that $P(k+1)$ holds by the starting assumption and the assumption that $P^*(k)$ holds and second that the natural numbers greater than or equal to n_0 and less than $k+1$ are precisely k and all those that are greater than or equal to n_0 are less than k. Thus, P holds for all of them; hence $P^*(k+1)$ holds. This completes the proof.

5.2. Divisibility

(1) (D1) It suffices to note that $b = 1 \times b$.
(D2) Since $0 = a \times 0$ and $a = a \times 1$.
(D3) Assume $a \mid b$. Then there is some integer k such that $b = ak$. However, then $b = (-a)(-k)$ and $-b = -ak = a(-k)$, so $-a \mid b$ and $a \mid -b$.
(D4) Assume $a \mid b$. Then there is an integer k such that $b = ak$. Hence, $bc = (ak)c = a(kc)$, and so $a \mid bc$ since $kc \in \mathbb{Z}$.
(D5) Assume $a \mid b$ and $b \mid c$. Then there are integers k_1 and k_2 such that $b = ak_1$ and $c = bk_2$. Hence, we get $c = (ak_1)k_2 = a(k_1k_2)$. Since $k_1k_2 \in \mathbb{Z}$, we have that $a \mid c$.
(D7) Assume $a \mid b$ and $b \mid a$. Then there are integers k_1 and k_2 such that $b = ak_1$ and $a = bk_2$. Hence, $a = (ak_1)k_2 = a(k_1k_2)$, and since $a \neq 0$, we can divide on both sides with a to obtain $k_1k_2 = 1$. However, since $k_1, k_2 \in \mathbb{Z}$, $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$. This means that $a = b$ or $a = -b$.
(D8) Let $a, b > 0$ and assume $a \mid b$. Then $b = ak$ for some integer k. Note that $k \geq 1$, for otherwise $b \leq 0$. Therefore, since $a \geq 1$ and $k \geq 1$, $ak \geq a$. Hence, $b \geq a$.
(D9) Let $m \neq 0$ and assume $a \mid b$. Then there is an integer k such that $b = ak$. Hence, $mb = m(ak) = (ma)k$, so $ma \mid mb$. For the converse, assume $ma \mid mb$. Then there is a integer k such that $mb = mak$. However, since $m \neq 0$, we can divide with m on both sides to get $b = ak$. Hence, $a \mid b$.
(D10) Assume $a \mid b$ and $c \mid d$. Then there are integers k_1 and k_2 such that $b = ak_1$ and $d = ck_2$. Multiplying these, we get

$$bd = (ak_1)(ck_2) = a(k_1c)k_2 = a(ck_1)k_2 = (ac)(k_1k_2).$$

Hence, since $k_1k_2 \in \mathbb{Z}$, $ac \mid bd$.

(2) Let $b \neq 0$ and suppose $a \mid b$. From $b \neq 0$, we know that $|b| > 0$, so, by (D8), $a \leq |b|$. Hence, b has only finitely many divisors.

(3a) $93 = 93 \cdot 1 + 0$

(3b) $93 = 3 \cdot 31 + 0$

(3c) $93 = 17 \cdot 5 + 8$

(4) Since $1000 = 90 \times 11 + 10$, it follows that there are 90 positive integers less than 1000 that are divisible by 11. However, 9 of these are less than or equal to 100. Hence, there are 81 integers between 100 and 1000 that are divisible by 11.

(5) Every integer is either even or odd, so consider the following two cases:

Case 1: n is even.
In this case, we can write n as $n = 2k$ for some integer k. Hence, $n^2 = 4k^2$ and so, by Theorem 5.2.3, the remainder is 0 when n^2 is divided by 4.

Case 2: n is odd.
Here n can be written as $n = 2k + 1$ for some integer k. Hence, $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, and so, by Theorem 5.2.3, the remainder is 1 when we divide n^2 by 4.

(6a) Let $n \in \mathbb{N}$ and let m be the last digit of n. For the right-to-left direction, assume $2 \mid m$. Now $n = 10k + m$ for some $k \in \mathbb{N}$. However, $2 \mid 10$, and hence $2 \mid 10k$ by (D4). Furthermore, by our assumption, $2 \mid m$, so, by (D6), $2 \mid n$. For the left-to-right direction, assume $2 \mid n$. However, $m = n - 10k$, and since $2 \mid n$ and $2 \mid 10k$, $2 \mid m$ by (D6).

(6b) Let $n \in \mathbb{N}$ and let m be the last two digits of n. For the right-to-left direction, assume $4 \mid m$. Now $n = 100k + m$ for some $k \in \mathbb{N}$. However, $4 \mid 100$, and hence $4 \mid 100k$ by (D4). Furthermore, by our assumption, $4 \mid m$, so $4 \mid n$, by (D6). For the left-to-right direction, assume $4 \mid n$. However, $m = n - 100k$ and since $4 \mid n$ and $4 \mid 100k$, it follows that $4 \mid m$ by (D6).

(6c) Let $n \in \mathbb{N}$ and let m be the last digit of n. For the right-to-left direction, assume $5 \mid m$. Now, $n = 10k + m$ for some $k \in \mathbb{N}$. However, $5 \mid 10$, and hence $5 \mid 10k$ by (D4). Furthermore, by our assumption, $5 \mid m$, so $5 \mid n$, by (D6). For the converse direction, assume $5 \mid n$. However, $m = n - 10k$, and since $5 \mid n$ and $5 \mid 10k$, it follows that $5 \mid m$ by (D6).

(7) Let $m, m+1, \ldots, m+k-1$ be k consecutive integers. If $k \mid m$, we are done, so suppose $k \nmid m$ and write $m = kn + r$, where $0 < r < k$. Now let $c = k - r$. Then $0 < c < k$, too. Therefore, $m + c$ is one of the k consecutive integers. Note that $k \mid m + c$ since $m + c = kn + r + k - r = kn + k = k(n + 1)$. Finally, to show that there is exactly one such c, let $0 \leq d < k$ such that $k \mid m + d$. Then $k \mid (m + d) - (m + c) = d - c$ and $0 \leq |d - c| < k$. Therefore, by (D8), $|d - c| = 0$, i.e. $d = c$.

(8a) Let $n = 2m + 1$. Then $(2m + 1)^2 - 1 = 4m^2 + 4m = 4m(m + 1)$. Note that $m(m + 1)$ is even, i.e. divisible by 2, and hence $4m(m + 1)$ is divisible by 8, by property (D10).

(8b) **Solution 1**. Let $n = 2m + 1$. Then

$$\begin{aligned}
&n^3 + 3n^2 - n - 3 \\
&= (2m+1)^3 + 3(2m+1)^2 - (2m+1) - 3 \\
&= 8m^3 + 12m^2 + 6m + 1 + 12m^2 + 12m + 3 - 2m - 1 - 3 \\
&= 8m^3 + 24m^2 + 16m \\
&= 8m(m^2 + 3m + 2) \\
&= 8m(m+1)(m+2).
\end{aligned}$$

Now, it suffices to note that, by Exercise 7, $m(m + 1)(m + 2)$ is divisible by 2 and by 3; hence it is divisible by 6.

Solution 2. Here is a proof by induction on n, where $n = 2m + 1$. For $n = 1$, $1^3 + 3(1)^2 - 1 - 3 = 0$ and $48 \mid 0$. Our inductive hypothesis is that $48 \mid k^3 + 3k^2 - k - 3$. Note that the next odd number is $k + 2$. To show that $48 \mid (k + 2)^3 + 3(k + 2)^2 - (k + 2) - 3$, we first prove that

$$48 \mid (k+2)^3 + 3(k+2)^2 - (k+2) - 3 - (k^3 + 3k^2 - k - 3).$$

Now,

$$\begin{aligned}
&(k+2)^3 + 3(k+2)^2 - (k+2) - 3 - (k^3 + 3k^2 - k - 3) \\
&= k^3 + 6k^2 + 12k + 8 + 3k^2 + 12k + 12 - k - 2 - 3 - k^3 - 3k^2 + k + 3 \\
&= 6k^2 + 24k + 18 \\
&= 6(k^2 + 4k + 3).
\end{aligned}$$

If we can show that $8 \mid k^2 + 4k + 3$, we are done since then, by (D10), $48 \mid 6(k^2 + 4k + 3)$. To show that $8 \mid k^2 + 4k + 3$, we use induction on k. If $k = 1$, $1^2 + 4(1) + 3 = 8$ and $8 \mid 8$. Now assume $8 \mid m^2 + 4m + 3$. For $k = m + 2$,

$$\begin{aligned}
(m+2)^2 + 4(m+2) + 3 &= m^2 + 4m + 4 + 4m + 8 + 3 \\
&= m^2 + 4m + 3 + 4(m+1) + 8.
\end{aligned}$$

However, since m is odd, $m = 2c + 1$ for some $c \in \mathbb{N}$. Hence,

$$\begin{aligned}
m^2 + 4m + 3 + 4(m+1) + 8 &= m^2 + 4m + 3 + 4(2c+2) + 8 \\
&= m^2 + 4m + 3 + 8(c+1) + 8.
\end{aligned}$$

By our inductive hypothesis, $8 \mid m^2 + 4m + 3$. We also know that $8 \mid 8$, so $8 \mid 8(c + 1)$ by (D4). Hence, $8 \mid m^2 + 4m + 3 + 8(c + 1) + 8$ by (D6). We have thus shown that $8 \mid (k^2 + 4k + 3)$, as required. We thus now know from (D6) and the inductive hypothesis that

$$48 \mid (k+2)^3 + 3(k+2)^2 - (k+2) - 3 - (k^3 + 3k^2 - k - 3) + (k^3 + 3k^2 - k - 3)$$

and so $48 \mid (k + 2)^3 + 3(k + 2)^2 - (k + 2) - 3$.

(8c) **Solution 1.** Note that $3^{2n} - 1 = (3^n - 1)(3^n + 1)$ and $3^n - 1$ and $3^n + 1$ are two consecutive even numbers, so one of them is also divisible by 4. Therefore, their product is divisible by $2.4 = 8$.
Solution 2. Here is a proof by induction on n. If $n = 0$, then $3^{2\cdot 0} - 1 = 1 - 1 = 0$ and $8 \mid 0$. Our inductive hypothesis is that $8 \mid 3^{2k} - 1$. Now, for $k + 1$,

$$\begin{aligned} 3^{2(k+1)} - 1 &= 3^{2k+2} - 1 \\ &= 3^{2k} \cdot 3^2 - 1 \\ &= 3^{2k} \cdot 3^2 - 3^2 + 8 \\ &= 3^2(3^{2k} - 1) + 8. \end{aligned}$$

However, by the inductive hypothesis, $8 \mid 3^{2k} - 1$, so, by (D4), $8 \mid 3^2(3^{2k} - 1)$. Furthermore, by (D2), $8 \mid 8$ and hence $8 \mid 3^2(3^{2k} - 1) + 8$, by (D6), which means that $8 \mid 3^{2(k+1)} - 1$.

(8d) We proceed by induction on n. For $n = 0$, $4^0 + 15(0) - 1 = 1 - 1 = 0$ and $9 \mid 0$. Our inductive hypothesis is that $9 \mid 4^k + 15k - 1$. Now, we first show that

$$9 \mid 4^{k+1} + 15(k + 1) - 1 - (4^k + 15k - 1).$$

Expanding, grouping, and simplifying terms, we find

$$\begin{aligned} &4^{k+1} + 15(k + 1) - 1 - (4^k + 15k - 1) \\ &= 4 \cdot 4^k + 15k + 15 - 1 - 4^k - 15k + 1 \\ &= 4 \cdot 4^k - 4^k + 15 \\ &= 3 \cdot 4^k + 15 \\ &= 3(4^k + 5). \end{aligned}$$

We now claim that $3 \mid 4^k + 5$. To see this, use induction on k. If $k = 0$, $4^0 + 5 = 1 + 5 = 6$ and $3 \mid 6$. Assume $3 \mid 4^m + 5$. Now, for $k = m + 1$,

$$4^{m+1} + 5 = 4 \cdot 4^m + 5 = 4 \cdot 4^m + 20 - 15 = 4(4^m + 5) - 15.$$

However, by the inductive hypothesis, $3 \mid 4^m + 5$, and hence $3 \mid 4(4^m + 5)$, by (D4). Furthermore, $3 \mid 15$ and hence $3 \mid 4(4^m + 5) - 15$, by (D6). Hence, $3 \mid 4^{m+1} + 5$, as required. We thus have $3 \mid 4^k + 5$, and therefore, since $3 \mid 3$, $9 \mid 3(4^k + 5)$ by (D10). Thus, by (D6) and the inductive hypothesis,

$$9 \mid 4^{k+1} + 15(k + 1) - 1 - (4^k + 15k - 1) + (4^k + 15k - 1),$$

and so $9 \mid 4^{k+1} + 15(k + 1) - 1$.

(8e) We proceed by induction on n. For $n = 0$, $2^{0+2} \cdot 3^0 + 5(0) - 4 = 4 - 4 = 0$ and $25 \mid 0$. Our inductive hypothesis is that

$$25 \mid 2^{k+2} \cdot 3^k + 5k - 4.$$

Now, as in Exercise 8(d), we first show that

$$25 \mid 2^{(k+1)+2} \cdot 3^{k+1} + 5(k + 1) - 4 - (2^{k+2} \cdot 3^k + 5k - 4).$$

Expanding, grouping and simplifying, we get

$$\begin{aligned} &2^{(k+1)+2} \cdot 3^{k+1} + 5(k + 1) - 4 - (2^{k+2} \cdot 3^k + 5k - 4) \\ &= 2^{k+3} \cdot 3^{k+1} + 5k + 5 - 4 - 2^{k+2} \cdot 3^k - 5k + 4 \\ &= 2^3 \cdot 2^k \cdot 3 \cdot 3^k - 2^2 \cdot 2^k \cdot 3^k + 5 \\ &= 24 \cdot 2^k \cdot 3^k - 4 \cdot 2^k \cdot 3^k + 5 \\ &= 20 \cdot 2^k \cdot 3^k + 5 \\ &= 5(4 \cdot 2^k \cdot 3^k + 1). \end{aligned}$$

We now claim that $5 \mid 4 \cdot 2^k \cdot 3^k + 1$. To see this, use induction on k. If $k = 0$, $4 \cdot 2^0 \cdot 3^0 + 1 = 4 + 1 = 5$ and $5 \mid 5$. Now assume $5 \mid 4 \cdot 2^m \cdot 3^m + 1$. For $k = m + 1$,

$$\begin{aligned} 4 \cdot 2^{m+1}3^{m+1} + 1 &= 4 \cdot 2 \cdot 2^m \cdot 3 \cdot 3^m + 1 \\ &= 24 \cdot 2^m \cdot 3^m + 1 \\ &= 24 \cdot 2^m \cdot 3^m + 6 - 1 \\ &= 6(4 \cdot 2^m \cdot 3^m + 1) - 5. \end{aligned}$$

However, by our inductive hypothesis, $5 \mid 4 \cdot 2^m \cdot 3^m + 1$, so, by (D4), $5 \mid 6(4 \cdot 2^m \cdot 3^m + 1)$. We also know that $5 \mid -5$, so by (D6), $5 \mid 6(4 \cdot 2^m \cdot 3^m + 1) - 5$. Hence, $5 \mid 4 \cdot 2^{m+1}3^{m+1} + 1$. We can thus now conclude that $5 \mid 4 \cdot 2^k \cdot 3^k + 1$, and hence $25 \mid 5(4 \cdot 2^k 3^k + 1)$ by (D10), since $5 \mid 5$. We thus know from (D6) and the inductive hypothesis that

$$25 \mid 2^{(k+1)+2} \cdot 3^{k+1} + 5(k+1) - 4 - (2^{k+2} \cdot 3^k + 5k - 4) + (2^{k+2} \cdot 3^k + 5k - 4),$$

which means that $25 \mid 2^{(k+1)+2} \cdot 3^{k+1} + 5(k+1) - 4$.

(9) Let $m, n > 0$ and assume $m \mid n$. Then there is some $k \in \mathbb{Z}^+$ such that $n = km$. Hence, $2^n = 2^{km}$, so $2^n - 1 = 2^{km} - 1$. However,

$$2^{km} - 1 = (2^m - 1)((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1),$$

which means that $2^m - 1 \mid 2^n - 1$.

(10a) $\gcd(24, 42) = 6$

(10b) $\gcd(24, -35) = 1$

(10c) $\gcd(-24, -72) = 24$

(11) Assume $\gcd(a, 4) = 2$ and $\gcd(b, 4) = 2$. Note that a and b are both even but not divisible by 4, so we can express a and b as follows: $a = 4 + 2k_1$ and $b = 4 + 2k_2$ for some odd integers k_1 and k_2. Hence,

$$a + b = 4 + 2k_1 + 4 + 2k_2 = 8 + 2(k_1 + k_2).$$

However, since k_1 and k_2 are odd, $k_1 + k_2$ is even, so $k_1 + k_2 = 2c$ for some integer c. We thus have that

$$a + b = 8 + 2(2c) = 8 + 4c.$$

Now, $4 \mid 4$, so, by (D4), $4 \mid 4c$. Hence, since $4 \mid 8$, $4 \mid a + b$ by (D6), so by (GCD2), $\gcd(a + b, 4) = |4| = 4$.

(12) Note that $k^n - a = k^n - b^n + b^n - a$ and $k - b \mid k^n - b^n$; hence $k - b \mid b^n - a$ for any $k \neq b$. Since $k - b > b^n - a$ for large enough values of k, it follows that $b^n - a = 0$.

(13) (GCD1) Immediate from the definition of gcd.
(GCD2) Assume $a \mid b$. Then $|a| \mid b$ and any divisor of a is not greater than $|a|$; hence $\gcd(a, b) = |a|$.
(GCD3) We know that $\gcd(a, b) \mid a$ and $\gcd(a, -b) \mid b$. Hence, $\gcd(a, -b)$ is a common divisor of a and b, i.e. $\gcd(a, -b) \mid \gcd(a, b)$. Likewise, $\gcd(a, b) \mid \gcd(a, -b)$, so $\gcd(a, b) = \gcd(a, -b)$ by (D7). The other equalities can be proved analogously.
(GCD7) Let $s_1 = \gcd(\gcd(a, b), c)$ and $s_2 = \gcd(a, \gcd(b, c))$. Then $s_1 \mid \gcd(a, b)$ and hence $s_1 \mid a$ and $s_1 \mid b$. Furthermore, $s_1 \mid \gcd(b, c)$ since $s_1 \mid c$. Therefore, by (GCD8), $s_1 \mid s_2$. Likewise, we show that $s_2 \mid s_1$, so $s_1 = s_2$ by (D7).
(GCD8) Let d be any common divisor of a and b. Then $a = k_1 d$ and $b = k_2 d$ for some $k_1, k_2 \in \mathbb{Z}$. Now, $\gcd(a, b) = ua + vb = (uk_1 + vk_2)d$ for some $u, v \in \mathbb{Z}$. Hence, $d \mid \gcd(a, b)$.

(14) Suppose $\gcd(x, y) = 3$. Then $3 \mid x$ and $3 \mid y$, and hence $3 \mid x + y$ by (D6). Hence, $3 \mid 1000$, which is not true. Therefore, $\gcd(x, y) \neq 3$.

(15a) By induction on k.

(15b) Directly from the definition of $\gcd(a_1, a_2, \ldots, a_k)$.

(16) The proof is by induction on k. For $k = 2$, the result follows from Theorem 5.2.5. Assume $\gcd(a_1, \ldots, a_n)$ exists and is unique and that $\gcd(a_1, \ldots, a_n) = u_1a_1 + \cdots + u_na_n$. Now, for $n = k + 1$,

$$\begin{aligned}\gcd(a_1, \ldots, a_n, a_{n+1}) &= \gcd(a_{n+1}, a_1, \ldots, a_n)\\ &= \gcd(a_{n+1}, \gcd(a_1, \ldots, a_n))\\ &= v_1a_{n+1} + v_2 \gcd(a_1, \ldots, a_n)\\ &= v_1a_{n+1} + v_2u_1a_1 + \cdots + v_2u_na_n,\end{aligned}$$

where the first equality follows from Exercise 15(a), the second equality from Exercise 15(b), the third equality from Theorem 5.2.5 and the last equality from the inductive hypothesis. The fact that $\gcd(a_1, \ldots, a_n, a_{n+1})$ exists and is unique follows from the third equality, Theorem 5.2.5 and the inductive hypothesis. To show that $\gcd(a_1, \ldots, a_k)$ is the least positive integer that can be represented in this way, suppose $d < \gcd(a_1, \ldots, a_k)$ and $d = u_1a_1 + u_2a_2 + \cdots u_ka_k = \gcd(a_1, \ldots, a_k)$, which means that $d < d$, a contradiction.

(17) We proceed by induction on k. For $k = 2$, the claim follows from (GCD8). Our inductive hypothesis is that every common divisor of $a_1, a_2, \ldots, a_n$ divides $\gcd(a_1, a_2, \ldots, a_n)$. For $k = n + 1$, let d be a common divisor of $a_1, a_2, \ldots, a_n, a_{n+1}$. Now,

$$\begin{aligned}&\gcd(a_1, a_2, \ldots, a_n, a_{n+1})\\ &= \gcd(a_{n+1}, a_1, a_2, \ldots, a_n)\\ &= \gcd(a_{n+1}, \gcd(a_1, \gcd(a_2, \ldots, \gcd(a_{n-1}, a_n))))\\ &= \gcd(a_{n+1}, \gcd(a_1, a_2, \ldots, a_n)).\end{aligned}$$

Here the first equality follows from Exercise 15(b), and the second and third equalities follow from Exercise 15(a). Using Theorem 5.2.5, we have

$$\gcd(a_{n+1}, \gcd(a_1, \ldots, a_n)) = ua_{n+1} + v \gcd(a_1, \ldots, a_n)$$

for some integers u and v. However, by the inductive hypothesis, $d \mid \gcd(a_1, \ldots, a_n)$. We also have that $d \mid a_{n+1}$. Hence, $d \mid ua_{n+1} + v \gcd(a_1, \ldots, a_n)$ by (D6), so $d \mid \gcd(a_1, a_2, \ldots, a_n, a_{n+1})$.

(18) By induction on k.

(19) Let $c = \gcd(a, b)$ and $d = \gcd(3a + 5b, 11a + 18b)$; hence $c \le d$. On the other hand, $d \mid 4(3a + 5b) - (11a + 18b) = a + 2b$. Therefore, $d \mid 3(a + 2b) - (3a + 5b) = b$ and hence $d \mid (a + 2b) - 2b = a$, so $d \le c$.

(20) Let $\gcd(a, b, c) = d$ and $\gcd\left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right) = e$. Then d is odd, and hence $\gcd(2, d) = 1$, so $1 = 2u + bv$ for some integers u, v. Then $\frac{a+b}{2} = \frac{a+b}{2}(2u + bv) = (a + b)u + bv\frac{a+b}{2}$ and d divides each of $(a + b)u$ and $bv\frac{a+b}{2}$; hence $d \mid \frac{a+b}{2}$ (see also property (RP2) of Theorem 5.4.1.) Likewise, $d \mid \frac{b+c}{2}$ and $d \mid \frac{c+a}{2}$, and therefore $d \le e$. On the other hand, $e \mid \frac{a+b}{2} + \frac{a+c}{2} = a + \frac{b+c}{2}$, and hence $e \mid a + \frac{b+c}{2} - \frac{b+c}{2} = a$. Likewise, $e \mid b$ and $e \mid c$, and hence $e \le d$. Therefore, $d = e$.

(21) Let $c = \gcd(a, b)$ and $d = \gcd(a + bc, a + b(c - 1))$. Then, by (D6), $c \mid a + bc$ and $c \mid a + b(c - 1)$, and hence $c \le d$. On the other hand, $d \mid (a + bc) - (a + b(c - 1)) = b$. Therefore, $d \mid bc$, and hence $d \mid (a + bc) - bc = a$. Thus, $d \le c$ and hence $c = d$.

(22) Let $d = \gcd(21n + 4, 14n + 3)$. Then, by (D6), $d \mid 3(14n + 3) - 2(21n + 4) = 1$.

(24a) Let the sides of the right-angled triangle be a, b, c, where c is the hypotenuse. Then $a^2 + b^2 = c^2$. Note that for every integer m, the remainder of m^2 when divided by 3 is either 0, if $3 \mid m$, or 1, if $3 \nmid m$. Therefore, if both a and b are not divisible by 3, then the remainder of c^2 when divided by 3 must be $1 + 1 = 2$, which is impossible.

(24b) Likewise, note that for every integer m, the remainder of m^2 when divided by 5 is either 0, if $5 \mid m$, or 1 or 4, if $5 \nmid m$ (check this for all possible remainders of m when divided by 5). Therefore, if neither of a, b nor c is divisible by 5, then the remainder of c^2 when divided by 5 must be $1 + 1 = 2$ or $4 + 4 - 5 = 3$, which is impossible.

5.3. Computing greatest common divisors. Least common multiples

(1) We are given that $a = bq + r$ for some $q \in \mathbb{N}$. Then $r = a - bq$. Now, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, and hence $\gcd(a, b) \mid r$ by (D4) and (D6). However, $\gcd(a, b) \mid \gcd(b, r)$ by (GCD8). Likewise, since $\gcd(b, r) \mid b$ and $\gcd(b, r) \mid r$, $\gcd(b, r) \mid a$ by (D4) and (D6). Then $\gcd(b, r) \mid \gcd(a, b)$ by (GCD8). Hence, by (D7), $\gcd(a, b) = \gcd(b, r)$.

(2a) Set $X := 112$ and $Y := 70$.

Divide X by Y with a remainder: $112 = 1 \cdot 70 + 42$.
The remainder is not 0, hence $X := 70$ and $Y := 42$.
Divide X by Y with a remainder: $70 := 1 \cdot 42 + 28$.
The remainder is not 0, hence $X := 42$ and $Y := 28$.
Divide X by Y with a remainder: $42 = 1 \cdot 28 + 14$.
The remainder is not 0, hence $X := 28$ and $Y := 14$.
Divide X by Y with a remainder: $28 = 2 \cdot 14 + 0$.
The remainder is 0, so $\gcd(70, 112) = 14$.

(2b) Set $X := 801$ and $Y := 258$.

Divide X by Y with a remainder: $801 = 3 \cdot 258 + 27$.
The remainder is not 0, hence $X := 258$ and $Y := 27$.
Divide X by Y with a remainder: $258 := 9 \cdot 27 + 15$.
The remainder is not 0, hence $X := 27$ and $Y := 15$.
Divide X by Y with a remainder: $27 = 1 \cdot 15 + 12$.
The remainder is not 0, hence $X := 15$ and $Y := 12$.
Divide X by Y with a remainder: $15 = 1 \cdot 12 + 3$.
The remainder is not 0, hence $X := 12$ and $Y := 3$.
Divide X by Y with a remainder: $12 = 4 \cdot 3 + 0$.
The remainder is 0, so $\gcd(801, 258) = 3$.

(2c) Set $X := 7469$ and $Y := 2464$.

Divide X by Y with a remainder: $7469 = 3 \cdot 2464 + 77$.
The remainder is not 0, hence $X := 2464$ and $Y := 77$.
Divide X by Y with a remainder: $2464 := 32 \cdot 77 + 0$.
The remainder is 0, so $\gcd(7469, 2464) = 77$.

(2d) Set $X := 4001$ and $Y := 2689$.

Divide X by Y with a remainder: $4001 = 1 \cdot 2689 + 1312$.
The remainder is not 0, hence $X := 2689$ and $Y := 1312$.
Divide X by Y with a remainder: $2689 := 2 \cdot 1312 + 65$.
The remainder is not 0, hence $X := 1312$ and $Y := 65$.
Divide X by Y with a remainder: $1312 = 20 \cdot 65 + 12$.

The remainder is not 0, hence $X := 65$ and $Y := 12$.
Divide X by Y with a remainder: $65 = 5 \cdot 12 + 5$.
The remainder is not 0, hence $X := 12$ and $Y := 5$.
Divide X by Y with a remainder: $12 = 2 \cdot 5 + 2$.
The remainder is not 0, hence $X := 5$ and $Y := 2$.
Divide X by Y with a remainder: $5 := 2 \cdot 2 + 1$.
The remainder is not 0, hence $X := 2$ and $Y := 1$.
Divide X by Y with a remainder: $2 = 2 \cdot 1 + 0$.
The remainder is 0, so $\gcd(2689, 4001) = 1$.

(3a) Let $n, n+1$ and $n+2$ be three consecutive integers. Then 2 divides at least one of them, and hence, by (D4), $2 \mid n(n+1)(n+2)$. Likewise, 3 divides at least (in fact, exactly) one of them. Hence, $3 \mid n(n+1)(n+2)$. We thus have that $n(n+1)(n+2)$ is a common multiple of 2 and 3 and $\operatorname{lcm}(2,3) = 6$, so, by Theorem 5.3.6, $6 \mid n(n+1)(n+2)$.

(3b) Let $n, n+1, n+2$ and $n+3$ be four consecutive integers. Then 2 of them are even and 4 divides exactly one of them, while 2 divides the other. Hence, by (D10), $2 \times 4 = 8$ divides the product of these 4 integers. Besides, 3 divides at least one of them and $\operatorname{lcm}(8,3) = 24$. We therefore have, by Theorem 5.3.6, that $24 \mid n(n+1)(n+2)(n+3)$.

(3c) Likewise, using the previous exercise and the fact that one of any 5 consecutive integers is divisible by 5.

(4a) Factorizing $n^3 - n$ gives $n^3 - n = n(n^2-1) = n(n-1)(n+1)$, and so, since we have a product of 3 consecutive integers, $6 \mid n^3 - n$ by 3(a).

(4b) Factorizing $n^5 - n$ gives $n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = (n-1)n(n+1)(n^2+1)$. Now, $(n-1)n(n+1)$ is a product of three consecutive integers. Then $6 \mid (n-1)n(n+1)$, by 3(a), and hence $6 \mid n^5 - n$ by (D4). Besides, $5 \mid n^5 - n$, which can be shown by considering the possible cases of remainders of n when divided by 5:

Case 1: $n = 5k$. Then $5 \mid n$, so $5 \mid n^5 - n$ by (D4) and (D6).

Case 2: $n = 5k+1$. Then $n - 1 = 5k + 1 - 1 = 5k$, so $5 \mid n - 1$. Hence, $5 \mid n^5 - n$ by (D4).

Case 3: $n = 5k+2$. Then we have $n^2 = (5k+2)^2 = 25k^2 + 10k + 4$, so $n^2 + 1 = 25k^2 + 10k + 5 = 5(5k^2 + 2k + 1)$. Then $5 \mid n^2 + 1$, and hence, by (D4), $5 \mid n^5 - n$.

Case 4: $n = 5k+3$. Then $n^2 = (5k+3)^2 = 25k^2 + 30k + 9$, so $n^2 + 1 = 25k^2 + 30k + 10 = 5(5k^2 + 6k + 2)$. Hence, $5 \mid n^2 + 1$, so $5 \mid n^5 - n$ by (D4).

Case 5: $n = 5k+4$. Then $n + 1 = 5k + 5 = 5(k+1)$, so $5 \mid n + 1$. Hence, by (D4), $5 \mid n^5 - n$. Now, since $\operatorname{lcm}(5,6) = 30$, all we have is that $30 \mid n^5 - n$, by Theorem 5.3.6.

(4c) Factorizing $n^5 - 5n^3 + 4n$ yields

$$\begin{aligned} n^5 - 5n^3 + 4n &= n(n^4 - 5n + 4) \\ &= n(n^2-1)(n^2-4) \\ &= n(n-1)(n+1)(n-2)(n+2) \\ &= (n-2)(n-1)n(n+1)(n+2). \end{aligned}$$

We thus have a product of 5 consecutive integers; hence, by 3(c), $120 \mid n^5 - 5n^3 + 4n$.

(5) (LCM1) Directly from the definition of lcm.

(LCM2) Assume $a \mid b$. Now, we also know that $b \mid b$, so b is a common multiple of a and b. Hence, by Theorem 5.3.6, $\text{lcm}(a, b) \mid b$, but $b \mid \text{lcm}(a, b)$, so, by (D7), $\text{lcm}(a, b) = -b$ or $\text{lcm}(a, b) = b$. It thus follows from the definition of the absolute value that $\text{lcm}(a, b) = |b|$.
(LCM3) We know that $b \mid \text{lcm}(a, b)$, so $-b \mid \text{lcm}(a, b)$ by (D3). Also, $a \mid \text{lcm}(a, b)$, which means that $\text{lcm}(a, b)$ is a common multiple of a and $-b$. Hence, by Theorem 5.3.6, $\text{lcm}(a, -b) \mid \text{lcm}(a, b)$. Likewise, $-b \mid \text{lcm}(a, -b)$, so $b \mid \text{lcm}(a, -b)$ by (D3). We also have $a \mid \text{lcm}(a, -b)$. Hence, $\text{lcm}(a, -b)$ is a common multiple of a and b, so $\text{lcm}(a, b) \mid \text{lcm}(a, -b)$ by Theorem 5.3.6. We thus have that $\text{lcm}(a, b) = \text{lcm}(a, -b)$ by (D7). The other equalities can be proved in a similar way.
(LCM4) First, we know that $a \mid \text{lcm}(a, b)$, $b \mid \text{lcm}(a, b)$ and $n \mid |n|$, so $an \mid |n|\text{lcm}(a, b)$ and $bn \mid |n|\text{lcm}(a, b)$ by (D10). Hence, by Theorem 5.3.6, $\text{lcm}(an, bn) \mid |n|\text{lcm}(a, b)$. Now, we also know that $an \mid \text{lcm}(an, bn)$ and $bn \mid \text{lcm}(an, bn)$, which means that $\text{lcm}(an, bn) = (an)k_1$ and $\text{lcm}(an, bn) = (bn)k_2$ for some integers k_1 and k_2. However, then $\frac{\text{lcm}(an, bn)}{|n|} = ac_1$ and $\frac{\text{lcm}(an, bn)}{|n|} = bc_2$, where $c_1 = k_1$ and $c_2 = k_2$ or $c_1 = -k_1$ and $c_2 = -k_2$. Hence, $a \mid \frac{\text{lcm}(an, bn)}{|n|}$ and $b \mid \frac{\text{lcm}(an, bn)}{|n|}$, so $\text{lcm}(a, b) \mid \frac{\text{lcm}(an, bn)}{|n|}$ by Theorem 5.3.6. Therefore, by (D9), $|n|\text{lcm}(a, b) \mid \text{lcm}(an, bn)$. We thus have $|n|\text{lcm}(a, b) = \text{lcm}(an, bn)$ by (D7).
(LCM5) We know that $\text{lcm}(a, b) \mid \text{lcm}(\text{lcm}(a, b), c)$; hence, since $a \mid \text{lcm}(a, b)$ and $b \mid \text{lcm}(a, b)$, $a \mid \text{lcm}(\text{lcm}(a, b), c)$ and $b \mid \text{lcm}(\text{lcm}(a, b), c)$ by (D5). However, we also have that $c \mid \text{lcm}(\text{lcm}(a, b), c)$, so $\text{lcm}(\text{lcm}(a, b), c)$ is a common multiple of b and c. Hence, by Theorem 5.3.6, $\text{lcm}(b, c) \mid \text{lcm}(\text{lcm}(a, b), c)$. This means that $\text{lcm}(\text{lcm}(a, b), c)$ is a common multiple of a and $\text{lcm}(b, c)$. Thus, $\text{lcm}(a, \text{lcm}(b, c)) \mid \text{lcm}(\text{lcm}(a, b), c)$ by Theorem 5.3.6. Similarly, we have $\text{lcm}(\text{lcm}(a, b), c) \mid \text{lcm}(a, \text{lcm}(b, c))$. Hence, $\text{lcm}(\text{lcm}(a, b), c) = \text{lcm}(a, \text{lcm}(b, c))$ from (D7).

(6a) Using the Euclidean algorithm, we find $\gcd(70, 71) = 1$, so $\text{lcm}(70, 71) = \frac{70 \cdot 71}{1} = 4970$.

(6b) Using the Euclidean algorithm, we find $\gcd(630, 1344) = 42$, so $\text{lcm}(630, 1344) = \frac{630 \cdot 1344}{42} = 20\,160$.

(7) Using the Euclidean algorithm, we get that $\gcd(n, n + 1) = 1$. Hence, by Theorem 5.3.7, $\text{lcm}(n, n + 1) = n(n + 1) = n^2 + n$.

(8) Let m and n be natural numbers such that $\gcd(m, n) = \text{lcm}(m, n)$. We know that $\gcd(m, n) \mid m$ and $\gcd(m, n) \mid n$, which means that $\text{lcm}(m, n) \mid m$ and $\text{lcm}(m, n) \mid n$. However, $m \mid \text{lcm}(m, n)$ and $n \mid \text{lcm}(m, n)$, so, since m, n and $\text{lcm}(m, n)$ are natural numbers, $\text{lcm}(m, n) = m$ and $\text{lcm}(m, n) = n$ by (D7). Hence, $m = n$.

(9) By induction on k.

(10) Note that, by Theorem 5.3.7, $mn = \gcd(m, n)\text{lcm}(m, n)$, so $mn = 1000$. The only possible such pairs are 10 and 100 or 20 and 50.

(11) Since $\{n + 1, n + 2, \ldots, 2n\} \subset \{1, 2, 3, \ldots, 2n\}$, we have that $\text{lcm}(n + 1, n + 2, \ldots, 2n) \leq \text{lcm}(1, 2, 3, \ldots, 2n)$. Further, note that every integer in $\{1, 2, 3, \ldots, n\}$ has a multiple in $\{n + 1, n + 2, \ldots, 2n\}$ (why?), so every common multiple of $\{n + 1, n + 2, \ldots, 2n\}$ is also a common multiple of $\{1, 2, 3, \ldots, n\}$, and hence a common multiple of $\{1, 2, 3, \ldots, n, n + 1, \ldots, 2n\}$. Therefore, $\text{lcm}(1, 2, 3, \ldots, 2n) \leq \text{lcm}(n + 1, n + 2, \ldots, 2n)$.

(12) Likewise. It suffices to note that every integer in $\{1, 2, 3, \ldots, m\}$ has a multiple in $\{n, n + 1, \ldots, n + m - 1\}$.

(13) In fact, we can prove a stronger claim: $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$. Indeed, first note that if $d \mid k$, then $2^d - 1 \mid 2^k - 1$ because if $k = dq$, then $2^k - 1 = 2^{dq} - 1 = (2^d)^q - 1 = (2^d - 1)((2^d)^{q-1} + \cdots + 2^d + 1)$. Therefore, $2^{\gcd(m, n)} - 1 \mid 2^m - 1$ and $2^{\gcd(m, n)} - 1 \mid 2^n - 1$, and hence $2^{\gcd(m, n)} - 1 \leq \gcd(2^m - 1, 2^n - 1)$. For the converse, suppose $m < n$ and let $n = mq + r$ be the result of division of n by m with a remainder. Then $2^n - 1 = 2^{mq}2^r - 1 = 2^{mq}2^r - 2^r + 2^r - 1 = 2^r(2^{mq} - 1) + 2^r - 1$, so $(2^n - 1) - 2^r((2^m)^q - 1) = 2^r - 1$. Therefore, every common divisor of $(2^n - 1)$ and $(2^m - 1)$ must divide $2^r - 1$. Now, following Euclid's algorithm for computing $\gcd(m, n)$ and applying this argument repeatedly for every step of the application of that algorithm, we eventually find that every common divisor of $(2^n - 1)$ and $(2^m - 1)$ must divide $2^{\gcd(m, n)} - 1$; hence $\gcd(2^m - 1, 2^n - 1) \leq 2^{\gcd(m, n)} - 1$.

5.4. Prime numbers. The fundamental theorem of arithmetic

(1a) There are infinitely many such triples: pick three primes p, q and r and then generate the products pq, pr and qr. These integers are relatively prime, but no two of them are relatively prime. For example, let $p = 2$, $q = 3$ and $r = 5$. Then $pq = 6$, $pr = 10$ and $qr = 15$.

(1b) Likewise, pick four primes p, q, r and s, and then generate the products pqr, pqs, qrs and prs. These integers are relatively prime, but no three of them are relatively prime. For example, let $p = 2$, $q = 3$, $r = 5$ and $s = 7$; then we get 30, 70, 42 and 105.

(1c) Here is a general scheme for constructing such quadruples: take 6 different primes, p_{ij}, where $i, j \in \{1, 2, 3, 4\}$ and $i < j$. Then define the integers a_1, a_2, a_3, a_4 where each a_i is the product of the 3 primes of the type p_{ij} or p_{ji}. Then for any $i, j \in \{1, 2, 3, 4\}$, where $i < j$, we have that p_{ij} is a common divisor of a_i and a_j. On the other hand, none of p_{ij} divides any 3 of these integers.

(2) Let S be a set of 5 consecutive integers. First, note that any common divisor of any two of these integers is at most 4. Now, at most 3 of these integers are even. Of the odd ones, at most one is divisible by 3. Then the other odd integer must be relatively prime with the rest.

(3a) $128 = 2^7$

(3b) $129 = 3 \times 43$

(3c) $728 = 2^3 \times 7 \times 13$

(3d) $1599 = 3 \times 13 \times 41$

(3e) $8532 = 2^2 \times 3^3 \times 79$

(4) Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ be the decompositions of m and n in products of primes, where $p_1, p_2, \ldots, p_k$ are different and some of the α's and β's can be 0. Then

$$\begin{aligned}\gcd(m, n) &= \gcd(p_1^{\alpha_1} \cdots p_k^{\alpha_k}, p_1^{\beta_1} \cdots p_k^{\beta_k}) \\ &= p_1^{\gamma_1} \cdots p_k^{\gamma_k} \gcd(p_1^{\alpha_1 - \gamma_1} \cdots p_k^{\alpha_k - \gamma_k}, p_1^{\beta_1 - \gamma_1} \cdots p_k^{\beta_k - \gamma_k}),\end{aligned}$$

where $\gamma_i = \min(\alpha_i, \beta_i)$. We now claim that

$$\gcd(p_1^{\alpha_1 - \gamma_1} \cdots p_k^{\alpha_k - \gamma_k}, p_1^{\beta_1 - \gamma_1} \cdots p_k^{\beta_k - \gamma_k}) = 1.$$

To see this, let $d > 1$ and assume d is a common divisor of $p_1^{\alpha_1 - \gamma_1} \cdots p_k^{\alpha_k - \gamma_k}$ and $p_1^{\beta_1 - \gamma_1} \cdots p_k^{\beta_k - \gamma_k}$. However, since $d > 1$, it has a prime divisor q and, by (D5), $q \mid p_1^{\alpha_1 - \gamma_1} \cdots p_k^{\alpha_k - \gamma_k}$ and $q \mid p_1^{\beta_1 - \gamma_1} \cdots p_k^{\beta_k - \gamma_k}$. This means that $q \mid p_i^{\alpha_i - \gamma_i}$ and $q \mid p_j^{\beta_j - \gamma_j}$ for some i and j. If $i = j$, then $\alpha_i - \gamma_i = 0$ or $\beta_j - \gamma_j = 0$, which means that $q \mid 1$, a contradiction. On the other hand, if $i \neq j$, we have a contradiction again, since $\gcd(p_i^{\alpha_i - \gamma_i}, p_j^{\beta_j - \gamma_j}) = 1$. We thus have

$$\gcd(m, n) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where $\gamma_i = \min(\alpha_i, \beta_i)$.
Now, we can show that $\operatorname{lcm}(m, n) = p_1^{\delta_1} \cdots p_k^{\delta_k}$, where $\delta_i = \max(\alpha_i, \beta_i)$ by using Theorem 5.3.7 and the result for $\gcd(m, n)$.

(5a) $60 = 2^2 \times 3^1 \times 5$ and $144 = 2^4 \times 3^2 \times 5^0$, so we get $\gcd(60, 144) = 2^2 \times 3^1 \times 5^0 = 12$ and $\operatorname{lcm}(60, 144) = 2^4 \times 3^2 \times 5 = 730$.

(5b) We have that $728 = 2^3 \times 3^0 \times 7^1 \times 13^1 \times 79^0$ and $8532 = 2^2 \times 3^3 \times 7^0 \times 13^0 \times 79^1$, so $\gcd(728, 8532) = 2^2 \times 3^0 \times 7^0 \times 13^0 \times 79^0 = 4$ and $\operatorname{lcm}(728, 8532) = 2^3 \times 3^3 \times 7 \times 13 \times 79 = 1\,552\,824$.

(6a) First, note that p and q are not divisible by 3, so each of them leaves a remainder 1 or 2 when divided by 3. If they leave the same remainder, then $3 \mid p - q$. If they leave different remainders, then $3 \mid p + q$.

(6b) First, by (a) and (D4), $3 \mid p^2 - q^2$. Since $24 = \text{lcm}(3, 8)$, it remains to show that $8 \mid p^2 - q^2 = (p - q)(p + q)$. Since p and q primes are greater than 3 and prime, they are both odd; hence $(p - q)$ and $(p + q)$ are both even. Further, p and q leave remainders 1 or 3 when divided by 4. If they leave the same remainder, then $4 \mid p - q$. If they leave different remainders, then $4 \mid p + q$. In both cases, the product is divisible by $2 \times 4 = 8$.

(7) Let p be a prime such that $0 < k < p$. Now,

$$\begin{aligned}\binom{p}{k} &= \frac{p!}{k!(p-k)!} \\ &= \frac{p \times (p-1) \times \cdots \times (p-k) \times (p-k-1) \times \cdots \times 2 \times 1}{k \times (k-1) \times \cdots \times 2 \times 1 \times (p-k) \times (p-k-1) \times \cdots \times 2 \times 1} \\ &= \frac{p \times (p-1) \times \cdots \times (p-k+1)}{k \times (k-1) \times \cdots \times 2 \times 1}.\end{aligned}$$

Since $p \mid p$, we have $p \mid p \times (p-1) \times \cdots \times (p-k+1)$ by (D4). Since p is prime, all that we have to check now is that p does not divide the numerator, and hence does not cancel out. This is the case because $p > k$ and p is relatively prime with every $m < p$; hence, p is relatively prime with the denominator. Therefore, $p \mid \binom{p}{k}$.

(8a) First, note that every integer of the form $4n + 3$ has a prime factor of the same form. Indeed, all odd integers are of the form $4n + 1$ or $4n + 3$ and any product of integers of the form $4n + 1$ is again an integer of the same form (check!). Now, assume the contrary, that there are only finitely many primes of the form $4n + 3$ and let $p_1, p_2, \ldots, p_k$ be all of them. If k is even, then $p_1 p_2 \cdots p_k = 4m + 1$ for some $m \in \mathbb{N}$. Therefore, $M = p_1 p_2 \cdots p_k + 2 = 4m + 3$; hence M has a prime factor of the form $4n + 3$, which must be some of the primes $p_1, p_2, \ldots, p_k$, e.g. p_i. Then $p_i \mid M$ and $p_i \mid p_1, p_2, \ldots, p_k$, and hence $p_i \mid M - p_1, p_2, \ldots, p_k = 2$, which is impossible. Likewise, if k is odd, consider $M = p_1 p_2 \cdots p_k + 4$, which is again of the type $4m + 3$. By the same argument, we conclude that some p_i must divide M, and hence $p_i \mid 4$, which is impossible.

(8b) First, note that every integer of the form $6n + 5$ must have a prime factor of the same form. Then reason as in the previous exercise.

(9) Let p be any prime. If $p < 30$, we are done, so suppose $p > 30$. Divide p by 30 with remainder r, i.e. $p = 30k + r$, where $0 \leq r < 30$. Note that $r \neq 0$, since p is prime. Now suppose $r > 1$ and r is not prime; hence r is composite. However, all composite numbers less than 30 are divisible by 2, 3 or 5. Hence, $p = c(\frac{30}{c} + \frac{r}{c})$, where c is 2, 3 or 5, and $\frac{30}{c}$ and $\frac{r}{c}$ are integers. This means that $c \mid p$, which is a contradiction since $p > 30$ and p is prime.
The claim is not true if 30 is replaced by 60: consider $p = 109$.

(10) First, note that for any prime p other than 2 and 5, if $p \mid \underbrace{11\ldots1}_{k\ 1's}0\ldots0$, then $p \mid \underbrace{11\ldots1}_{k\ 1's}$. Indeed, $\underbrace{11\ldots1}_{k\ 1's}0\ldots0 = \underbrace{11\ldots1}_{k\ 1's} \times 10^m$ for some $m > 0$ and $\gcd(p, 10^m) = 1$, so $p \mid \underbrace{11\ldots1}_{k\ 1's}$ follows from property (RP2) in Theorem 5.4.1. Now, consider the infinite sequence of integers $1, 11, 111, \ldots$. It has an infinite subsequence of integers leaving the same remainder when divided by p (why?). Then the differences of any integer of that subsequence and the first term of the sequence is divisible by p and is of the form $\underbrace{11\ldots1}_{k\ 1's}0\ldots0$, whence the claim follows.

(11) We apply the principle of complete mathematical induction. For $n = 1$, $p_1 = 2 < 4 = 2^{2^1}$. Assume $p_i < 2^{2^i}$ for all $i \leq n$. Now, $p_1 \times p_2 \times \cdots \times p_n + 1$ is not divisible by any of the primes $p_1, p_2, \ldots, p_n$, for otherwise, since $p_1 \times p_2 \times \cdots \times p_n$ is divisible by p_i for all $1 \leq i \leq n$, $p_i \mid 1$, which is a contradiction.

This means that $p_1 \times p_2 \times \cdots \times p_1 + 1$ must be divisible by a prime p_m, where $m > n$. Hence, by (D8),

$$p_m \leq \prod_{i=1}^{n} p_i + 1$$

and so

$$\begin{aligned} p_m &< \prod_{i=1}^{n} 2^{2^i} + 1 \text{ (by the inductive hypothesis)} \\ &= 2^{\sum_{i=1}^{n} 2^i} + 1 \\ &= 2^{2^{n+1}-2} + 1 \\ &< 2^{2^{n+1}} \\ &\leq 2^{2^m}. \end{aligned}$$

(12) The claim follows easily from Theorem 5.4.13, but there is also a simple direct proof. Consider $n! - 1$. It is either prime, and then we are done, or is composite, and hence has a prime divisor. However, all prime divisors of $n! - 1$ must be greater than n, because every integer less than or equal to n divides $n!$.

(13) Assume $\gcd(a, b) = 1$ and let $\gcd(a + b, a^2 - ab + b^2) = d$. Then $d \mid a + b$ and $d \mid a^2 - ab + b^2$. Now,

$$a^2 - ab + b^2 = a^2 + 2ab + b^2 - 3ab = (a + b)^2 - 3ab.$$

However, $d \mid a + b$, so $d \mid (a + b)^2$ by (D4). Hence,

$$d \mid (a + b)^2 - 3ab - (a + b)^2$$

by (D6), so $d \mid 3ab$. Now, if $d = 1$, we are done, so assume $d > 1$. Let c be a prime divisor of d. Then $c \mid 3ab$ by (D5), and hence $c \mid 3$ or $c \mid a$ or $c \mid b$ by Theorem 5.4.6. If $c \mid a$, then $c \mid (a + b) - a$ since $c \mid a + b$ by (D5). Hence, $c \mid b$, which contradicts the fact that $\gcd(a, b) = 1$, so $c \nmid a$. Similarly, $c \nmid b$, and hence $c \mid 3$. However, since c is prime, $c = 3$. We can thus write d as $d = 3k$ for some $k \in \mathbb{Z}$. If $k = 1$, we are done, so suppose $k > 1$. Now, since $d \mid 3ab$, we have $3k \mid 3ab$ and hence, by (D9), $k \mid ab$. Let p be a prime divisor of k. Then $p \mid d$, so $p \mid a + b$ by (D5). We also have $p \mid ab$ by (D5); hence, by Theorem 5.4.6, $p \mid a$ or $p \mid b$. If $p \mid a$, $p \mid (a + b) - a$ by (D6), which means $p \mid b$, again this is a contradiction. Hence, $p \nmid a$ and, similarly, $p \nmid b$. This means that $k = 1$ and thus $d = 3$.

(14) The proof is by contraposition. Suppose p is composite. Then $p = ab$ for some integers $1 < a, b < p$ and

$$2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1.$$

Now, let $k = 2^a$. Then $2^p - 1 = k^b - 1$ and

$$k^b - 1 = (k - 1)(k^{b-1} + k^{b-2} + \cdots + k + 1),$$

so

$$2^p - 1 = (k - 1)(k^{b-1} + k^{b-2} + \cdots + k + 1),$$

which is composite.

(15) We use the following algebraic identity where n is an odd integer:

$$x^n + 1 = (x + 1) \sum_{k=0}^{n-1} (-1)^{n-1-k} x^k.$$

Assume $2^n + 1$ is prime and suppose that n is not a power of 2. Then $n = ab$, where b is odd and we have $1 \leq a < n$ and $1 < b \leq n$. Then we have

$$2^n + 1 = (2^a + 1) \sum_{k=0}^{b-1} (2^a)^k (-1)^{b-1-k},$$

which is composite.

(16) Let $d = \gcd(a, b)$. Then $a = dm$ and $b = dn$ for some integers m and n. Note that $\gcd(m, n) = 1$ by (GCD6). Then

$$a + b = dm + dn = d(m + n)$$

and

$$\operatorname{lcm}(a, b) = \operatorname{lcm}(dm, dn) = d \operatorname{lcm}(m, n) = d\frac{mn}{1} = dmn.$$

Therefore,

$$\gcd(a + b, \operatorname{lcm}(a, b)) = \gcd(d(m + n), dmn) = d \gcd(m + n, mn).$$

We now claim that $\gcd(m + n, mn) = 1$. To see this, suppose $e > 1$ and it divides both $m + n$ and mn. Since $e > 1$, it has a prime divisor p by Theorem 5.4.4. Hence, $p \mid m + n$ and $p \mid mn$ by (D5). However, p is prime so, by Theorem 4.4.6, $p \mid m$ or $p \mid n$. If $p \mid m$, $p \mid m + n - m$ by (D6). Thus, $p \mid n$, which contradicts the fact that $\gcd(m, n) = 1$. Similarly, if $p \mid n$, we get a contradiction. This means that $\gcd(m + n, mn) = 1$, so $\gcd(a + b, \operatorname{lcm}(a, b)) = d$.

(17) For each of these, we use Theorem 5.4.10. Let $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ and $c = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ be decompositions of a, b and c in products of powers of primes, where some of the α's, β's and γ's can be 0. Then:

(17a)

$$\begin{aligned}
&\gcd(a, \operatorname{lcm}(b, c)) \\
&= \gcd\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\beta_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right)\right) \\
&= \gcd\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\max(\beta_i, \gamma_i)}\right) \\
&= \prod_{i=1}^{k} p_i^{\min(\alpha_i,\ \max(\beta_i, \gamma_i))} \\
&= \prod_{i=1}^{k} p_i^{\max(\min(\alpha_i, \beta_i),\ \min(\alpha_i, \gamma_i))} \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}, \prod_{i=1}^{k} p_i^{\min(\alpha_i, \gamma_i)}\right) \\
&= \operatorname{lcm}\left(\gcd\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\beta_i}\right), \gcd\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right)\right) \\
&= \operatorname{lcm}(\gcd(a, b),\ \gcd(a, c)).
\end{aligned}$$

The key fact in the proof above was that for any numbers α, β, γ, the following identity, which we leave to the reader to verify, holds:

$$\min(\alpha,\ \max(\beta, \gamma)) = \max(\min(\alpha, \beta),\ \min(\alpha, \gamma)).$$

(17b) Likewise:

$$\begin{aligned}
&\operatorname{lcm}(a,\ \gcd(b, c)) \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\alpha_i},\ \gcd\left(\prod_{i=1}^{k} p_i^{\beta_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right)\right) \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\min(\beta_i, \gamma_i)}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \min(\beta_i,\, \gamma_i))} \\
&= \prod_{i=1}^{k} p_i^{\min(\max(\alpha_i,\, \beta_i),\, \max(\alpha_i,\, \gamma_i))} \\
&= \gcd\left(\prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \beta_i)}, \prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \gamma_i)}\right) \\
&= \gcd\left(\operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\beta_i}\right), \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right)\right) \\
&= \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c)).
\end{aligned}
$$

The key fact in the proof above was that for any numbers α, β, γ, the following identity, which we leave to the reader to verify, holds:

$$\max(\alpha,\, \min(\beta, \gamma)) = \min(\max(\alpha, \beta),\, \max(\alpha, \gamma)).$$

(17c)

$$
\begin{aligned}
&\operatorname{lcm}(\gcd(a, b),\, \gcd(b, c),\, \gcd(a, c)) \\
&= \operatorname{lcm}\left(\gcd\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\beta_i}\right),\, \gcd\left(\prod_{i=1}^{k} p_i^{\beta_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right),\, \gcd\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right)\right) \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\min(\alpha_i,\, \beta_i)}, \prod_{i=1}^{k} p_i^{\min(\beta_i,\, \gamma_i)}, \prod_{i=1}^{k} p_i^{\min(\alpha_i,\, \gamma_i)}\right) \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\min(\alpha_i,\, \beta_i)}, \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\min(\beta_i,\, \gamma_i)}, \prod_{i=1}^{k} p_i^{\min(\alpha_i,\, \gamma_i)}\right)\right) \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\min(\alpha_i,\, \beta_i)}, \prod_{i=1}^{k} p_i^{\max(\min(\beta_i,\, \gamma_i),\, \min(\alpha_i,\, \gamma_i))}\right) \\
&= \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\min(\alpha_i,\, \beta_i)}, \prod_{i=1}^{k} p_i^{\min(\max(\alpha_i,\, \beta_i),\, \gamma_i)}\right) \\
&= \prod_{i=1}^{k} p_i^{\max(\min(\alpha_i,\, \beta_i),\, \min(\max(\alpha_i,\, \beta_i),\, \gamma_i))} \\
&= \prod_{i=1}^{k} p_i^{\min(\max(\alpha_i,\, \beta_i),\, \min(\max(\beta_i,\, \gamma_i),\, \max(\alpha_i,\, \gamma_i)))} \\
&= \gcd\left(\prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \beta_i)}, \gcd\left(\prod_{i=1}^{k} p_i^{\max(\beta_i,\, \gamma_i)}, \prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \gamma_i)}\right)\right) \\
&= \gcd\left(\prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \beta_i)}, \prod_{i=1}^{k} p_i^{\max(\beta_i,\, \gamma_i)}, \prod_{i=1}^{k} p_i^{\max(\alpha_i,\, \gamma_i)}\right) \\
&= \gcd\left(\operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\beta_i}\right), \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\beta_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right), \operatorname{lcm}\left(\prod_{i=1}^{k} p_i^{\alpha_i}, \prod_{i=1}^{k} p_i^{\gamma_i}\right)\right) \\
&= \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(b, c), \operatorname{lcm}(a, c))
\end{aligned}
$$

The key fact in the proof above was that for any numbers α, β, γ, the following identity, which we leave to the reader to verify, holds:

$$\max(\min(\alpha,\beta),\ \min(\max(\alpha,\beta),\gamma)) = \min(\max(\alpha,\beta),\ \max(\beta,\gamma),\ \max(\alpha,\gamma)).$$

(17d) We show that $\operatorname{lcm}(a,b,c)\gcd(ab,bc,ac) = abc$:

$$\begin{aligned}
&\gcd(ab,bc,ac)\operatorname{lcm}(a,b,c)\\
&= \gcd(ab,\ \gcd(bc,ac))\operatorname{lcm}(a,\operatorname{lcm}(b,c))\\
&= \gcd\left(\prod_{i=1}^k p_i^{\alpha_i}\prod_{i=1}^k p_i^{\beta_i},\ \gcd\left(\prod_{i=1}^k p_i^{\beta_i}\prod_{i=1}^k p_i^{\gamma_i},\ \prod_{i=1}^k p_i^{\alpha_i}\prod_{i=1}^k p_i^{\gamma_i}\right)\right)\operatorname{lcm}\left(\prod_{i=1}^k p_i^{\alpha_i},\operatorname{lcm}\left(\prod_{i=1}^k p_i^{\beta_i},\ \prod_{i=1}^k p_i^{\gamma_i}\right)\right)\\
&= \gcd\left(\prod_{i=1}^k p_i^{\alpha_1+\beta_i},\ \gcd\left(\prod_{i=1}^k p^{\beta_i+\gamma_i},\ \prod_{i=1}^k p_i^{\alpha_i+\gamma_i}\right)\right)\operatorname{lcm}\left(\prod_{i=1}^k p_i^{\alpha_i},\operatorname{lcm}\left(\prod_{i=1}^k p_i^{\beta_i},\ \prod_{i=1}^k p_i^{\gamma_i}\right)\right)\\
&= \gcd\left(\prod_{i=1}^k p_i^{\alpha_1+\beta_i},\ \prod_{i=1}^k p_i^{\min(\beta_i+\gamma_i,\ \alpha_i+\gamma_i)}\right)\operatorname{lcm}\left(\prod_{i=1}^k p_i^{\alpha_i},\ \prod_{i=1}^k p_i^{\max(\beta_i,\ \gamma_i)}\right)\\
&= \prod_{i=1}^k p_i^{\min(\alpha_i+\beta_i,\ \min(\beta_i+\gamma_i,\ \alpha_i+\gamma_i))}\prod_{i=1}^k p_i^{\max(\alpha_i,\ \max(\beta_i,\ \gamma_i))}\\
&= \prod_{i=1}^k p_i^{\min(\alpha_1+\beta_i,\ \beta_i+\gamma_1,\ \alpha_i+\gamma_i)}\prod_{i=1}^k p_i^{\max(\alpha_i,\ \beta_i,\ \gamma_i)}\\
&= \prod_{i=1}^k p_i^{\alpha_i+\beta_i+\gamma_i}\\
&= \left(\prod_{i=1}^k p_i^{\alpha_i}\right)\left(\prod_{i=1}^k p_i^{\beta_i}\right)\left(\prod_{i=1}^k p_i^{\gamma_i}\right)\\
&= abc.
\end{aligned}$$

(18) First, suppose that m_i and m_j, for some $i \neq j$, have a common divisor $d > 1$. Since $m_j \mid M_k$ for every $k \neq j$, we have that $d \mid M_k$ for every $k \neq j$. Besides, $m_i \mid M_j$, and hence $d \mid M_j$. Therefore, $\gcd(M_1, \ldots, M_n) > 1$. Conversely, let $d > 1$ be a common divisor of $M_1, \ldots, M_n$. We can assume that d is prime. Then $d \mid M_1 = m_2 \cdots m_n$, and hence $d \mid m_j$ for some $j > 1$. Since $d \mid M_j$ we also have that d divides m_i for some $i \neq j$; therefore m_i and m_j are not relatively prime.

(19) This follows immediately from Theorem 5.4.10.

(21) Hint: for any given $m \geq 1$ prove by induction on n that for every $n > m$, t_n leaves a remainder 1 when divided by t_m.

(22) Let A be an arbitrary set of 16 consecutive integers. Clearly, if p is a common prime factor of two integers in A, then $p \in \{2, 3, 5, 7, 11, 13\}$. It therefore suffices to show that we can find an element of A that is not divisible by any number from this set. Now consider the remainders of division by 30 that are relatively prime to 30. They are $1, 7, 11, 13, 17, 19, 23, 29$. Further, note that no matter how we choose the 16 consecutive integers, there are always 4 of them that leave a remainder when divided by 30, which is one of these. Then note that the difference between two of these remainders is never divisible by 7 and 13, and the only differences divisible by 11 are $23 - 1$ and $29 - 7$, but each of these pairs of numbers are too far apart to be in the same set of 16 consecutive integers. Therefore, among these 4 numbers there is at most one divisible by 7, at most one divisible by 11 and at most one divisible by 13. Therefore, we can choose a number among these 4 numbers that is not divisible by any of these. Finally, since that number is relatively prime to 30, it is not divisible by 2, 3 or 5, either. Thus, it must be relatively prime with each of the others.

(23) Let $2^m - 1$ be prime. Then the proper positive divisors of $2^{m-1}(2^m - 1)$ are

$$2^0, 2^1, \ldots, 2^{m-1}, 2^0(2^m - 1), 2^1(2^m - 1), \ldots, 2^{m-2}(2^m - 1)$$

Their sum is

$$\begin{aligned} &2^0 + 2^1 + \cdots + 2^{m-1} + 2^0(2^m - 1) + 2^1(2^m - 1) + \cdots + 2^{m-2}(2^m - 1) \\ &= 2^m - 1 + (2^0 + 2^1 + \cdots + 2^{m-2})(2^m - 1) \\ &= 2^m - 1 + (2^{m-1} - 1)(2^m - 1) \\ &= 2^{m-1}(2^m - 1). \end{aligned}$$

(24) See the solution of Exercise 13 in Section 5.3.

5.5. Congruence relations

(1) (CON1) Assume $a \equiv b \pmod{n}$. Then $n \mid a - b$, so $n \mid a - b - 0$, and hence $a - b \equiv 0 \pmod{n}$. Conversely, assume $a - b \equiv 0 \pmod{n}$. Then $n \mid a - b - 0$, so $n \mid a - b$.
(CON2) $n \mid 0$, so $n \mid a - a$ and hence $a \equiv a \pmod{n}$.
(CON3) Let $a \equiv b \pmod{n}$. Then $n \mid a - b$ and so $n \mid -(a - b)$, by (D3). Hence, $n \mid b - a$, so $b \equiv a \pmod{n}$.
(CON4) Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n \mid a - b$ and $n \mid b - c$, so $n \mid (a - b) + (b - c)$, by (D6). Hence, $n \mid a - c$, so $a \equiv c \pmod{n}$.
(CON5) Assume $a \equiv b \pmod{n}$. Then $n \mid a - b = (a + c) - (b + c)$. We thus have that $n \mid (a + c) - (b + c)$. Hence, $a + c \equiv b + c \pmod{n}$. From $n \mid (a + c) - (b + c)$ it also follows that $n \mid (a - c) - (b - c)$, which means that $a - c \equiv b - c \pmod{n}$. Also, by (D4), $n \mid (a - b)c$, and hence $n \mid ac - bc$. Hence, $ca \equiv cb \pmod{n}$.
(CON8) By straightforward induction on k, using (CON7).
(CON9) Let $d > 0$ and assume $a \equiv b \pmod{n}$ and that $d \mid n$. Then $n \mid a - b$, so $d \mid a - b$ by (D5). Hence, $a \equiv b \pmod{d}$.
(CON10) Assume $a \equiv b \pmod{n}$ and that $c > 0$. Then $n \mid a - b$, so $cn \mid c(a - b)$ by (D9). Hence, $nc \mid ac - bc$, so $ac \equiv bc \pmod{nc}$.

(2a) Let k be the unit digit of a square n^2. Then $n^2 \equiv k \pmod{10}$, so $(n \text{ rem } 10)^2 \equiv k \pmod{10}$. Now, $(n \text{ rem } 10) \in \{0, 1, \ldots, 9\}$; substituting these different possible values for n rem 10 shows that $k \in \{0, 1, 4, 5, 6, 9\}$.

(2b) Likewise.

(3a) Let $n^2 \equiv k \pmod{8}$. Then $(n \text{ rem } 8)^2 \equiv k \pmod{8}$. Now $(n \text{ rem } 8) \in \{0, 1, \ldots, 7\}$; substituting these values for $(n \text{ rem } 8)$ shows that $k \in \{0, 1, 4\}$.

(3b) Let k be the remainder modulo 7 of the square of some integer n. Then $n^3 \equiv k \pmod{7}$, so $(n \text{ rem } 7)^3 \equiv k \pmod{7}$. Now $n \pmod{7} \in \{0, 1, \ldots, 6\}$; substituting these different values for $(n \text{ rem } 7)$ shows that $k \in \{0, 1, 6\}$.

(4a) The last digit is the remainder of 2^{222} modulo 10. Therefore, we have to solve for x in

$$2^{222} \equiv x \pmod{10},$$

where $0 \le x < 10$. Let us list the first few powers of 2 modulo 10:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{10}, & 2^4 &\equiv 4 \pmod{10}, \\ 2^2 &\equiv 4 \pmod{10}, & 2^5 &\equiv 2 \pmod{10}, \\ 2^3 &\equiv 8 \pmod{10}, & 2^6 &\equiv 4 \pmod{10}. \end{aligned}$$

Thus, we see that the pattern repeats after every 4 powers of 2. Since $222 = 4 \cdot 55 + 2$, we have $2^{222} \equiv 2^2 \equiv 4 \pmod{10}$. Hence, the last digit is 4.

(4b) The last digit is the remainder of 3^3 modulo 10. We thus have to solve for x in

$$3^{333} \equiv x \pmod{10},$$

where $0 \leq x < 10$. Let us list the first few powers of 3 modulo 10:

$$3^1 \equiv 3 \pmod{10}, \qquad 3^5 \equiv 3 \pmod{10},$$
$$3^2 \equiv 9 \pmod{10}, \qquad 3^6 \equiv 9 \pmod{10},$$
$$3^3 \equiv 7 \pmod{10}, \qquad 3^7 \equiv 7 \pmod{10}.$$
$$3^4 \equiv 1 \pmod{10},$$

Thus, we see that the pattern repeats after every 4 powers of 3. Since $333 = 4 \cdot 83 + 1$, we have $3^{333} \equiv 3^1 \equiv 3 \pmod{10}$. Hence, the last digit is 3.

(4c) The last digit is the remainder of 7^{777} modulo 10. Therefore, we have to solve for x in

$$7^{777} \equiv x \pmod{10},$$

where $0 \leq x < 10$. Let us list the first few powers of 7 modulo 10:

$$7^1 \equiv 7 \pmod{10}, \qquad 7^4 \equiv 1 \pmod{10},$$
$$7^2 \equiv 9 \pmod{10}, \qquad 7^5 \equiv 7 \pmod{10}.$$
$$7^3 \equiv 3 \pmod{10},$$

Thus, we see that the pattern repeats after every 4 powers of 7. Since $777 = 4 \cdot 194 + 1$, we have $7^{777} \equiv 7^1 \equiv 7 \pmod{10}$. Hence, the last digit is 7.

(5) For the sake of a contradiction, assume $3n^2 - 5$ is a perfect square. Then $3n^2 - 5 \equiv 0 \pmod 4$ or $3n^2 - 5 \equiv 1 \pmod 4$, so $3n^2 \equiv 5 \pmod 4$ or $3n^2 \equiv 6 \pmod 4$, by (CON1). Hence, $3n^2 \equiv 1 \pmod 4$ or $3n^2 \equiv 2 \pmod 4$. But $n^2 = 4k_1 + 1$ or $n^2 = 4k_2$ for $k_1, k_2 \in \mathbb{Z}$, so $3n^2 = 3 \cdot 4k_1 + 3$ or $3n^2 = 3 \cdot 4k_2$. We thus have that $3n^2 \equiv 3 \pmod 4$ or $3n^2 \equiv 0 \pmod 4$, which contradicts the above.

(6) Assume $x \equiv y \pmod n$. Then $n \mid x - y$. Now, let $z = \gcd(x, n)$. Then $z \mid x$ and $z \mid n$, so $z \mid x - y$ by (D5). Hence, by (D6), $z \mid x - y + x$, so $z \mid y$ by (D3). This means that z is a common divisor of y and n; hence $z \leq \gcd(x, n)$. Likewise, we show that $\gcd(x, n) \leq \gcd(y, n)$, and hence $\gcd(x, n) = \gcd(y, n)$.
The converse is not true: take for instance $x = 2$, $y = 3$ and $n = 5$.

(7) The two cases are analogous, so we will only prove (b). Let $n \in \mathbb{N}$, and let $\overline{a_k \cdots a_1 a_0}$ be the decimal representation of n, where a_0 is the digit of units, a_1 is in the digit of 10's, etc. Then

$$n = a_k 10^k + \cdots + a_2 10^2 + a_1 10 + a_0.$$

Since $10 \equiv 1 \pmod 9$, we have by (CON8) that $10^i \equiv 1 \pmod 9$, and hence $a_i 10^i \equiv a_i \pmod 9$ for all $0 \leq i \leq k$. Hence, by (CON5),

$$a_k 10^k + \cdots + a_2 10^2 + a_1 10 + a_0 \equiv (a_k + \cdots + a_1 + a_0) \pmod 9.$$

Therefore, $3 \mid n - (a_1 + a_2 + \cdots + a_k)$ by (D4). Hence, by definition, n and $(a_1 + a_2 + \cdots + a_k)$ leave the same remainders when divided by 3. In particular, they are equally divisible by 3.

(8) We have to show that $p \mid (a + b)^p - a^p - b^p$. Now, by the binomial theorem,

$$(a + b)^p - a^p - b^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k - a^p - b^p = \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k.$$

By Exercise 6 in Section 5.4, $p \mid \left(\frac{p}{k}\right)$ for all $0 < k < p$, so, by (D4), $p \mid \left(\frac{p}{k}\right) a^{p-k} b^k$ for all $0 < k < p$. Hence, by (D6),

$$p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k,$$

which means that $p \mid (a+b)^p - a^p - b^p$. Thus,

$$(a+b)^p \equiv (a^p + b^p) \pmod{p}.$$

(9) Note that $4444^{4444} < 10000^{4444} = (10^4)^{4444} = 10^{17776}$. Therefore 4444^{4444} has less than 17776 digits. Hence, $A < 9.17775 = 159975$. Therefore, the sum of the digits of A is maximal when $A = 99999$, so $B \leq 45$. Further, the maximal sum of the digits of any positive integer $n \leq 45$ is 12, when $n = 39$. Furthermore, as shown in the solution of Exercise 7, every integer is congruent modulo 9 to the sum of its digits. Thus, $4444^{4444} \equiv A \equiv B \pmod 9$. We want to compute the number X, where $1 \leq X \leq 12$, such that $4444^{4444} \equiv X \pmod 9$. Note that

$$4444^1 \equiv 7 \pmod 9,$$
$$4444^2 \equiv 4 \pmod 9 \text{ and}$$
$$4444^3 \equiv 1 \pmod 9.$$

Since $4444 = 3 \cdot 1481 + 1$, we have that $4444^{4444} \equiv 4444^{3\cdot 1481+1} \equiv (4444^3)^{1481} \cdot 4444 \equiv 1 \cdot 4444 \equiv 7 \pmod 9$. Thus, $X = 7$, which means that the sum of the digits of B is 7.

(11) Dividing 5555 and 2222 by 7 we find that $2222 \equiv 3 \pmod 7$ and $5555 \equiv 4 \pmod 7$. Hence, $2222^{5555} \equiv 3^{5555} \pmod 7$ and $5555^{2222} \equiv 4^{2222} \pmod 7$ by (CON8). Let us now list the first few powers of 3 modulo 7:

$$3^1 \equiv 3 \pmod 7, \qquad 3^5 \equiv 5 \pmod 7,$$
$$3^2 \equiv 2 \pmod 7, \qquad 3^6 \equiv 1 \pmod 7,$$
$$3^3 \equiv 6 \pmod 7, \qquad 3^7 \equiv 3 \pmod 7.$$
$$3^4 \equiv 4 \pmod 7,$$

We see that the remainder starts repeating after the 6th power of 3 and $5555 \equiv 5 \pmod 6$; hence $3^{5555} \equiv 3^5 = 243 \equiv 5 \pmod 7$. Similarly, the first few powers of 4 modulo 7 are

$$4^1 \equiv 4 \pmod 7, \qquad 4^3 \equiv 1 \pmod 7,$$
$$4^2 \equiv 2 \pmod 7, \qquad 4^4 \equiv 4 \pmod 7.$$

We see that the remainder repeats after the 3rd powers of 4 and $2222 \equiv 2 \pmod 3$. Hence, $4^{2222} \equiv 4^2 \equiv 2 \pmod 7$. Therefore, $2222^{5555} \equiv 5 \pmod 7$ and $5555^{2222} \equiv 2 \pmod 7$ by (CON4), so by (CON6):

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 \equiv 0 \pmod 7.$$

Thus, $7 \mid 2222^{5555} + 5555^{2222}$.

(12) We calculate the last two digits of 2^{999} and 3^{999} separately. We begin by calculating the last two digits of the powers of 2 as follows:

$$2^1 \equiv 2 \pmod{100},$$
$$2^2 \equiv 4 \pmod{100},$$
$$2^4 \equiv 16 \pmod{100},$$
$$2^8 \equiv 56 \pmod{100},$$
$$2^{16} \equiv 2^8 \times 2^8 \equiv 56 \times 56 \equiv 3136 \equiv 36 \pmod{100},$$
$$2^{32} \equiv 2^{16} \times 2^{16} \equiv 36 \times 36 \equiv 1296 \equiv 96 \pmod{100},$$
$$2^{64} \equiv 2^{32} \times 2^{32} \equiv 96 \times 96 \equiv 9216 \equiv 16 \pmod{100},$$
$$2^{128} \equiv 2^{64} \times 2^{64} \equiv 16 \times 16 \equiv 256 \equiv 56 \pmod{100},$$
$$2^{256} \equiv 2^{128} \times 2^{128} \equiv 56 \times 56 \equiv 3136 \equiv 36 \pmod{100} \text{ and}$$
$$2^{512} \equiv 2^{256} \times 2^{256} \equiv 36 \times 36 \equiv 1296 \equiv 96 \pmod{100}.$$

Now, by (CON7),

$$2^{999} \equiv 2^{512} \times 2^{256} \times 2^{128} \times 2^{64} \times 2^{32} \times 2^4 \times 2^2 \times 2^1 \equiv 96^2 \times 36 \times 56 \times 16^2 \times \times 4 \times 2 \equiv 88 \pmod{100}.$$

Likewise, for 3:

$$3^1 \equiv 3 \pmod{100},$$
$$3^2 \equiv 9 \pmod{100},$$
$$3^4 \equiv 81 \pmod{100},$$
$$3^8 \equiv 3^4 \times 3^4 \equiv 81 \times 81 \equiv 6561 \equiv 61 \pmod{100},$$
$$3^{16} \equiv 3^8 \times 3^8 \equiv 61 \times 61 \equiv 3721 \equiv 21 \pmod{100},$$
$$3^{32} \equiv 3^{16} \times 3^{16} \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100},$$
$$3^{64} \equiv 3^{32} \times 3^{32} \equiv 41 \times 41 \equiv 1681 \equiv 81 \pmod{100},$$
$$3^{128} \equiv 3^{64} \times 3^{64} \equiv 81 \times 81 \equiv 6561 \equiv 61 \pmod{100},$$
$$3^{256} \equiv 3^{128} \times 3^{128} \equiv 61 \times 61 \equiv 3721 \equiv 21 \pmod{100} \text{ and}$$
$$3^{512} \equiv 3^{256} \times 3^{256} \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}.$$

Hence, by (CON7),

$$3^{999} \equiv 3^{512} \times 3^{256} \times 3^{128} \times 3^{64} \times 3^{32} \times 3^4 \times 3^2 \times 3^1 \equiv 41^2 \times 21 \times 61 \times 81^2 \times 9 \times 3 \equiv 67 \pmod{100}.$$

Now, by (CON6):

$$2^{999} + 3^{999} \equiv 88 + 67 \equiv 155 \equiv 55 \pmod{100}.$$

(13) Answer: 5.

5.6. Equivalence classes and residue systems modulo n

(1) We have to show that if $[x]_n = [x']_n$ and $[y]_n = [y']_n$, then $[x]_n \oplus [y]_n = [x']_n \oplus [y']_n$ and $[x]_n \odot [y]_n = [x']_n \odot [y']$. Assume $[x]_n = [x']_n$ and $[y]_n = [y']_n$. Then $x \equiv y \pmod{n}$ and $x' \equiv y' \pmod{n}$. Hence, by (CON6) and (CON7), $x + y \equiv x' + y' \pmod{n}$ and $x \cdot y \equiv x' \cdot y' \pmod{n}$. This means that $[[x + y]]_n = [[x' + y']]_n$ and $[[x \cdot y]]_n \equiv [[x' \cdot y']]_n$, so, by definition, $[[x]]_n \oplus [[y]]_n = [[x']]_n \oplus [[y']]_n$ and $[[x]]_n \odot [[y]]_n = [[x']]_n \odot [[y']]_n$. Thus, $[x]_n \oplus [y]_n = [x']_n \oplus [y']_n$ and $[x]_n \odot [y]_n = [x']_n \odot [y']_n$.

(2) $\oplus$ is commutative:

$$\begin{aligned}[a]_n \oplus [b]_n &= [[a]]_n \oplus [[b]]_n \\ &= [[a + b]]_n \\ &= [[b + a]]_n \\ &= [[b]]_n \oplus [[a]]_n \\ &= [b]_n \oplus [a]_n.\end{aligned}$$

$\odot$ is commutative: likewise.
$\oplus$ is associative:

$$\begin{aligned}([a]_n \oplus [b]_n) \oplus [c]_n &= ([[a]]_n \oplus [[b]]_n) \oplus [[c]]_n \\ &= [[a + b]]_n \oplus [[c]]_n \\ &= [[(a + b) + c]]_n \\ &= [[a + (b + c)]]_n \\ &= [[a]]_n \oplus [[b + c]]_n \\ &= [[a]]_n \oplus ([[b]]_n \oplus [[c]]_n) \\ &= [a]_n \oplus ([b]_n \oplus [c]_n).\end{aligned}$$

$\odot$ is associative: likewise.
$\odot$ is distributive over $\oplus$:

$$\begin{aligned}[a]_n \odot ([b]_n \oplus [c]_n) &= [[a]]_n \odot ([[b]]_n \oplus [[c]]_n) \\ &= [[a]]_n \cdot [[b+c]]_n \\ &= [[a \cdot (b+c)]]_n \\ &= [[(a \cdot b) + (a \cdot c)]]_n \\ &= [[a \cdot c]]_n \oplus [[a \cdot c]]_n \\ &= ([[a]]_n \odot [[b]]_n) \oplus ([[a]]_n \odot [[c]]_n) \\ &= ([a]_n \odot [b]_n) \oplus ([a]_n \odot [c]_n).\end{aligned}$$

$[a]_n \oplus [0]_n = [a]_n$:

$$[a]_n \oplus [0]_n = [[a]]_n \oplus [[0]]_n = [[a+0]]_n = [[a]]_n = [a]_n,$$

$[a]_n \odot [0]_n = [0]_n$:

$$[a]_n \odot [0]_n = [[a]]_n \odot [[0]]_n = [[a \cdot 0]]_n = [[0]]_n = [0]_n,$$

$[a]_n \odot [1]_n = [a]_n$:

$$[a]_n \odot [1]_n = [[a]]_n \odot [[1]]_n = [[a \cdot 1]]_n = [[a]]_n = [a]_n.$$

(3a) 29 rem 8 = 5, so $[[29]]_8 = [5]_8$.

(3b) 182 rem 13 = 0, so $[[182]]_{13} = [0]_{13}$.

(3c) $[7]_9 \oplus [8]_9 = [[7+8]]_9 = [[15]]_9 = [6]_9$.

(3d) $[7]_9 \odot [8]_9 = [[7 \cdot 8]]_9 = [[56]]_9 = [2]_9$.

(4a) $x = [2]_4$

(4b) $x = [4]_5$

(4c) $x = [2]_5$

(4d) $x = [0]_5$

(4e) $x = [0]_4$ or $x = [2]_4$

(5) The product of two nonzero elements in $\mathbb{Z}_n$ can be $[0]_n$ if and only if n is composite.

(6) The first property is straightforward. For the second property, suppose that $\{x_1, \ldots, x_n\}$ is a complete residue system modulo n and consider $\{x_1 + a, \ldots, x_n + a\}$. For every integer y, there is a (unique) x_i such that $x_i \equiv y - a \pmod{n}$; hence $x_i + a \equiv y \pmod{n}$. Further, if $x_j + a \equiv y \pmod{n}$, for some j, then $x_i + a \equiv x_j + a \pmod{n}$; hence $x_i \equiv x_j \pmod{n}$. Therefore $i = j$ because $\{x_1, \ldots, x_n\}$ is a complete residue system modulo n. Thus, $\{x_1 + a, \ldots, x_n + a\}$ is also a complete residue system modulo n.

(7) It is not a complete residue system because for any $m > 2$, both $1^2 \equiv 1 \pmod{m}$ and $(m-1)^2 \equiv 1 \pmod{m}$ since $(m-1)^2 = m(m-2) + 1$.

5.7. Linear Diophantine equations and linear congruences

(1a) One solution of $81x - 24y = 18$ is $x_0 = \frac{3 \times 18}{3} = 18$ and $y_0 = \frac{10 \times 18}{3} = 60$. The general solution is given by $x = 18 + \frac{81}{3}t = 18 + 27t$ and $y = 60 + \frac{-24}{3}t = 60 - 8t$.

(1b) $28x + 91y = 146$ has no solutions since $\gcd(28, 91) = 7$ and $7 \nmid 146$.

(1c) One solution of $429x + 154y = 121$ is $x_0 = \frac{(-5)\times 121}{11} = -55$ and $y_0 = \frac{14\times 121}{11} = 154$. The general solution is given by $x = -55 + \frac{429}{11}t = -55 + 39t$ and $y = 154 + \frac{154}{11}t = 154 + 14t$.

(2a) $27x \equiv 12 \pmod{15}$ has a solution $x_0 = \frac{(-1)\times 12}{3} = -4$, so all its solutions are the numbers $x = -4 + \frac{15}{3}k = -4 + 5k$, $k \in \mathbb{Z}$.

(2b) $25x \equiv 5 \pmod{16}$ has a solution $x_0 = \frac{(-7)\times 5}{1} = -35$, so all its solutions are given as $x = -35 + \frac{16}{1}k = -35 + 16k$, $k \in \mathbb{Z}$.

(2c) $166x \equiv 18 \pmod{38}$ has a solution $x_0 = \frac{(-8)\times 18}{2} = -72$, so all of its solutions are given as $x = -72 + \frac{38}{2}k = -72 + 19k$, $k \in \mathbb{Z}$.

(2d) $84x \equiv 24 \pmod{35}$ has no solutions since $\gcd(84, 35) = 7$ and $7 \nmid 24$.

(2e) $28x \equiv 42 \pmod{49}$ has a solution $x_0 = \frac{2\times 42}{7} = 12$, so all its solutions are the numbers $x = 12 + \frac{49}{7}k = 12 + 7k$, $k \in \mathbb{Z}$.

(2f) $1001x \equiv 91 \pmod{104}$ has a solution $x_0 = \frac{(-3)\times 91}{13} = -21$, so all its solutions are the numbers $x = -21 + \frac{104}{13}k = -21 + 8k$, $k \in \mathbb{Z}$.

(2g) $3700x \equiv 11 \pmod{111}$ has no solutions since $\gcd(3700, 111) = 37$ and $37 \nmid 11$.

5.8. Chinese remainder theorem

(1a) Applying the Chinese remainder theorem: $M = 4 \times 9 = 36$, $M_1 = \frac{36}{4} = 9$, and $M_2 = \frac{36}{9} = 4$. We look for integers y_1 and y_2 such that

$$9y_1 \equiv 2 \pmod 4 \text{ and}$$
$$4y_2 \equiv 3 \pmod 9.$$

Possible values are $y_1 = 2$ and $y_2 = 3$, so we then have that $x_0 = (9 \cdot 2 + 4 \cdot 3) \text{ rem } 36 = 30 \text{ rem } 36 = 30$. All other solutions are given as $x = 30 + 36n$.

(1b) Applying the Chinese remainder theorem: $M = 14 \times 15 = 210$, $M_1 = \frac{210}{14} = 15$, and $M_2 = \frac{210}{15} = 14$. We look for integers y_1 and y_2 such that

$$15y_1 \equiv 13 \pmod{14} \text{ and}$$
$$14y_2 \equiv 9 \pmod{15}.$$

Possible values are $y_1 = 13$ and $y_2 = 6$, so we then have that $x_0 = (15 \cdot 13 + 14 \cdot 6) \text{ rem } 210 = 279 \text{ rem } 210 = 69$. All other solutions are given as $x = 69 + 210n$.

(1c) Applying the Chinese remainder theorem: $M = 4 \times 9 \times 35 = 1260$, $M_1 = \frac{1260}{4} = 315$, $M_2 = \frac{1260}{9} = 140$ and $M_3 = \frac{1260}{35} = 36$. We look for integers y_1, y_2 and y_3 such that

$$315y_1 \equiv 3 \pmod 4,$$
$$140y_2 \equiv 5 \pmod{9} \text{ and}$$
$$36y_3 \equiv 10 \pmod{35}.$$

Possible values are $y_1 = 1$, $y_2 = 1$ and $y_3 = 10$, so

$$x_0 = (315 \cdot 1 + 140 \cdot 1 + 36 \times 10) \text{ rem } 1260 = 815 \text{ rem } 1260 = 815.$$

All other solutions are obtained as $x = 815 + 1260n$.

(1d) Applying the Chinese remainder theorem: $M = 3 \times 7 \times 10 = 210$, $M_1 = \frac{210}{3} = 70$, $M_2 = \frac{210}{7} = 30$ and $M_3 = \frac{210}{10} = 21$. We look for integers y_1, y_2 and y_3 such that

$$70y_1 \equiv 2 \pmod 3,$$
$$30y_2 \equiv 3 \pmod 7 \text{ and}$$
$$21y_3 \equiv 0 \pmod 1.$$

Possible values are $y_1 = 2$, $y_2 = 5$ and $y_3 = 0$, so

$$x_0 = (70 \cdot 2 + 30 \cdot 5 + 21 \cdot 0) \text{ rem } 210 = 290 \text{ rem } 210 = 80.$$

All other solutions are obtained by $x = 80 + 210n$.

(1e) Applying the Chinese remainder theorem: $M = 5 \times 4 \times 7 \times 9 = 1260$, $M_1 = \frac{1260}{5} = 252$, $M_2 = \frac{1260}{4} = 315$, $M_3 = \frac{1260}{7} = 180$ and $M_4 = \frac{1260}{9} = 140$. We look for integers y_1, y_2, y_3 and y_4 such that

$$252y_1 \equiv 4 \pmod 5,$$
$$315y_2 \equiv 3 \pmod 4,$$
$$180y_3 \equiv 2 \pmod 7 \text{ and}$$
$$140y_4 \equiv 6 \pmod 9.$$

Possible values are $y_1 = 2$, $y_2 = 1$, $y_3 = 6$, and $y_4 = 3$, so

$$x_0 = (252 \cdot 2 + 315 \cdot 1 + 180 \cdot 6 + 140 \cdot 3) \text{ rem } 1260 = 2319 \text{ rem } 1260 = 1059.$$

All other solutions are obtained by $x = 1059 + 1260n$.

(2) We have to solve the following system of congruences:

$$x \equiv 1 \pmod 2,$$
$$x \equiv 1 \pmod 3,$$
$$x \equiv 1 \pmod 4,$$
$$x \equiv 1 \pmod 5,$$
$$x \equiv 1 \pmod 6 \text{ and}$$
$$x \equiv 0 \pmod 7.$$

Since the modulo numbers are not relatively prime, we cannot use directly the Chinese remainder rheorem. However, the 1st congruence follows from the 3rd, so we can omit it from the system. 6's are also not relatively prime. Moreover, we omit for now the 4th congruence, but remember to ensure at the end of the calculation that our answer has a remainder of 1 when we divide it by 6. Now, we can apply the Chinese remainder theorem to the rest: $M = 3 \times 4 \times 5 \times 7 = 420$, $M_1 = \frac{420}{3} = 140$, $M_2 = \frac{420}{4} = 105$, $M_3 = \frac{420}{5} = 84$ and $M_4 = \frac{420}{7} = 60$. We look for integers y_1, y_2, y_3 and y_4 such that

$$140y_1 \equiv 1 \pmod 3,$$
$$105y_2 \equiv 1 \pmod 4,$$
$$84y_3 \equiv 1 \pmod 5 \text{ and}$$
$$60y_4 \equiv 0 \pmod 7.$$

Possible values are $y_1 = 2$, $y_2 = 1$, $y_3 = 4$ and $y_4 = 7$, so the least solution is

$$x_0 = (140 \cdot 2 + 105 \cdot 1 + 84 \cdot 4 + 60 \cdot 7) \text{ rem } 420 = 301.$$

Since $301 \equiv 1 \pmod 6$, it is also a solution of the entire original system. Therefore, the smallest number of eggs the woman could have had is 301.

(3) Answer: $b_i \equiv b_j \pmod{\gcd(m_i, m_j)}$ for $1 \leq i < j \leq k$.

5.9. Euler's function. Theorems of Euler and Fermat

(1) We evaluate $\phi(n)$ for $1 \leq n \leq 16$:

$$\begin{array}{llll} \phi(1) = 1 & \phi(2) = 1 & \phi(3) = 2 & \phi(4) = 2 \\ \phi(5) = 4 & \phi(6) = 2 & \phi(7) = 6 & \phi(8) = 4 \\ \phi(9) = 6 & \phi(10) = 4 & \phi(11) = 10 & \phi(12) = 4 \\ \phi(13) = 12 & \phi(14) = 6 & \phi(15) = 8 & \phi(16) = 8 \end{array}$$

(2) $\{0, 3, 6, 9, 12, 15, 18\}$

(3) $\gcd(13, 56) = 1$ so, by Euler's theorem,

$$13^{\phi(56)} = 13^{24} \equiv 1 \pmod{56}.$$

Hence, by (CON8),

$$(13^{24})^{10} \equiv 1^{10} \pmod{56},$$

so $13^{240} \equiv 1 \pmod{56}$. However, we also have that

$$13^2 = 169 \equiv 1 \pmod{56}.^1$$

Thus, we find that

$$13^{240} \cdot 13^2 = 13^{242} \equiv 1 \pmod{56}$$

by (CON7). Therefore, $13^{242} \bmod 56$ is 1.

(4) Consider the following two cases:

Case 1: $p \mid a$.

Then $p \mid a^p$. Hence, by (D6), $p \mid a^p - a$, so $a^p \equiv a \pmod{p}$.

Case 2: $p \nmid a$.

Now we have $a^{p-1} \equiv 1 \pmod{p}$ by Theorem 5.9.8, so $p \mid a^{p-1} - 1$. Hence, by (D6), $p \mid a(a^{p-1} - 1)$, so $p \mid a^p - a$. We can thus conclude that $a^p \equiv a \pmod{p}$.

(5) Note that $42 = 2 \cdot 3 \cdot 7$. Since 2, 3 and 7 are relatively prime in pairs, if we can show that $2 \mid n^7 - n$, $3 \mid n^7 - n$ and $7 \mid n^7 - n$, we are done. Since 2, 3 and 7 are primes, using the previous exercise we find that

$n^2 \equiv n \pmod{2}$, hence by $n^7 \equiv n^6 \equiv \cdots \equiv n \pmod{2}$,
$n^3 \equiv n \pmod{3}$, hence by $n^7 \equiv n^5 \equiv n^3 \equiv n \pmod{3}$,
$n^7 \equiv n \pmod{7}$.

(6) Assume $\gcd(n, 10) = 1$. Then $n^{\phi(10)} = n^4 \equiv 1 \pmod{10}$ by Euler's theorem. Hence, by (CON8), $n^{12} = (n^4)^3 \equiv 1^3 = 1 \pmod{10}$. Hence, $10 \mid n^{12} - 1$.

[1] If we had known that earlier, we would not had to use Euler's theorem.

(7) Assume $\gcd(n, 30) = 1$ and write $30 = 2 \times 3 \times 5$. Note that $2 \nmid n$ because $2 \mid 30$. Likewise, $3 \nmid n$ and $5 \nmid n$. Hence, by Fermat's little theorem,

$$n \equiv 1 \pmod 2,$$
$$n^2 \equiv 1 \pmod 3,$$
$$n^4 \equiv 1 \pmod 5.$$

Using (CON8), we then get

$$n^4 \equiv 1 \pmod 2,$$
$$n^4 \equiv 1 \pmod 3,$$
$$n^4 \equiv 1 \pmod 5.$$

We will prove that $240 \mid n^4 - 1$. Since $240 = 2^4 \times 3 \times 5$, it only remains to prove that $n^4 \equiv 1 \pmod{16}$. Indeed, $n^4 - 1 = (n^2 - 1)(n^2 + 1) = (n - 1)(n + 1)(n^2 + 1)$. Since n is odd, we have that each of $(n - 1)$, $(n + 1)$ and $(n^2 + 1)$ is even, and moreover one of $(n - 1)$, $(n + 1)$ is divisible by 4. Therefore, $16 = 2.4.2 \mid (n - 1)(n + 1)(n^2 + 1) = n^4 - 1$, so $n^4 \equiv 1 \pmod{16}$.

(8) Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the decomposition of n in products of powers of primes. Then

$$\begin{aligned}\phi(n) &= \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).\end{aligned}$$

Now, $24 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot 19^0 \cdot 23^0$, so we have to find all the possible ways in which these prime factors can be distributed in the product above. We have the following possibilities:

$$24 = 2^{3-1}(2 - 1)3^{2-1}(3 - 1),$$
$$24 = 3^{2-1}(3 - 1)5^{1-1}(5 - 1),$$
$$24 = 2^{3-1}(2 - 1)7^{1-1}(7 - 1),$$
$$24 = 2^{2-1}(2 - 1)3^{1-1}(3 - 1)7^{1-1}(7 - 1),$$
$$24 = 2^{1-1}(2 - 1)3^{2-1}(3 - 1)5^{1-1}(5 - 1),$$
$$24 = 5^{1-1}(5 - 1)7^{1-1}(7 - 1),$$
$$24 = 2^{1-1}(2 - 1)5^{1-1}(5 - 1)7^{1-1}(7 - 1),$$
$$24 = 2^{2-1}(2 - 1)13^{1-1}(13 - 1),$$
$$24 = 3^{1-1}(3 - 1)13^{1-1}(13 - 1) \text{ and}$$
$$24 = 2^{1-1}(2 - 1)3^{1-1}(3 - 1)13^{1-1}(13 - 1).$$

Hence, $n = 35, 39, 45, 52, 56, 70, 72, 78, 84, 90$.

(9) Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the decomposition of n in products of powers of primes, where $p_1 < \cdots < p_k$. Then

$$\begin{aligned}\phi(n) &= \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).\end{aligned}$$

Therefore,

$$\frac{n}{\phi(n)} = \frac{p_1 \cdots p_k}{(p_1 - 1) \cdots (p_k - 1)}.$$

Consider two cases:

Case 1: $p_1 > 2$.

Then n is odd and $p_1 - 1, \ldots, p_k - 1$ are even, so $\phi(n) \nmid n$.

Case 2: $p_1 = 2$.

Then $p_2, \ldots, p_k$ are all odd. Hence, $p_2 - 1, \ldots, p_k - 1$ are all even, so if $\phi(n) \mid n$ there can be at most one of them, i.e. $k = 2$ and $n = 2p$. Then we want $p - 1 \mid 2p$. However, $\gcd(p - 1, p) = 1$; hence $p - 1 \mid 2$, so $p = 3$. Thus, the only possible solutions are $n = 2$ and $n = 2 \cdot 3 = 6$.

(10) Since $d \mid n$, then every integer less than d that is not relatively prime with d is also less than n and not relatively prime with n. In addition, d is less than n and not relatively prime with n. It now remains to note that the number of integers less than d that are not relatively prime with d is $d - \phi(d)$, while the number of integers less than n that are not relatively prime with n is $n - \phi(n)$.

(11) First, note that for any integer a such that $1 \leq a < n$, $\gcd(a, n) = 1$ iff $\gcd(n - a, n) = 1$. Indeed, any common divisor of a and n divides $n - a$ and any common divisor of $n - a$ and n divides $n - (n - a) = a$. Now, let $a_1, a_2, \ldots, a_{\phi(n)}$ be the integers less than n and relatively prime to n. Then all integers in $\{n - a_1, \ldots, n - a_{\phi(n)}\}$ are different and relatively prime with n; hence $\{a_1, \ldots, a_{\phi(n)}\} = \{n - a_1, \ldots, n - a_{\phi(n)}\}$. Thus, we have

$$a_1 + \cdots + a_{\phi(n)} = n - a_1 + \cdots + n - a_{\phi(n)},$$

and hence

$$2a_1 + \cdots + 2a_{\phi(n)} = \phi(n)n.$$

Therefore,

$$2(a_1 + \cdots + a_{\phi(n)}) = \frac{\phi(n)n}{2}.$$

(12) First, note that $56\,786\,730 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 31 \times 61$. It suffices to show that each of these primes divides $mn(m^{60} - n^{60})$. Now, let $p \in \{2, 3, 5, 7, 11, 13, 31, 61\}$. If $p \mid m$ or $p \mid n$, we are done, so suppose $p \nmid m$ and $p \nmid n$. Note that for each such p, $p - 1 \mid 60$, and hence $m^{60} = m^{k(p-1)}$ and $n^{60} = n^{l(p-1)}$ for some integers k and l. Furthermore, $p \nmid m^k$ and $p \nmid n^l$. Applying Fermat's little theorem, we then have that $m^{60} = m^{k(p-1)} \equiv 1 \pmod{p}$ and $n^{60} = n^{l(p-1)} \equiv 1 \pmod{p}$ Hence, $m^{60} - n^{60} \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus, $p \mid mn(m^{60} - n^{60})$ for each $p \in \{2, 3, 5, 7, 11, 13, 31, 61\}$, and so $56\,786\,730 \mid mn(m^{60} - n^{60})$.

(13a) First, $11.31 = 341$. Now, by Fermat's little theorem, we have that $2^{10} \equiv 1 \pmod{11}$; hence $2^{10.34} \equiv 1 \pmod{11}$, so $2^{341} \equiv 2 \pmod{11}$, i.e. $11 \mid 2^{341} - 2$. We also have that $2^5 = 32 \equiv 1 \pmod{31}$; hence $2^{340} = 2^{5.68} \equiv 1 \pmod{31}$, so $2^{341} \equiv 2 \pmod{31}$, i.e. $31 \mid 2^{341} - 2$. Since $\gcd(11, 31) = 1$, we obtain $11.31 \mid 2^{341} - 2$, i.e. $2^{341} \equiv 2 \pmod{11.31}$.

(13b) Likewise. Note that $19.73 = 1387 = 18.77 + 1$ and that $2^9 = 512 = 73.7 + 1$.

(14) The powers of 2 leave repeating reminders $2, 4, 1, 2, 4, 1, \ldots$ modulo 7. Therefore:

1. $7 \mid 2^n - 1$ iff $n \equiv 0 \pmod{3}$.

2. The reminders modulo 7 of $2^n + 1$ are $3, 5, 2, 3, 5, 2, \ldots$.

(15) The condition is equivalent to $1000 \mid 1978^n - 1978^m = 1978^m(1978^{n-m} - 1)$. Since $1000 = 2^3 \times 5^3$ and $(1978^{n-m} - 1)$ is odd, it must be the case that $2^3 \mid 1978^m$. Since $1978 = 2 \times 989$ the minimal value of m for which this is possible is $m = 3$. Then n must be the least integer greater than 3 such that $5^3 \mid 1978^{n-3} - 1$. Given that $\phi(5^3) = 5^2 \times (5-1) = 100$ and $\gcd(125, 1978) = 1$, by Euler's theorem we find that $n = \phi(5^3) + 3 = 103$ suffices. Then, the least such n will be $k + 3$, where k is the least positive integer such that $1978^k \equiv 1 \pmod{125}$. This k must be a divisor of 100. Note, further, that the least power of 1978 that leaves remainder 1 modulo 5 is 1978^4; hence $4 \mid k$, so k can only be $4, 20$ or 100. We find that $1978 \equiv 103 \pmod{125}$, so $1978^2 \equiv 103^2 = 10\,609 \equiv 109 \equiv -16 \pmod{125}$; hence $1978^4 \equiv (-16)^2 = 256 \equiv 6 \pmod{125}$. Then $1978^{20} \equiv 6^5 = 7776 \equiv 26 \pmod{125}$. Therefore, $k = 100$ and hence $n = 103$ is the least possible value of n. Thus, the solution is $m = 3$ and $n = 103$.

5.10. Wilson's theorem. Order of an integer

(1) Let $n > 4$. By Wilson's theorem, if n is prime, then $(n-1)! \equiv -1 \pmod{n}$; hence, $(n-1)! \not\equiv 0 \pmod{n}$. For the converse, suppose n is composite. We will consider two cases:

Case 1: n is the product of two different positive integers, i.e. n = ab, where $2 \le a < b \le n - 1$.

Then both a and b appear in the product

$$(n-1) \times (n-2) \times \cdots \times 2 \times 1.$$

Hence, ab is a factor of $(n-1)!$, so $n \mid (n-1)!$. We thus have that $(n-1)! \equiv 0 \pmod{n}$.

Case 2: n is a square of a prime, i.e. $n = p^2$ for a prime p.

Since $n > 4$, we have $p < 2p < p^2 = n$. This means that p and $2p$ appear in the product

$$(n-1) \times (n-2) \times \cdots \times 2 \times 1.$$

Hence, p^2 is a factor of $(n-1)!$. Therefore, $n \mid (n-1)!$, which means that $(n-1)! \equiv 0 \pmod{n}$.

(3) Hint: let n be a positive integer, $\gcd(n, a) = 1$, $k = \operatorname{ord}_n a$ and m be any positive integer. Let, further, $d = \gcd(k, m)$. Then $(a^m)^{k/d} = (a^{m/d})^k = (a^k)^{m/d} \equiv 1^{m/d} = 1 \pmod{n}$. Suppose $(a^m)^l \equiv 1 \pmod{n}$ for some positive integer $l < k/d$. Then we reach a contradiction with the assumption that k is the least positive integer such that $a^k \equiv 1 \pmod{n}$.

(4) Note that $k = p - h - 1$ and $h! \equiv (-1)^h (p-1)(p-1) \cdots (p-h) \pmod{p}$. Therefore:

$$\begin{aligned} h!k! &\equiv (-1)^h (p-1)(p-1) \cdots (p-h)(p-h-1) \cdots 1 \\ &= (-1)^h (p-1)! \equiv (-1)^h (-1) = -(-1)^h \pmod{p}, \end{aligned}$$

where the third step follows from Wilson's theorem.

(5) Since $\gcd(n, p-1) = 1$, there is an integer u such that $un \equiv 1 \pmod{p-1}$, so $un = q(p-1) + 1$. Then we will show that $1^n, 2^n, \ldots, (p-1)^n$ forms a reduced residue system modulo p, from which the claim of the exercise follows. It suffices to show that for any $1 < x < y < p - 1$, $x^n \not\equiv y^n \pmod{p}$. Suppose the contrary. Then $x^{un} \equiv y^{un} \pmod{p}$. By Fermat's little theorem, $x^{p-1} \equiv 1 \pmod{p}$, and hence, $x^{un} = x^{q(p-1)+1} = x^{q(p-1)} \cdot x \equiv x \pmod{p}$. Likewise, $y^{un} \equiv y \pmod{p}$. Thus, we find that $x \equiv y \pmod{p}$, which is impossible.

(6) Suppose n is composite. Then $\phi(n) < n - 1$. Since $a^{n-1} \equiv 1 \pmod{n}$ it follows that $\gcd(a, n) = 1$. Then, by Theorem 5.10.3, $\operatorname{ord}_n a \mid \phi(n)$, which contradicts the condition.

5.11. Application: public key cryptography

(1a) The word "HELP", encoded in ASCII as (72, 69, 76, 80), is encrypted as

$$(72^{77} \text{ rem } 403, 69^{77} \text{rem} 403, 76^{77} \text{ rem } 403, 80^{77} \text{ rem } 403)$$
$$= (193, 49, 72, 45).$$

(1b) The ASCII code encrypted as (45, 208, 148, 148) is decrypted as

$$(46^{173} \text{ rem } 403, 208^{173} \text{ rem } 403, 148^{173} \text{ rem } 403, 148^{173} \text{ rem } 403)$$
$$= (80, 65, 83, 83).$$

The encoded word is therefore "PASS".

(2a) We have to solve the following congruence:

$$11x \equiv 1 \pmod{120}.$$

First, we calculate $\gcd(11, 120) = 1$. Now, we look for integers u and v such that $11u + 120v = 1$, we get $v = 11$ and $v = -1$. Thus, one solution is $x_0 = \frac{(11)(1)}{1} = 11$. Therefore, the minimal d is 11.

(2b) The word "STOP", encoded in ASCII as (83, 84, 79, 80), is encrypted as

$$(83^{11} \text{ rem } 143, 84^{11} \text{ rem } 143, 79^{11} \text{ rem } 143, 80^{11} \text{ rem } 143)$$
$$= (138, 128, 79, 124).$$

(2c) (111, 4, 88, 57, 116, 67) is decrypted as

$$(111^{11} \text{ rem } 143, 4^{11} \text{ rem } 143, 88^{11} \text{ rem } 143, 57^{11} \text{ rem } 143, 116^{11} \text{ rem } 143, 67^{11} \text{ rem } 143)$$
$$= (67, 114, 121, 112, 116, 111).$$

The encoded word is therefore "Crypto".

(3a) We have to solve the following congruence:

$$143x \equiv 1 \pmod{2520}.$$

First, we calculate $\gcd(143, 2520) = 1$. Looking for integers u and v such that $143u + 2520v = 1$, we get $u = -793$ and $v = 45$. Hence, one solution is $x_0 = \frac{(-793)(1)}{1} = -793$. Therefore, the minimal d is 1727.

(3b) The word "ONE", encoded in ASCII as (79, 78, 69), is encrypted as

$$(79^{143} \text{ rem } 2623, 78^{143} \text{ rem } 2623, 69^{143} \text{ rem } 2623)$$
$$= (92, 1466, 2342).$$

(3c) (2, 3, 4, 5) is decrypted as

$$(2^{1727} \text{ rem } 2623, 3^{1727} \text{ rem } 2623, 4^{1727} \text{ rem } 2623, 5^{1727} \text{ rem } 2623)$$
$$= (505, 845, 594, 158).$$

(4a) We have to solve the following congruence:

$$125x \equiv 1 \pmod{2592}.$$

First, we have $\gcd(125, 2592) = 1$. Now, looking for integers u and v such that $125u + 2592v = 1$, we get $u = -1099$ and $v = 53$. Hence, one solution is $x_0 = \frac{(-1099)(1)}{1} = -1099$. Therefore, the minimal e is 1493.

(4b) The word "SECRET", encoded in ASCII as (83, 69, 67, 82, 69, 84), is encrypted as

$$(83^{1493} \text{ rem } 2701, 69^{1493} \text{ rem } 2701, 67^{1493} \text{ rem } 2701, 82^{1493} \text{ rem } 2701,$$
$$69^{1493} \text{ rem } 2701, 84^{1493} \text{ rem } 2701) = (2253, 237, 280, 430, 237, 248).$$

(4c) $(1, 11, 111, 1111)$ is decrypted as

$$(1^{125} \text{ rem } 2701, 11^{125} \text{ rem } 2701, 111^{125} \text{ rem } 2701, 1111^{125} \text{ rem } 2701) = (1, 175, 851, 2295).$$

(5) We have to solve the following congruence:

$$55x \equiv 1 \pmod{8736}.$$

First, $\gcd(55, 8736) = 1$. Now, looking for integers u and v such that $55u + 8736v = 1$, we get $u = -953$ and $v = 6$. Hence, one solution is $x_0 = \frac{(-953)(1)}{1} = -953$. Therefore, the minimal d is 7783.

6

Combinatorics

6.1. Two basic counting principles

(1) By the Multiplication Principle, there are $3 \times 5 = 15$ flights passing through London.

(2a) By the Multiplication Principle, there are $25 \times 6 \times 7 \times 4 = 4200$ meals.

(2b) We ignore beverages. There are 6 ways to select a starter, 7 ways to select the main course and 1 way to choose the desert. Thus, by the Multiplication Principle, there are $6 \times 7 \times 1 = 42$ meals.

(2c) By the Multiplication Principle, there are $6 \times 2 \times 4 = 48$ meals.

(3) 9^4

(4) $10!$ and $8! \times 3! = 241\,920$ if Rob, Alice and Lee want to stay together.

(5a) $12! = 479\,001\,600$

(5b) $\frac{12!}{12} = 11! = 39\,916\,800$

(6a) $7! - 6! = 4320$

(6b) $2 \times 6! = 1440$

(7) $10!$ and $5! \times 5! \times 2$ if men and women must alternate seats.

(8a) $4 \times 3 + 2 = 14$

(8b) $14 \times 14 = 196$

(8c) $(3 \times 2) + (1 \times 3) + 2 = 11$

(8d) $4 + 2 \times 3 = 10$

(9) There are two cases. In the first case, Alice picks a CD and then Bob picks a CD from the remaining 11 CDs and a book from the 9 books. In the second case, Alice picks a book and Bob picks a book from the remaining 8 books and a CD from 12 CDs. In total, this can be done in $12 \times 11 \times 9 + 9 \times 12 \times 8 = 2052$ ways.

(10) The lowest total you can roll is 2 and the highest is 12. The only numbers divisible by 3 between 2 and 12 are 3, 6, 9 and 12. There are only 2 ways to roll a total of 3, namely 1 and 2 or 2 and 1. Similarly, there are 5 ways to roll 6, 4 ways to roll 9 and 1 way to roll 12. Hence, by the Addition Principle, there are $2 + 5 + 4 + 1 = 12$ ways to roll a sum divisible by 3.

Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

(11) There are $21^3 \times 10^3 = 9\ 261\ 000$ possible license plates.

(12a) $P(6,4) = \frac{6!}{(6-4)!} = 6 \times 5 \times 4 \times 3 = 360$

(12b) Fix the letter a in one of four positions. This can be done in 4 ways. Then for the remaining three positions, there are $P(5,3) = \frac{5!}{(5-3)!} = 5 \times 4 \times 3 = 60$ possibilities since we select 3 letters from the remaining 5. Thus, there are $4 \times 60 = 240$ possible words.

(12c) There are $P(4,4) = 4! = 24$ words containing neither a nor b. Thus, there are $360 - 24 = 336$ words containing at least one of a and b.

(12d) Fix the letter a in one of four positions. This can be done in 4 ways. Then we must fill the remaining three positions with the letters c, d, e and f, and this can be done in $P(4,3) = \frac{4!}{(4-3)!} = 4 \times 3 \times 2 = 24$ ways. Thus, there are $4 \times 24 = 96$ possible words.

(12e) By symmetry, and from Exercise 12 (d), there are 96 words containing b but not a. Hence, there are $96 + 96 = 192$ words containing exactly one of a and b.

(12f) First, assign a to any of the four positions and then b to any of the remaining three positions. Then assign any two of the remaining four letters c, d, e and f to the remaining two positions. This can be done in $P(4,2) = \frac{4!}{(4-2)!} = 4 \times 3 = 12$ ways. Thus, there are $4 \times 3 \times 12 = 144$ words. Alternatively, subtract answer (e) from answer (c).

(13a) $6^4 = 1296$

(13b) There are 5^4 words not containing a. Hence, there are $6^4 - 5^4 = 671$ words containing a.

(13c) There are 4^4 words containing neither a nor b. Thus, there are $6^4 - 4^4 = 1040$ words containing at least one of a and b.

(13d) Since the word may not contain b, we restrict our attention to the five letters a, c, d, e and f. There are 5^4 such words in total of which 4^4 do not contain a. Hence, there are $5^4 - 4^4 = 369$ words containing a but not b.

(13e) By symmetry, and from (d), there are $369 + 369 = 738$ words.

(13f) Subtract answer (e) from answer (c). There are $1040 - 738 = 302$ such words.

(14) From 1 to 100, 4 is written $10 + 10 = 20$ times, from 101 to 1000, 4 is written $(9 \times 10) + (9 \times 10) + 100 = 280$ times and from 1001 to 10 000 it is written $(9 \times 10 \times 10) + (9 \times 10 \times 10) + (9 \times 10 \times 10) + 1000 = 3700$ times. Thus, by the Addition Principle, the digit 4 is written $20 + 280 + 3700 = 4000$ times.

(15) Such a product has the form $2^i \times 3^j \times 5^k \times 7^\ell$, where $0 \le i \le 3$, $0 \le j \le 1$, $0 \le k \le 2$, $0 \le \ell \le 1$. There are $4 \times 2 \times 3 \times 2$ such products. However, we need to impose the constraint that at least two of i, j, k and ℓ are nonzero – there is one product in which all of them are zero and 4 products in which exactly one is nonzero. Thus the correct number is $4 \times 2 \times 3 \times 2 - (1 + 4) = 43$.

(16a) 2^n

(16b) $2 \times 2^{n-2} = 2^{n-1}$

(16c) $2 \times 2^{n-2} = 2^{n-1}$

(16d) $2 \times 1^{n-1} = 2$

(17a) 3^n

(17b) $3 \times 3^{n-2} = 3^{n-1}$

(17c) $6 \times 3^{n-2} = 2 \times 3^{n-1}$

(17d) $3 \times 2^{n-1}$

(18) $\sum_{n=1}^{10} 6^n$

6.2. Combinations. The binomial theorem

(1a) $\binom{22}{5} = \frac{22!}{5!17!} = 26\,334$

(1b) There are $\binom{19}{5} = 11628$ ways to choose a committee containing no electrical engineers, so there are $26\,334 - 11\,628 = 14\,706$ ways to choose a committee containing at least one electrical engineer.

(1c) $\underbrace{\binom{22}{5}}_{\text{total}} - \left[\underbrace{\binom{12}{5} + \binom{7}{5}}_{\text{only one type}} + \underbrace{\binom{19}{5} + \binom{15}{5} + \binom{10}{5}}_{\text{only two types}}\right] = 10\,638$

(1d) Note that such a committee can only consist of 0 electrical engineers, 1 civil engineer and 4 mechanical engineers, or 0 electrical engineers, 2 civil engineers and 3 mechanical engineers. Hence, by the multiplicative principle, there are $\binom{7}{1} \times \binom{12}{4} + \binom{7}{2} \times \binom{12}{3} = 8\,085$ ways to choose the committee.

(2) There are $\binom{8}{3}$ ways to choose 3 ladies from 8 and there are $\binom{7}{4}$ ways to choose 4 men from 7, so there are $\binom{8}{3} \times \binom{7}{4} = 1960$ committees in total. Now, suppose Mrs Smith refuses to serve with Mr Jones. The number of committees containing both Mrs Smith and Mr Jones is $\binom{7}{2} \times \binom{6}{3} = 420$, since, after choosing Mrs Smith, we need to select two other women from the remaining seven and, after choosing Mr Jones, we need to select three other men from the remaining six. Hence, there will be $1960 - 420 = 1540$ committees that do not contain both Mrs Smith and Mr Jones.

(3a) $5 \times 6 = 30$

(3b) $P(15, 4) = 32\,760$

(3c) $P(8, 3) = 336$

(3d) $P(26, 4) = 358\,800$

(3e) $10! = 3628\,800$

(3f) $6! \times 4! = 17\,280$

(3g) First, decide the order in which the three subjects must appear in 3! ways. Then the 8 math books (respectively, 5 physics books and 7 chemistry books) can be arranged in 8! (respectively, 5! and 7!) ways. Hence, there is a total of $3! \times 8! \times 5! \times 7!$ arrangements.

(4a) $\binom{13}{11} = \frac{13!}{11!2!} = 78$

(4b) $\binom{6}{3} \times \binom{7}{5} = \left(\frac{6!}{3!3!}\right) \times \left(\frac{7!}{5!2!}\right) = 420$

(4c) $\binom{6}{3} \times \binom{9}{8} \times \binom{4}{2} \times \binom{5}{2} = \left(\frac{6!}{3!3!}\right) \times \left(\frac{9!}{8!1!}\right) \times \left(\frac{41}{2!2!}\right) \times \left(\frac{5!}{2!3!}\right) = 10\,800$

(4d) $\binom{52}{13} \times \binom{39}{13} \times \binom{26}{13} \times \binom{13}{13} = \frac{52!}{13!13!13!13!}$

(5) $\binom{15}{7} \times \binom{8}{8} n = \frac{15!}{7!8!} = 6435$

(6) $\binom{64}{8} \times \binom{56}{8}$

(7) 2^n

(8a) $\binom{8}{4} = \frac{8!}{4!4!} = 70$

(8b) $\binom{7}{4} = \frac{7!}{4!3!} = 35$

(8c) $\binom{7}{5} = \frac{7!}{5!2!} = 21$

(8d) $\binom{5}{4} = \frac{5!}{4!1!} = 5$

(8e) $\binom{8}{4} + \binom{8}{5} + \binom{8}{6} + \binom{8}{7} + \binom{8}{8} = \frac{8!}{4!4!} + \left(\frac{8!}{5!3!}\right) + \left(\frac{8!}{6!2!}\right) + \left(\frac{8!}{7!1!}\right) + \left(\frac{8!}{8!0!}\right) = 163$

(8f) $1 + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} + \binom{8}{4} + \binom{8}{5} + \binom{8}{6} = 1 + 8 + \left(\frac{8!}{6!2!}\right) + \left(\frac{8!}{5!3!}\right) + \left(\frac{8!}{4!4!}\right) + \left(\frac{8!}{3!5!}\right) + \left(\frac{8!}{2!6!}\right) = 247$

(9a) $\binom{60}{5} = 5\,461\,512$

(9b) Since the jobs are different, we have to select 5 candidates from 60, where the order in which they are selected matters. Thus, there are

$$P(60,5) = \frac{60!}{(60-5)!} = 60 \times 59 \times 58 \times 57 \times 56 = 655\,381\,440$$

ways to fill the vacancies.

(9c) First, choose 3 applicants for the functional analysis positions. This can be done in $\binom{60}{3}$ ways. Then choose 2 applicants from the remaining 57 applicants for the universal algebra positions in $\binom{57}{2}$ ways. Thus, all five jobs can be assigned in $\binom{60}{3}\binom{57}{2} = 54\,615\,120$ ways.

(10) Let $|S| = n$. Then we know that $\binom{n}{5} \geq 100$, so $n \geq 9$.

(11) The number of subsets of size 5 is $\binom{m}{5}$, whereas the number of subsets of size 5 containing the element 2 is $\binom{m-1}{4}$. Thus, we have the equation

$$\binom{m-1}{4} = \frac{1}{4}\binom{m}{5},$$

which becomes

$$\frac{(m-1)!}{(m-5)!\,4!} = \frac{1}{4}\frac{m!}{(m-5)!\,5!}.$$

This gives

$$\frac{m!}{(m-1)!} = \frac{5!}{3!}$$

and so $m = 20$.

(12a) $(x+1)^7$

$= \binom{7}{0}x^7 + \binom{7}{1}x^6 + \binom{7}{2}x^5 + \binom{7}{3}x^4 + \binom{7}{4}x^3 + \binom{7}{5}x^2 + \binom{7}{6}x + \binom{7}{7}$

$= x^7 + 7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x + 1$

(12c) $(3x - \frac{1}{2})^3$

$= \binom{3}{0}(3x)^3 + \binom{3}{1}(3x)^2(-\tfrac{1}{2}) + \binom{3}{2}(3x)(-\tfrac{1}{2})^2 + \binom{3}{3}(-\tfrac{1}{2})^3$

$= 27x^3 - \frac{27}{2}x^2 + \frac{9}{4}x - \frac{1}{8}$

(13a) $(3x - 2y)^4$

$= \binom{4}{0}(3x)^4 + \binom{4}{1}(3x)^3(-2y) + \binom{4}{2}(3x)^2(-2y)^2 + \binom{4}{3}(3x)(-2y)^3 + \binom{4}{4}(-2y)^4$

$= 81x^4 - 216x^3y + 216x^2y^2 - 96xy^3 + 16y^4$

(13b) $(x^2 + 3y^2)^5$

$= (x^2)^5 + \binom{5}{1}(x^2)^4(3y^2) + \binom{5}{2}(x^2)^3(3y^2)^2 + \binom{5}{3}(x^2)^2(3y^2)^3 + \binom{5}{4}(x^2)(3y^2)^4 + \binom{5}{5}(3y^2)^5$

$= x^{10} + 15x^8y^2 + 90x^6y^4 + 270x^4y^6 + 405x^2y^8 + 243y^{10}$

(14a) Since

$$(x+1)^8 = \sum_{r=0}^{8}\binom{8}{r}x^{8-r},$$

the coefficient of x^6 is obtained when $r = 2$, which gives $\binom{8}{2} = 28$.

(14c) Since

$$(3x-4y)^{13}=\sum_{r=0}^{13}\binom{13}{r}(3x)^{13-r}(-4y)^r,$$

the coefficient of x^8y^5 is obtained when $r=5$, which gives $\binom{13}{5}\times 3^{13-5}\times(-4)^5=-\quad 3^8\times 4^5\times\binom{13}{5}$.

6.3. The Principle of Inclusion – Exclusion

(1) Let U be the set of households and let T and E be the sets of households that subscribe to *TIME* and *The Economist*, respectively.

(1a) The number of households subscribing to at least one is

$$\begin{aligned}|T\cup E| &= |T|+|E|-|T\cap E|\\ &= 83+41-32\\ &= 92.\end{aligned}$$

Therefore, the number subscribing to neither is

$$|U|-|T\cup E| = 100-92=8.$$

(1b) The number subsribing to precisely one is

$$|T\cup E|-|T\cap E| = 92-32=60.$$

(2) Let U be the set of all students and let M, S and Z be the sets of mathematics, statistics and zoology students, respectively.

(2a) The number of students who taking at least one of the three subjects is

$$\begin{aligned}|M\cup S\cup Z| &= |M|+|S|+|Z|-|M\cap S|-|M\cap Z|-|S\cap Z|+|M\cap S\cap Z|\\ &= 75+70+75-40-35-20+15\\ &= 140.\end{aligned}$$

(2b) The number of students taking mathematics and statistics but not zoology is

$$|(M\cap S)\setminus Z| = |M\cap S|-|M\cap S\cap Z| = 40-15=25.$$

Likewise,

$$|(M\cap Z)\setminus S| = 20 \text{ and } |(S\cap Z)\setminus M| = 5.$$

Therefore, the number of students taking exactly two subjects is $25+20+5=50$. Since the number of students taking three subjects is 15, the number of students taking exactly one subject is $140-50-15=75$.

(2c) The number of students taking statistics or mathematics but not zoology is

$$\begin{aligned}|(S\cup M)\setminus Z| &= |S\cup M|-|(S\cup M)\cap Z|\\ &= |S\cup M|-|(S\cap Z)\cup(M\cap Z)|\\ &= (|S|+|M|-|S\cap M|)-(|S\cap Z|+|M\cap Z|-|S\cap M\cap Z|)\\ &= (70+75-40)-(20+35-15)\\ &= 65.\end{aligned}$$

(2d) There are 50 students taking exactly two subjects, so there are $200 - 50 = 150$ students not taking exactly two subjects.

(2e) The number of students who take neither statistics nor mathematics is

$$\begin{aligned}|(S \cup M)^c| &= |U| - |S \cup M| \\ &= |U| - (|S| + |M| - |S \cap M|) \\ &= 200 - (70 + 75 - 40) \\ &= 95.\end{aligned}$$

(3) Let S be the set of all positive four-digit integers. Then $|S| = 9 \times 10^3$. Let S_0 and S_3 be the subsets of S consisting of all positive four-digit integers containing no 0's and 3's, respectively. Clearly, $|S_0| = 9^4$ and $|S_3| = 8 \times 9^3$. We also have $|S_0 \cap S_3| = 8^4$.

(3a) The number of four-digit integers that miss at least one of the digits 0 and 3 is

$$\begin{aligned}|S_0 \cup S_3| &= |S_0| + |S_3| - |S_0 \cap S_3| \\ &= 9^4 + 8 \times 9^3 - 8^4 \\ &= 8297.\end{aligned}$$

(3b) The number of four-digit integers that contain at least one of the digits 0 and 3 is

$$\begin{aligned}|S \ (S_0 \cap S_3)| &= |S| - |S_0 \cap S_3| \\ &= p \times 10^3 - 8^4 \\ &= 4904.\end{aligned}$$

(4) Let U be the set of movie goers and let A, C and D be the sets of movie goers who like action, comedy and drama, respectively.

(4a) The number of movie goers who like to watch action but not comedy is

$$|A| - |A \cap C| = 95 - 35 = 60.$$

(4b) The number of movie goers who like to watch action or comedy but not drama is

$$\begin{aligned}|(A \cup C) - D| &= |A \cup C| - |(A \cup C) \cap D| \\ &= |A \cup C| - |(A \cap D) \cup (C \cup D)| \\ &= |A| + |C| - |A \cap C| - (|A \cap D| + |C \cap D| - |A \cap C \cap D|) \\ &= 95 + 125 - 35 - 25 - 45 + 5 \\ &= 120.\end{aligned}$$

(4c) The number of movie goers who like to watch action or comedy is

$$|A \cup C| = |A| + |C| - |A \cap C| = 95 + 125 - 35 = 185.$$

(4d) The number of movie goers who do not watch comedy only is

$$\begin{aligned}|(C - (A \cup D))^c| &= |U| - |C - (A \cup D)| \\ &= |U| - (|C| - |C \cap (A \cup D)|) \\ &= |U| - |C| + |(C \cap A) \cup (C \cap D)| \\ &= |U| - |C| + |C \cap A| + |C \cap D| - |C \cap A \cap D| \\ &= 250 - 125 + 35 + 45 - 5 \\ &= 200.\end{aligned}$$

(4e) The number of movie goers who like to watch comedy and drama but not action is

$$|(C \cap D) \backslash A| = |C \cap D| - |C \cap D \cap A| = 45 - 5 = 40.$$

(5) Let C, L and N be the sets of mathematicians who like Combinatorics, Logic and Number Theory, respectively. Note that $L \subseteq N$, and therefore $L \cap N = L$ and $L \cap C = L \cap N \cap C$. Then the number of mathematicians at the meeting who like at least one of these three subjects is

$$\begin{aligned}
&|C \cup L \cup N| \\
&= |C| + |L| + |N| - |C \cap L| - |C \cap N| - |L \cap N| + |C \cap L \cap N| \\
&= 22 + 14 + 25 - 5 - 9 - 14 + 5 \\
&= 38.
\end{aligned}$$

(6) Let S be the set of all positive 6-digit integers. Then $|S| = 9 \times 10^5 = 900\,000$. Let S_2, S_4 and S_6 be the subsets of S consisting of all 6-digit integers containing no 2's, 4's and no 6's, respectively. Then $|S_2 \cap S_4 \cap S_6| = 6 \times 7^5 = 100\,842$. Hence, the number of 6-digit integers containing 2, 4 or 6 is

$$|S_2^c \cup S_4^c \cup S_6^c| = |S| - |S_2 \cap S_4 \cap S_6| = 900\,000 - 100\,842 = 799\,158.$$

(7) Let S_3 and S_4 be the sets of integers less than or equal to 2013 divisible by 3 and 4, respectively. Then $|S_3| = 671$, $|S_4| = 503$ and $|S_3 \cap S_4| = 167$. Hence, the number of positive integers less than or equal to 2013 divisible by 3 or 4 is

$$|S_3 \cup S_4| = |S_3| + |S_4| - |S_3 \cap S_4| = 671 + 503 - 167 = 1007.$$

(8) Let S_3, S_4 and S_5 be the sets of integers less than or equal to 2013 divisible by 3, 4 and 5, respectively. Then $|S_3| = 671$, $|S_5| = 402$, $|S_3 \cap S_4| = 167$, $|S_3 \cap S_5| = 134$, $|S_4 \cap S_5| = 100$ and $|S_3 \cap S_4 \cap S_5| = 33$. Hence, the number of positive integers less than or equal to 2013 divisible by 3 or 5 but not 4 is

$$\begin{aligned}
&|(S_3 \cup S_5) \backslash S_4| = |S_3| + |S_5| - |S_3 \cap S_5| - |(S_3 \cup S_5) \cap S_4| \\
&= |S_3| + |S_5| - |S_3 \cap S_5| - (|(S_3 \cap S_4) \cup (S_5 \cap S_4)|) \\
&= |S_3| + |S_5| - |S_3 \cap S_5| - (|S_3 \cap S_4| + |S_5 \cap S_4| - |S_3 \cap S_4 \cap S_5|) \\
&= 671 + 402 - 134 - 167 - 100 + 33 \\
&= 705.
\end{aligned}$$

(9) Using the Inclusion – Exclusion Principle for five sets, we know that

$$\begin{aligned}
&5 \times 10 - \binom{5}{2} \times 5 + \binom{5}{3} \times 3 - \binom{5}{4} \times 2 + 1 \\
&= 50 - 50 + 30 - 10 + 1 \\
&= 21.
\end{aligned}$$

Computers have at least one of the additional features. Hence, the company have $21 + 6 = 27$ computers in stock.

(10) Using the Inclusion – Exclusion Principle for six sets, we know there are

$$\begin{aligned}
&6 \times 5! - \binom{6}{2} \times 4! + \binom{6}{3} \times 3! - \binom{6}{4} \times 2! + \binom{6}{5} \times 1! - 1 \\
&= 720 - 360 + 120 - 30 + 6 - 1 \\
&= 455.
\end{aligned}$$

arrangements that have at least one letter in its original position. Hence, there are $6! - 455 = 265$ arrangements in which no letter is in its original position.

(11) Let S be the set of all permutations of the 26 letters from the alphabet and let S_{SO}, S_{SHE} and S_{WINS} be the sets of permutations containing the sequences SO, SHE and WINS, respectively. Then the number of permutations containing at least one of the squences SO, SHE or WINS is

$$\begin{aligned}
&|S_{\text{SO}} \cup S_{\text{SHE}} \cup S_{\text{WINS}}| \\
&= |S_{\text{SO}}| + |S_{\text{SHE}}| + |S_{\text{WINS}}| - |S_{\text{SO}} \cap S_{\text{SHE}}| - |S_{\text{SO}} \cap S_{\text{WINS}}| - |S_{\text{SHE}} \cap S_{\text{WINS}}| \\
&\quad + |S_{\text{SO}} \cap S_{\text{SHE}} \cap S_{\text{WINS}}| \\
&= 25! + 24! + 23! - 0 - 22! - 21! + 0.
\end{aligned}$$

Hence, the number of permutations that contain none of the sequences SO, SHE or WINS is

$$\begin{aligned}
&|\overline{S_{\text{SO}} \cup S_{\text{SHE}} \cup S_{\text{WINS}}}| \\
&= |S| - |S_{\text{SO}} \cup S_{\text{SHE}} \cup S_{\text{WINS}}| \\
&= 26! - 25! - 24! - 23! + 22! + 21!.
\end{aligned}$$

(12) Let S be the set of all permutations of the 26 letters from the alphabet and let S_{HE}, S_{WAS}, S_{SO} and S_{BAD} be the sets of permutations containing the sequences HE, WAS, SO and BAD, respectively. Then the number of sequences containing at least one of these four sequences is

$$\begin{aligned}
&|S_{\text{HE}} \cup S_{\text{WAS}} \cup S_{\text{SO}} \cup S_{\text{BAD}}| \\
&= |S_{\text{HE}}| + |S_{\text{WAS}}| + |S_{\text{SO}}| + |S_{\text{BAD}}| - |S_{\text{HE}} \cap S_{\text{WAS}}| - |S_{\text{HE}} \cap S_{\text{SO}}| \\
&\quad - |S_{\text{HE}} \cap S_{\text{BAD}}| - |S_{\text{SO}} \cap S_{\text{WAS}}| - |S_{\text{WAS}} \cap S_{\text{BAD}}| - |S_{\text{SO}} \cap S_{\text{BAD}}| \\
&\quad |S_{\text{HE}} \cap S_{\text{WAS}} \cap S_{\text{SO}}| + |S_{\text{HE}} \cap S_{\text{WAS}} \cap S_{\text{BAD}}| + |S_{\text{HE}} \cap S_{\text{SO}} \cap S_{\text{BAD}}| + \\
&\quad + |S_{\text{WAS}} \cap S_{\text{SO}} \cap S_{\text{BAD}}| - |S_{\text{HE}} \cap S_{\text{WAS}} \cap S_{\text{SO}} \cap S_{\text{BAD}}| \\
&= 25! + 24! + 25! + 24! - 23! - 24! - 23! - 23! - 0 - 23! + 22! + 0 + 22! + 0 - 0 \\
&= 2 \times 25! + 24! - 4 \times 23! + 2 \times 22!,
\end{aligned}$$

and so the number of sequences containing none of these four sequences is

$$\begin{aligned}
&|\overline{S_{\text{HE}} \cup S_{\text{WAS}} \cup S_{\text{SO}} \cup S_{\text{BAD}}}| \\
&= |S| - |S_{\text{HE}} \cup S_{\text{WAS}} \cup S_{\text{SO}} \cup S_{\text{BAD}}| \\
&= 26! - 2 \times 25! - 24! + 4 \times 23! - 2 \times 22!.
\end{aligned}$$

(14) Let S be the set of all sequences and S_i the set of sequences not containing any double i's for $1 \leq i \leq 6$. Then we are interested in the cardinality of the set $S - \bigcup_{i=1}^{6} S_i$. If the two identical dice are rolled once, then there can be 6 doubles and $\binom{6}{2}$ non-doubles. Hence, there are $6 + \binom{6}{2} = 21$ possible different outcomes of rolling the dice once. Now, if the dice are rolled n successive times, there are 21^n possible different sequences of outcomes. Therefore, for $i < j < k < l < m$,

$$\begin{gathered}
|S_i| = 20^n, \quad |S_i \cap S_j| = 19^n, \quad |S_i \cap S_j \cap S_k| = 18^n, \\
|S_i \cap S_j \cap S_k \cap S_l| = 17^n, \quad |S_i \cap S_j \cap S_k \cap S_l \cap S_m| = 16^n \text{ and} \\
|S_1 \cap S_2 \cap S_3 \cap S_4 \cap S_5 \cap S_6| = 15^n.
\end{gathered}$$

Hence,

$$\begin{aligned}
&|S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6| \\
&= 6 \times 20^n - \binom{6}{2} \times 19^n + \binom{6}{3} \times 18^n - \binom{6}{4} \times 17^n + \binom{6}{5} \times 16^n - 15^n,
\end{aligned}$$

which means that

$$\left|S - \bigcup_{i=1}^{6} S_i\right| = 21^n - \left(6 \times 20^n - \binom{6}{2} \times 19^n + \binom{6}{3} \times 18^n - \binom{6}{4} \times 17^n + \binom{6}{5} \times 16^n - 15^n\right).$$

6.4. The Pigeonhole Principle

(1) Let P be the set of socks and H the pairs of socks. Using the PHP, we know that $|P| > |H| = 19$, so choosing 20 socks will ensure that at least 1 pair is selected.

(2) Since $7 \times 14 = 98$, there are 14 integers in the range $1, \ldots, 100$ that are divisible by 7. Hence, the set S consisting of those integers in the range $1, \ldots, 100$ that are *not* divisible by 7 must have $100 - 14 = 86$ elements. By the PHP, there is no injective mapping from a set with 87 elements to S, so selecting 87 integers will guarantee a multiple of 7.

(3) Suppose there are n people in the group. If two people each have $n - 1$ friends, we are done, so suppose there is at most one person who has $n - 1$ friends. Then there are two cases:

Case 1: some person has $n - 1$ friends.

Then the number of friends that the remaining $n - 1$ people can have ranges from 1 to $n - 2$ (nobody in the group can have 0 friends since everyone is a friend of the person with $n - 1$ friends). Now, label the pigeonholes from 1 to $n - 2$ and let the pigeons be the remaining $n - 1$ people. Hence, by the PHP, there are two people with the same number of friends.

Case 2: nobody has $n - 1$ friends.

Then the number of friends that any person can have ranges from 0 to $n - 2$, i.e. $n - 1$ possibilities. However, there are n people, so by the PHP, at least two of them have the same number of friends.

(4) Let the pigeons be the chosen numbers and define the pigeonholes as the sets $\{1, 99\}, \{2, 98\}, \{3, 97\}, \ldots, \{49, 51\}, \{50, 50\}$. Notice that the numbers in each of the sets sum to 100. Since there are 50 pigeonholes, we must select 51 numbers according to the PHP.

(5) Let P be the set of people living in Johannesburg and H the number of hairs on their heads. Then $|P| > 4\ 000\ 000$ and $|H| \leq 200\ 000$, so $|P| > (20)(200\ 000)$. Hence, by the CPHP, at least 21 people in Johannesburg have exactly the same numbers of hairs on their heads.

(6) Let P be the set of people we select and H the set of nationalities. Therefore, by the CPHP with $k = 3$ and $|H| = 7$, $|P| > (3)(7) = 21$. Hence, choosing 22 people will ensure that at least 4 people are compatriots.

(7) Let P be the set of students and H the classes. Then $393 > (23)(17) = 391$, and so, by the CPHP, there is one class with at least $23 + 1 = 24$ students. However, if there was only one class with 24 students the school would accommodate at most $23 \times 16 + 24 = 392$ students. Thus, either 2 classes with at least 24 are needed, giving $2 \times 24 + 15 \times 23 = 393$, or one class with 25, giving $25 + 16 \times 23 = 393$.

(8) There are 26^2 ways to choose the first and last letters of any word. Since $2 \times 26^2 + 1 > 2 \times 26^2$, then, by the CPHP, with $m = 2 \times 26^2 + 1$, $k = 2$ and $n = 26^2$, choosing $2 \times 26^2 + 1$ (or any greater integer) words will guarantee having at least three that begin with the same letter and end with the same letter. The pigeons are the words we are choosing, while the pigeonholes are the 26^2 possibilities for first and last letters.

(9) We have $606 > 605 = (5)(121)$, so, by the CPHP, if we divide the square into a 11×11 grid so that each of the smaller squares has a side $\frac{1}{11}$, at least 6 points will end up in the same small square. The farthest apart any two points in this square can be is the length of its diagonal; that is, $\sqrt{\left(\frac{1}{11}\right)^2 + \left(\frac{1}{11}\right)^2} = \sqrt{\frac{1}{121} + \frac{1}{121}} = \sqrt{\frac{2}{121}} = \frac{\sqrt{2}}{11}$. Inscribe the square in a circle with diameter $\frac{\sqrt{2}}{11}$, i.e. a radius of $\frac{\sqrt{2}}{22}$. However, $\frac{1}{15} > \frac{\sqrt{2}}{22}$, so we can cover the six points with a circle of radius $\frac{1}{15}$.

(10a) Let P be the set of balls we select and H the set of different colours. To apply the CPHP, we need $|P| > (4)(4) = 16$, so choosing 17 or more balls will guarantee 5 balls of the same colour.

(10b) The worst case scenario is selecting all the blue, red and yellow balls without selecting any green balls. In total, we can select $13 + 10 + 6 = 29$ balls without selecting a green ball. Hence, we have to select at least 32 balls in order to make sure that there will be at least 3 green balls.

(10c) The worst case scenario is selecting all the blue, red and green balls without selecting a yellow ball. In total, we can select $13 + 10 + 8 = 31$ balls without selecting a yellow ball. Hence, we must select at least 32 balls to ensure we select at least one of each colour.

(11) Choose any one of the six people, say a. Then take the remaining five people and group those who like a in the set L and those who hate a in the set H. By the CPHP, one of these sets, say L, contains at least three people. If these three people hate each other, then we are done; otherwise, there must be two of them who like each other and, together with a, we then have three people who like each other. Likewise if the set H contains at least three people.

(14) Suppose there is a map from P to H that maps only finitely many elements of P to every element of H. Let m be the maximum number of elements of P mapped to any element of H. Then $|P| \leq m|H|$, which contradicts the fact that P is an infinite set.

(15) There are two possibilities:

Case 1: there are m distinct sets each containing n of the same integers.

$mn + 1 > mn$, so, by the CPHP, with $|P| = mn + 1$, $|H| = m$ and $k = n$, there is one such set containing $n + 1$ equal integers.

Case 2: there are n equal sets containing m distinct integers.

$mn + 1 > mn$, so, by the CPHP (with $|P| = mn + 1$, $|H| = n$ and $k = m$), one of these sets must contain at least $m + 1$ distinct integers.

(16) Note that the size of the subset is not specified, so it makes sense to consider the subsets of $\{m_1, \ldots, m_n\}$ as posets under inclusion. A natural inclusion structure is ascending chains, sequences of sets where one contains the next. If we define the subsets $T_k = \{m_1, \ldots, m_k\}$ for $k = 1, 2, \ldots, n$ the sum corresponding to T_k is $t_k = m_1 + m_2 + \cdots + m_k$ for $1 \leq k \leq n$. If t_k is a multiple of n for some k, we are done. Otherwise, let n be the pigeons and the remainders modulo n the pigeonholes. Then $|P| = n$ and $|H| = n - 1$. Therefore, by the PHP, there are at least two such sums, say t_i and t_j for $i < j$, that have the same remainder after division by n. Hence, by (CON1) of Theorem 5.5.3, n divides $t_j - t_i = m_{i+1} + \cdots + m_j$ and so the set $T_j - T_i$ works.

(17) Consider the sequence of integers

$$m \cdot 1 - 1, \quad m \cdot 2 - 1, \ldots, \quad m \cdot n - 1.$$

Choose any two integers in this sequence, say $m \cdot k_1 - 1$ and $m \cdot k_2 - 1 \pmod{n}$. Then $m \cdot k_1 - 1 \equiv m \cdot k_2 - 1 \pmod{n}$ iff $k_1 \equiv k_2$. Thus, no two of the n distinct members of the sequence are congruent modulo n. Therefore, the sequence represents a complete residue system modulo n. However, then one of its members is congruent to 0 modulo n, so there is a positive k such that n divides $m \cdot k - 1$.

(18) Let the powers of 7 be the pigeons and let the remainder they leave upon division by 100 000 000 the pigeonholes. Obviously there are 100 000 000 pigeonholes. Since there is an infinite number of powers of 7, two of them, say 7^m and 7^n with $m > n$, leave the same remainder upon division by 100 000 000. Hence, by (CON1) of Theorem 5.5.3, $7^m - 7^n = 7^n(7^{m-n} - 1)$ is a multiple of 100 000 000. Now, $100\,000\,000 = 2^8 \times 3^0 \times 5^8 \times 7^0$ and $7^n = 2^0 \times 3^0 \times 5^0 \times 7^n$, so $\gcd(100\,000\,000, 7^n) = 1$. We can thus use (RP2) of Theorem 5.4.1 to conclude that $100\,000\,000 \mid 7^{m-n} - 1$. This means that $7^{m-n} = 100\,000\,000k$ for some $k \in \mathbb{Z}^+$. Thus, $7^{m-n} = 100\,000\,000k + 1$, which clearly ends in 00000001.

(20) Consider the set $\{1, 2, 3, \ldots, m_{n+1} - 2, m_{n+1} - 1, m_{n+1}\}$. Note that since $1 \leq m_1 < \cdots < m_{n+1} \leq 2n$, all $n + 1$ integers $m_1, \ldots, m_{n+1}$ belong to this set. We now consider the following two cases:

Case 1: m_{n+1} is even.

Define the pigeonholes as the sets

$$\{1, m_{n+1} - 1\}, \{2, m_{n+1} - 2\}, \ldots, \left\{\frac{m_{n+1}}{2}, \frac{m_{n+1}}{2}\right\}.$$

Then there are obviously $\frac{m_{n+1}}{2}$ pigeonholes. Let the $n + 1$ integers $m_1, m_2, \ldots, m_{n+1}$ be the pigeons. Now, place them each into the pigeonhole corresponding to the set that contains it. However, since $m_{n+1} \leq 2n$, $\frac{m_{n+1}}{2} \leq n < n + 1$, and so, by the PHP, there will be one pigeonhole that contains two of the integers $m_1, \ldots, m_{n+1}$; clearly, from the way the pigeonholes were constructed, these integers add up to give m_{n+1} (note that at most one of the integers can go into the set $\left\{\frac{m_{n+1}}{2}, \frac{m_{n+1}}{2}\right\}$, so we do not end up with a problem).

Case 2: m_{n+1} is odd.

In this case, define the pigeonholes as the sets

$$\{1, m_{n+1} - 1\}, \{2, m_{n+1} - 2\}, \ldots, \left\{\frac{m_{n+1} - 1}{2}, \frac{m_{n+1} + 1}{2}\right\}.$$

Therefore there are $\frac{m_{n+1}-1}{2}$ pigeonholes. Again, let the $n + 1$ integers $m_1, m_2, \ldots, m_{n+1}$ be the pigeons. Place them each into the pigeonhole corresponding to the set that contains it. However, $m_{n+1} \leq 2n$, so $m_{n+1} - 1 \leq 2n - 1$, giving $\frac{m_{n+1}-1}{2} \leq \frac{2n-1}{2} < n + 1$. Hence, by the PHP, there is a pigeonhole that contains two of the integers $m_1, m_2, \ldots, m_{n+1}$, and, clearly, from the way the pigeonholes were constructed, their sum equals m_{n+1}.

(21) Let the pigeonholes be all the possible sums. Although we do not know what the 10 chosen numbers are, we know the range of the sums. First, since all the integers are positive, the sum must be at least 1. Furthermore, the sum is at most $91 + 92 + \cdots + 100 = 955$. Therefore, in total there are 955 pigeonholes. Now let the subsets of M be the pigeons. Obviously there are $2^{10} - 1 = 1023$ pigeons (nonempty subsets). Since $1023 > 955$, we know from the PHP that there are two subsets giving the same sum of elements. Note that these cannot be a subset of the other, for otherwise, they cannot have the same sum. If the two subsets are disjoint, we are done. If they have common elements, we may remove the common elements from both sets. It reduces the sums by the same amount, so the new subsets give the same sums again.

(22) By factoring out as many 2's from each of the integers from 1 to 200, we see that all of them can be written in the form $a \cdot 2^k$, where $k \geq 0$ and a is an odd integer. For the integers from 1 to 200, a will always be one of the 100 odd integers $1, 3, 5, \ldots, 199$. Since there are 101 integers in A, we know from the PHP that there are two integers in A with the same a value. Let us call them b and c, respectively. Then $b = a \cdot 2^m$ and $c = a \cdot 2^n$ for $m, n \in \mathbb{N}$. If $m > n$, then

$$b = a \cdot 2^m = a \cdot 2^n \cdot 2^{m-n} = c \cdot 2^{m-n},$$

which means that $c \mid b$. Similarly, if $n > m$,

$$c = a \cdot 2^n = a \cdot 2^m \cdot 2^{n-m} = b \cdot 2^{n-m},$$

and so $b \mid c$.

6.5. Generalized permutations, distributions and the multinomial theorem

(1a) $P(9; 1, 1, 1, 2, 2, 2)$ (1b) $P(11; 1, 2, 4, 4)$

(2) $P(18; 6, 5, 3, 4)$

(3a) $P(12; 6, 3, 3) + 4P(12; 5, 4, 3) + P(12; 4, 4, 4)$ (3b) 6

(4a) 5^{20} (4c) $P(20; 4, 4, 4, 4, 4)$

(4b) $P(20; 6, 6, 6, 1, 1)$

(5) $P(15; 5, 7, 3)$

(6a) $P(40; 10, 10, 10, 10)$ (6b) $P(40; 8, 8, 8, 8, 4, 4)$

(7a) Note that each box must contain one object, so distribute the n objects into n boxes, one per box. There are n boxes for the first object, $n-1$ boxes for the second object, etc. Hence, there are $n!$ distributions.

(7b) Pick which box must be empty in $\binom{n}{1} = n$ ways. Then pick which box must get two objects in $\binom{n-1}{1} = n-1$ ways and which two objects go into this box in $\binom{n}{2}$ ways. Then distribute the remaining $n-2$ objects into the remaining $n-2$ boxes, one per box, in $(n-2)!$ ways. Hence, in total there are $n \times (n-1) \times \binom{n}{2} \times (n-2)!$ distributions.

(7c) We subtract the number of distributions in which no box is empty from the total number of distributions: $n^n - n!$.

(7d) Choose which two boxes are empty in $\binom{n}{2}$ ways. Then there are two cases:

Case 1: one box gets three objects.

Choose the box in $n-2$ ways, then pick which three objects go into this box in $\binom{n}{3}$ ways. Then distribute the remaining $n-3$ objects into the remaining $n-3$ boxes in $(n-3)!$ ways. Hence, there are $\binom{n}{2} \times (n-2) \times \binom{n}{3} \times (n-3)!$ distributions.

Case 2: two boxes each get two objects.

Choose these two boxes in $\binom{n-2}{2}$ ways. Then choose two objects which go into the first of these two boxes and another two objects which go into the second of these two boxes in $\binom{n}{2} \times \binom{n-2}{2}$ ways. Finally, distribute the remaining $n-4$ objects into the remaining $n-4$ boxes in $(n-4)!$ ways. In this case, there are $\binom{n}{2} \times \binom{n-2}{2} \times \binom{n}{2} \times \binom{n-2}{2} \times (n-4)!$ distributions.

Hence, in total, there are

$$\binom{n}{2} \times \left((n-2) \times \binom{n}{3} \times (n-3)! + \binom{n-2}{2} \times \binom{n}{2} \times \binom{n-2}{2} \times (n-4)! \right)$$

distributions.

(8) Since

$$(x + 2y + 3z)^{12} = \sum_{n_1+n_2+n_3=12} P(12; n_1, n_2, n_3)x^{n_1}(2y)^{n_2}(3z)^{n_3},$$

to get the coefficient of $x^3y^6z^3$ we need $n_1 = 3$, $n_2 = 6$ and $n_3 = 3$. Hence, the coefficient is $P(12; 3, 6, 3) \times 2^6 \times 3^3 = 31\,933\,440$.

(9) Since

$$(x + 2y2 + 4z^3)^{10} = \sum_{n_1+n_2+n_3=10} P(10; n_1, n_2, n_3)x^{n_1}(2y^2)^{n_2}(4z^3)^{n_3},$$

to get the coefficient of $x^3y^6z^{12}$, we need $n_1 = 3$, $n_2 = 3$ and $n_3 = 4$. Hence, the coefficient is $P(10; 3, 3, 4) \times 2^3 \times 4^4 = 8601\,600$.

6.6. Selections and arrangements with repetition; distributions of identical objects

(1) Choose 5 hearts from 13 hearts, 3 spades from 13 spades, 4 diamonds from 13 diamonds and 1 club from 13 clubs. This can be done in $\binom{13}{5} \times \binom{13}{3} \times \binom{13}{4} \times \binom{13}{1}$ ways.

(2a) $C(26 + 12 - 1, 26)$

(2b) Give each child one sweet. This can be done in only one way because the sweets are identical. Then distribute the remaining 14 sweets amongst the children in $C(14 + 12 - 1, 14)$ ways. Hence, there are $C(14 + 12 - 1, 14)$ ways to distribute the sweets.

(2c) Again the problem is equivalent to finding the number of ways in which 14 sweets can be distributed amongst 12 children, but with the added constraint that no child may get more than 2 sweets. Consider the following cases: (i) 7 children get 2 sweets each, (ii) 6 children get 2 sweets and 2 children get 1 sweet, (iii) 5 children get 2 sweets and 4 children get 1 sweet, (iv) 4 children get 2 sweets and 6 children get 1 sweet, (v) 3 children get 2 sweets and 8 children get 1 sweet and (vi) 2 children get 2 sweets and 10 children get 1 sweet. Then there are

$$\binom{12}{7} + \binom{12}{6}\binom{6}{2} + \binom{12}{5}\binom{7}{4} + \binom{12}{4}\binom{8}{6} + \binom{12}{3}\binom{9}{8} + \binom{12}{2}\binom{10}{10}$$

ways to distribute the sweets.

(3) $\binom{19+5-1}{19} = \binom{23}{19} = \frac{23!}{19!4!} = 8855$

(4) $\binom{17-1}{17-4} = \binom{16}{13} = \frac{16!}{13!3!} = 560$

(5) The number of non-negative integer solutions is given by $C(21 + 4 - 1, 21)$. The second problem is equivalent to calculating the number of ways in which 21 identical objects can be placed into 4 different boxes so that box i has at least i objects. Place 1 object in box 1, 2 objects in box 2, 3 objects in box 3 and 4 objects in box 4. This can be done in one way since the objects are identical. Then distribute the remaining 11 objects into the 4 boxes in $C(11 + 4 - 1, 11) = 364$ ways. Hence, the equation has 364 solutions.

(6) There are $\binom{36+4-1}{36} = \binom{39}{36} = \frac{39!}{36!3!} = 9139$ ways to compose the choir. To compose the choir so that at least 6 members of each group is chosen, begin by selecting 6 singers from each group. There is one way to do this. Now, we still have to pick 12 members out of 4 types of singers. This can be done in $\binom{12+4-1}{12} = \binom{15}{12} = \frac{15!}{12!3!} = 455$ ways.

(7) $C(10 + 3 - 1, 10) = 66$

(8) There are $C(6+3-1,6)=28$ selections of 6 balls. The number of ways to select 10 balls is the same as the number of ways to select 8 balls. Hence, the problem becomes to find the number of selections of 8 balls from 3 types so that we do not select more than 6 of any type. Then the number of selections having exactly 7 objects of one type is 3×2, while the number of selections having exactly 8 objects of one type is 3. Hence, there are $C(8+3-1,8)-(3\times 2+3)=36$ selections.

(9) Consider the following cases: (i) choose 2 ties to wear on 3 days each, (ii) wear each of the ties on 2 days and (iii) wear 1 of the ties on 3 days, another tie on 2 days and the last tie on 1 day. Then this can be done in

$$\binom{3}{1}\binom{6}{3}\binom{2}{1}\binom{3}{3}+\binom{3}{1}\binom{6}{2}\binom{2}{1}\binom{4}{2}\binom{2}{2}+\binom{3}{1}\binom{6}{3}\binom{2}{1}\binom{3}{2}=1020$$

ways.

(10) $\binom{16}{6}\left[\binom{6}{1}P(10;5,1,1,1,1,1)+\binom{6}{1}\binom{5}{1}P(10;4,2,1,1,1,1)\right.$
$\left.+\binom{6}{2}P(10;3,3,1,1,1,1)+\binom{6}{1}\binom{5}{2}P(10;3,2,2,1,1,1)+\binom{6}{4}P(10;2,2,2,2,1,1)\right]$

(11) Consider the following cases: (i) choose 3 of one kind of letter and 1 of another letter, (ii) choose 2 of one kind and 2 of another and (iii) choose 2 of one letter and 1 each of two other kinds. Then there are

$$4P(4;3,1)+3P(4;2,2)+3P(4;2,1,1)=70$$

arrangements.

(13) We have to find the number of selections of $3n$ balls from 3 types so that we do not select more than $2n$ of any type. The number of selections having at least $2n+1$ balls of one type is $3\times C((n-1)+3-1,n-1)$. Hence, the number of ways to select $3n$ balls without selecting more than $2n$ of each type is $C(3n+3-1,3n)-3\times C((n-1)+3-1,n-1)$.

6.7. Recurrence relations and their solution

(1) Let a_n be the number of ways to distribute n distinct objects into 4 boxes. Now, to distribute n objects, we first distribute the first $n-1$ of these in a_{n-1} ways, followed by distributing the last object in 4 possible ways. Hence,

$$a_1=4 \text{ and}$$
$$a_n=4a_{n-1} \text{ for } n>1.$$

(2a) Denote the number of ways to count out the coins by a_n. Then $a_n=a_{n-1}+a_{n-2}$. The characteristic equation of this recurrence relation is $x^2-x-1=0$, which has roots $\frac{1}{2}+\frac{\sqrt{5}}{2}$ and $\frac{1}{2}-\frac{\sqrt{5}}{2}$. Hence, the general solution has the form

$$a_n=k_1\left(\frac{1}{2}+\frac{\sqrt{5}}{2}\right)^n+k_2\left(\frac{1}{2}-\frac{\sqrt{5}}{2}\right)^n.$$

Using the initial conditions $a_1=1$ and $a_2=2$, we obtain the following system of equations:

$$\frac{1}{2}k_1+\frac{\sqrt{5}}{2}k_1+\frac{1}{2}k_2-\frac{\sqrt{5}}{2}k_2=1 \text{ and}$$
$$\frac{3}{2}k_1+\frac{\sqrt{5}}{2}k_1+\frac{3}{2}k_2-\frac{\sqrt{5}}{2}k_2=2.$$

Solving this system, we get $k_1 = \frac{1}{2} + \frac{\sqrt{5}}{10}$ and $k_2 = \frac{1}{2} - \frac{\sqrt{5}}{10}$. Thus,

$$a_n = \left(\frac{1}{2} + \frac{\sqrt{5}}{10}\right)\left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right)^n + \left(\frac{1}{2} - \frac{\sqrt{5}}{10}\right)\left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^n.$$

(2b) Denote the number of ways to count out the coins by a_n. Then $a_n = a_{n-1} + a_{n-2} + a_{n-5}$. The initial conditions are $a_0 = 1$, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and $a_4 = 5$.

(3) The characteristic equation of the Lucas recurrence relation is $x^2 - x - 1 = 0$, which has roots $\frac{1}{2} + \frac{\sqrt{5}}{2}$ and $\frac{1}{2} - \frac{\sqrt{5}}{2}$. Hence, the general solution has the form

$$L_n = k_1\left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right)^n + k_2\left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^n.$$

Using the initial conditions $L_1 = 2$ and $L_2 = 1$, we obtain the following system of equations:

$$\frac{1}{2}k_1 + \frac{\sqrt{5}}{2}k_1 + \frac{1}{2}k_2 - \frac{\sqrt{5}}{2}k_2 = 2 \text{ and}$$
$$\frac{3}{2}k_1 + \frac{\sqrt{5}}{2}k_1 + \frac{3}{2}k_2 - \frac{\sqrt{5}}{2}k_2 = 1.$$

Solving this system, we get $k_1 = -\frac{1}{2} + \frac{5\sqrt{5}}{10}$ and $k_2 = -\frac{1}{2} - \frac{5\sqrt{5}}{10}$. Thus,

$$L_n = \left(-\frac{1}{2} + \frac{5\sqrt{5}}{10}\right)\left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right)^n + \left(-\frac{1}{2} - \frac{5\sqrt{5}}{10}\right)\left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^n.$$

(4) Denote the number of ways to make an n centimetre long row of electronic components on a circuit board by a_n. Then $a_n = 2a_{n-1} + a_{n-2}$. The characteristic equation of this recurrence relation is $x^2 - 2x - 1 = 0$, which has roots $1 + \sqrt{2}$ and $1 - \sqrt{2}$. Hence, the general solution has the form

$$a_n = k_1(1 + \sqrt{2})^n + k_2(1 - \sqrt{2})^n.$$

Using the initial conditions $a_1 = 2$ and $a_2 = 3$, we obtain the following system of equations:

$$k_1 + \sqrt{2}k_1 + k_2 - \sqrt{2}k_2 = 2 \text{ and}$$
$$3k_1 + 2\sqrt{2}k_1 + 3k_2 - 2\sqrt{2}k_2 = 3.$$

Solving this system, we get $k_1 = -\frac{1}{2} + \frac{3\sqrt{2}}{4}$ and $k_2 = -\frac{1}{2} - \frac{3\sqrt{2}}{4}$. Thus,

$$a_n = \left(-\frac{1}{2} + \frac{3\sqrt{2}}{4}\right)(1 + \sqrt{2})^n + \left(-\frac{1}{2} - \frac{3\sqrt{2}}{4}\right)(1 - \sqrt{2})^n.$$

(5a) Let a_n denote the number of n digit ternary sequences with no consecutive digits being the same. Then

$$a_1 = 3 \text{ and}$$
$$a_n = 2a_{n-1} \text{ for } n > 1.$$

The characteristic equation of this recurrence relation is $x - 2 = 0$, which has one root 2. Hence, the general solution has the form

$$a_n = k_1 2^n.$$

Solving this equation gives $k_1 = \frac{3}{2}$. Thus, $a_n = 3 \cdot 2^{n-1}$.

(5b) Let a_n be the number of all ternary sequences of length n with no 1 appearing directly to the left of any 2, let b_n be the number of ternary sequences of length n with no 1 appearing directly to the left of any 2 ending in a 0 or a 2, and let c_n be the number of sequences of length n with no 1 appearing directly to the left of any 2 ending in a 1. Clearly, $a_1 = 3$ and $a_2 = 3^2 - 1 = 8$. Now, $c_n = a_{n-1}$ because if a sequence of length n ends in a 1, there are a_{n-1} ways to generate the first $n-1$ terms of the sequence. Hence, since $a_n = b_n + c_n$, $b_n = a_n - c_n = a_n - a_{n-1}$. Now, consider a sequence of length $n+1$ with no 1 appearing directly to the left of any 2. If the last term of this sequence is a 2, then there are b_n ways to generate the first n terms of the sequence, while if the last term is a 0 or a 1, then in each case there are a_n ways to generate the first n terms of the sequence. Thus, $a_{n+1} = b_n + 2a_n = 3a_n - a_{n-1}$, so the problem can be described by the recurrence relation

$$a_1 = 3,$$
$$a_2 = 8 \text{ and}$$
$$a_n = 3a_{n-1} - a_{n-2} \text{ for } n > 2.$$

The recurrence relation has the characteristic equation $x^2 - 3x + 1 = 0$, which admits the roots $\frac{3-\sqrt{5}}{2}$ and $\frac{3+\sqrt{5}}{2}$. Hence, the general solution has the form

$$a_n = k_1\left(\frac{3-\sqrt{5}}{2}\right)^n + k_2\left(\frac{3+\sqrt{5}}{2}\right)^n.$$

Using the initial conditions $a_1 = 3$ and $a_2 = 8$, we obtain the following system of equations:

$$k_1\left(\frac{3-\sqrt{5}}{2}\right) + k_2\left(\frac{3+\sqrt{5}}{2}\right) = 3 \text{ and}$$
$$k_1\left(\frac{7-3\sqrt{5}}{2}\right) + k_2\left(\frac{7+3\sqrt{5}}{2}\right) = 8.$$

Solving this system, we get $k_1 = \frac{5-3\sqrt{5}}{10}$ and $k_2 = \frac{5+3\sqrt{5}}{10}$. The general solution is therefore

$$a_n = \left(\frac{5-3\sqrt{5}}{10}\right)\left(\frac{3-\sqrt{5}}{2}\right)^n + \left(\frac{5+3\sqrt{5}}{10}\right)\left(\frac{3+\sqrt{5}}{2}\right)^n.$$

(6) The recurrence relation is given by $a_n = a_{n-1} + 3(a_{n-1} - a_{n-2}) = 4a_{n-1} - 3a_{n-2}$ for $n \geq 2$. The recurrence relation has the characteristic equation $x^2 - 4x + 3 = 0$, which permits the roots 3 and 1. Hence, the general solution has the form

$$a_n = k_1 + 3^n k_2.$$

Using the initial conditions $a_1 = 1000$ and $a_2 = 1200$, we obtain the following system of equations:

$$k_1 + 3k_2 = 1000 \text{ and}$$
$$k_1 + 9k_2 = 1200.$$

Solving this system, we get $k_1 = 900$ and $k_2 = \frac{100}{3}$. Thus,

$$a_n = 900 + 100 \cdot 3^{n-1}.$$

(7a) This recurrence relation has the characteristic equation $x^2 - 3x - 4 = 0$, which admits the roots 2 and -3. Hence, the general solution has the form

$$a_n = k_1(2)^n + k_2(-3)^n.$$

Using the initial conditions $a_0 = 1$ and $a_1 = -2$, we obtain the following system of equations:

$$k_1 + k_2 = 1 \text{ and}$$
$$2k_1 - 3k_2 = -2.$$

Solving this system, we get $k_1 = \frac{1}{5}$ and $k_2 = \frac{4}{5}$. Thus, the general solution is

$$a_n = \frac{1}{5}(2)^n + \frac{4}{5}(-3)^n.$$

(7b) The general solution is $a_n = 1$.

(7c) This recurrence relation has the characteristic equation $x^2 - 3x - 10 = 0$, which has roots -2 and 5. Hence, the general solution has the form

$$a_n = k_1(-2)^n + k_2(5)^n.$$

Using the initial conditions $a_1 = 0$ and $a_2 = 3$, we obtain the following system of equations:

$$-2k_1 + 5k_2 = 0 \text{ and}$$
$$4k_1 - 25k_2 = 3.$$

Solving this system, we get $k_1 = \frac{3}{14}$ and $k_2 = \frac{3}{35}$. Thus, the general solution is

$$a_n = \frac{3}{14}(-2)^n + \frac{3}{35}(5)^n.$$

(7d) The general solution is $a_n = \frac{14}{9}(3)^n - \frac{8}{9}n(3)^n$.

(7e) The recurrence relation has the characteristic equation $x^3 - 3x^2 + 3x - 1 = 0$, which has one root of multiplicity 3, namely 1. Hence, the general solution has the form

$$\begin{aligned} a_n &= k_1(1)^n + k_2 n(1)^n + k_3 n^2(1)^n \\ &= k_1 + k_2 n + k_3 n^2. \end{aligned}$$

Using the initial conditions $a_0 = a_1 = 1$ and $a_2 = 2$, we obtain the following system of equations:

$$k_1 = 1,$$
$$k_1 + k_2 + k_3 = 1 \text{ and}$$
$$k_1 + 2k_2 + 4k_3 = 2.$$

Solving this, we get $k_1 = 1$, $k_2 = -\frac{1}{2}$ and $k_3 = \frac{1}{2}$. Thus, the general solution is

$$a_n = 1 - \frac{1}{2}n + \frac{1}{2}n^2.$$

(7f) The general solution is $a_n = -4n3^{n-1} + 5^n$.

(8a) The recurrence relation has the characteristic equation $x^2 - \sqrt{2}x - 1 = 0$, which has roots $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ and $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$. Rewriting this in polar form, we get $\rho = \sqrt{\frac{2}{4} + \frac{2}{4}} = 1$, while $\cos\theta = \frac{\sqrt{2}}{2}$ and $\sin\theta = \frac{\sqrt{2}}{2}$, which gives $\theta = \frac{\pi}{4}$. Hence, the general solution has the form

$$a_n = k_1 \cos\left(\frac{\pi}{4}n\right) + k_2 \sin\left(\frac{\pi}{4}n\right).$$

Using the initial conditions $a_0 = -1$ and $a_1 = 1$, we obtain the following system of equations:

$$k_1 = -1 \text{ and}$$
$$\frac{\sqrt{2}}{2}k_1 + \frac{\sqrt{2}}{2}k_2 = 1.$$

Solving this system, we get $k_1 = -1$ and $k_2 = \sqrt{2} + 1$. The general solution is therefore

$$a_n = -\cos\left(\frac{\pi}{4}n\right) + (\sqrt{2} + 1)\sin\left(\frac{\pi}{4}n\right).$$

(8b) The general solution is $a_n = 2^n\left(3\cos\left(\frac{\pi}{2}n\right) + 2\sin\left(\frac{\pi}{2}n\right)\right)$.

(8d) The recurrence relation has the characteristic equation $x^2 - x + 1 = 0$, which has roots $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Rewriting this in polar form, we get $\rho = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$, while $\cos\theta = \frac{1}{2}$ and $\sin\theta = \frac{\sqrt{3}}{2}$, which gives $\theta = \frac{\pi}{3}$. Hence, the general solution has the form

$$a_n = k_1\cos\left(\frac{\pi}{3}n\right) + k_2\sin\left(\frac{\pi}{3}n\right).$$

Using the initial conditions $a_0 = 1$ and $a_1 = 2$, we obtain the following system of equations:

$$k_1 = 1 \text{ and}$$
$$\frac{1}{2}k_1 + \frac{\sqrt{3}}{2}k_2 = 2.$$

Solving this system, we get $k_1 = 1$ and $k_2 = \sqrt{3}$. The general solution is therefore

$$a_n = \cos\left(\frac{\pi}{3}n\right) + \sqrt{3}\sin\left(\frac{\pi}{3}n\right).$$

(8e) The general solution is $a_n = 4^{n+1}\cos\left(\frac{\pi}{2}n\right) + 3\cdot 4^{n-1}\sin\left(\frac{\pi}{2}n\right)$.

(8f) The recurrence relation has the characteristic equation $x^2 + 2\sqrt{2}x + 4 = 0$, which has roots $-\sqrt{2} + \sqrt{2}i$ and $-\sqrt{2} - \sqrt{2}i$. Rewriting this in polar form, we get $\rho = \sqrt{2+2} = 2$, while $\cos\theta = -\frac{\sqrt{2}}{2}$ and $\sin\theta = \frac{\sqrt{2}}{2}$, which gives $\theta = \frac{3\pi}{4}$. Hence, the general solution has the form

$$a_n = 2^n\left(k_1\cos\left(\frac{3\pi}{4}n\right) + k_2\sin\left(\frac{3\pi}{4}n\right)\right).$$

Using the initial conditions $a_0 = 1$ and $a_1 = 0$, we obtain the following system of equations:

$$k_1 = 1 \text{ and}$$
$$-\sqrt{2}k_1 + \sqrt{2}k_2 = 0.$$

Solving this system, we get $k_1 = 1$ and $k_2 = 1$. The general solution is therefore

$$a_n = 2^n\left(\cos\left(\frac{3\pi}{4}n\right) + \sin\left(\frac{3\pi}{4}n\right)\right).$$

6.8. Generating functions

(1) We have

$$\begin{aligned}(1 + x + x^2 + \cdots)^5 &= \frac{1}{(1-x)^5}\\ &= 1 + \binom{1+5-1}{1}x + \cdots + \binom{r+5-1}{r}x^r + \cdots,\end{aligned}$$

so the coefficient of x^9 is

$$\binom{9+5-1}{9} = \binom{13}{9} = 715.$$

(2) We have

$$(1+x)^m(1 + x^2 + x^4 + x^6) = \left(\sum_{r=0}^{m}\binom{m}{r}x^r\right)(1 + x^2 + x^4 + x^6),$$

so the coefficient of x^7 is

$$\binom{m}{7} + \binom{m}{5} + \binom{m}{3} + \binom{m}{1}$$

(3) We have

$$(1+x^2)^m = \left(\sum_{r=0}^{m} \binom{m}{r} (x^2)^r\right),$$

so the coefficient of x^{12} is $\binom{m}{6}$.

(4) We have

$$(x^3+x^4+x^5+\cdots)^6 = x^{18}(1+x+x^2+\cdots)^6 = \frac{x^{18}}{(1-x)^6},$$

so the coefficient of x^k in $(x^3+x^4+x^5+\cdots)^6$ is the same as the coefficient of x^{k-18} in $\frac{1}{(1-x)^6}$, which is

$$\binom{(k-18)+6-1}{k-18} = \binom{k-13}{k-18}.$$

(5) We have

$$(x+x^3+x^5)(1+x)^n = (x+x^3+x^5)\sum_{r=0}^{n} \binom{n}{r} x^r,$$

so the coefficient of x^k is

$$\binom{n}{k-1} + \binom{n}{k-3} + \binom{n}{k-5}.$$

(6) We have

$$\begin{aligned}
&(1+x+x^2+x^3+\cdots)^4 \frac{1-x^7}{1-x} \\
&= \frac{1}{(1-x)^4}(1+x+x^2+x^3+x^4+x^5+x^6) \\
&= \left(\sum_{r=0} \binom{r+4-1}{r} x^r\right)(1+x+x^2+x^3+x^4+x^5+x^6),
\end{aligned}$$

so the coefficient of x^k is

$$\begin{aligned}
&\binom{k+4-1}{k} + \binom{k-1+4-1}{k-1} + \binom{k-2+4-1}{k-2} + \cdots + \binom{k-6+4-1}{k-6} \\
&= \binom{k+3}{k} + \binom{k+2}{k-1} + \binom{k+1}{k-2} + \cdots + \binom{k-3}{k-6}.
\end{aligned}$$

(7) First, there is 1 way to select 0 of each colour pen, 1 way to select 1 of each colour pen, 1 way to select 2 of each colour pen and 1 way to select 3 of each colour pen, so the generating function for the number of ways to select blue pens is $1+x+x^2+x^3$. Similiarly, the generating function for the number of ways to select black pens is $1+x+x^2+x^3$, and the same for the other two colours. The generation function for the number of composite outcomes is therefore

$$\begin{aligned}
A(x) &= (1+x+x^2+x^3)^4 \\
&= \left(\frac{1-x^4}{1-x}\right)^4 \\
&= (1-x^4)^4 \frac{1}{(1-x)^4} \\
&= (1-4x^4+6x^8-4x^{12}+x^{16})\frac{1}{(1-x)^4}.
\end{aligned}$$

Hence, the number of selections of 5 pens is simply the coefficient of x^5 in $A(x)$, which is

$$\binom{5+4-1}{5} + (-4)\binom{1+4-1}{1} = 40.$$

(8a) The generating function for the number of ways to select cricket balls is $1 + x + x^2 + x^3$. Similiarly, the generating function for the number of ways to select rugby balls is $1 + x + x^2 + x^3 + x^4$ and, finally, the generating function for the number of ways to select tennis balls is also $1 + x + x^2 + x^3 + x^4$. The generation function for the number of composite outcomes is therefore

$$\begin{aligned} A(x) &= (1 + x + x^2 + x^3)(1 + x + x^2 + x^3 + x^4)^2 \\ &= \frac{1 - x^4}{1 - x}\left(\frac{1 - x^5}{1 - x}\right)^2 \\ &= (1 - x^4)(1 - x^5)^2 \frac{1}{(1 - x)^3} \\ &= (1 - x^4 - 2x^5 + 2x^9 + x^{10} - x^{14})\frac{1}{(1 - x)^3}. \end{aligned}$$

Hence, the number of selections of 5 balls is simply the coefficient of x^5, which is

$$\binom{5 + 3 - 1}{5} + (-1)\binom{1 + 3 - 1}{1} + (-2)(1) = 16.$$

(8b) The generating function is

$$\begin{aligned} A(x) &= (x + x^2 + x^3)(x + x^2 + x^3 + x^4 + x^5)(x + x^2 + \cdots + x^8) \\ &= x^3(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2 + x^3 + \cdots + x^7) \\ &= x^3\left(\frac{1 - x^3}{1 - x}\right)\left(\frac{1 - x^5}{1 - x}\right)\left(\frac{1 - x^8}{1 - x}\right) \\ &= x^3(1 - x^3 - x^5 + x^{11} + x^{13} - x^{16})\frac{1}{(1 - x)^3}. \end{aligned}$$

The number of selections of 4 glasses is simply the coefficient of x^4, which is

$$\binom{1 + 3 - 1}{1} = 3.$$

(8c) The generating function for the number of ways to select a transistor of the first type is $x + x^3 + \cdots$, with the same for the seventh type. The generating function for the number of ways to select a transistor of the second type is $1 + x + x^2 + x^3 + \cdots$, with the same for the remaining types of transistors. The generation function for the number of composite outcomes is therefore

$$\begin{aligned} A(x) &= (x + x^3 + x^5 + \cdots)^2(1 + x + x^2 + \cdots)^5 \\ &= x^2(1 + x^2 + x^4 + \cdots)^2(1 + x + x^2 + \cdots)^5 \\ &= x^2\frac{1}{(1 - x^2)^2}\frac{1}{(1 - x)^5}. \end{aligned}$$

Hence, the number of selections of 10 transistors is simply the coefficient of x^{10} in $A(x)$, which is the coefficient of x^8 in $\frac{1}{(1-x^2)^2}\frac{1}{(1-x)^5}$. This means there are

$$\begin{aligned} &\binom{12}{8} + \binom{2}{1}\binom{10}{6} + \binom{3}{2}\binom{8}{4} + \binom{4}{3}\binom{6}{2} + \binom{5}{4} \\ &= 495 + (2)(210) + (3)(70) + (4)(15) + (5)(1) \\ &= 1190 \end{aligned}$$

selections of 10 transistors.

(9a) The number of ways to distribute r balls into 10 boxes with at least 1 ball in each box is the coefficient of x^r in $A(x) = (x + x^2 + x^3 + \cdots)^{10}$.

(9b) The number of ways to distribute r balls into 5 boxes with at most 4 balls in each box is the coefficient of x^r in $A(x) = (1 + x + x^2 + x^3 + x^4)^5$.

(9c) The number of ways to distribute r identical balls into 4 boxes with between 2 and 7 balls in each box is simply the coefficient of x^r in $A(x) = (x^2 + x^3 + x^4 + x^5 + x^6 + x^7)^4$.

(9d) The number of ways to distribute r identical balls into 4 boxes with fewer than 6 balls in each box is simply the coefficient of x^r in $A(x) = (1 + x + x^2 + x^3 + x^4 + x^5)^4$.

(10a) The generating function for the number of possible election outcomes is

$$A(x) = (1 + x + x^2 + x^3 + \cdots)^4 = \left(\frac{1}{1-x}\right)^4 = \frac{1}{(1-x)^4}$$

The number of election outcomes is simply the coefficient of x^{30}, which is

$$\binom{4+30-1}{30} = \binom{33}{30} = \frac{33!}{30!3!} = 5456.$$

(10b) Note that if each nominated member votes for himself, they each receive at least one vote, so the generating function for the number of possible election outcomes is

$$\begin{aligned} A(x) &= (x + x^2 + x^3 + x^4 + \cdots)^4 \\ &= x^4(1 + x + x^2 + x^3 + \cdots)^4 \\ &= x^4 \frac{1}{(1-x)^4}. \end{aligned}$$

Hence, the number of election outcomes is simply the coefficient of x^{30}, which is

$$\binom{26+4-1}{26} = \binom{29}{26} = \frac{29!}{23!3!} = 3654.$$

(10c) This problem is equivalent to adding a fifth candidate, called "abstain", to the four being voted for. The generating function for the number of possible election outcomes is

$$A(x) = (1 + x + x^2 + x^3 + x^4 + \cdots)^5 = \frac{1}{(1-x)^5}$$

Hence, the number of election outcomes is simply the coefficient of x^{30}, which is

$$\binom{30+5-1}{50} = 142\,506.$$

(11) The number of ways to buy n pieces of fruit is simply the coefficient of x^n in the generating function

$$A(x) = (1 + x^2 + x^4 + \cdots)(1 + x^6 + x^{12} + \cdots)(1 + x + x^2 + \cdots).$$

(12a) The problem is equivalent to calculating the number of non-negative integer solutions to the equation $z_1 + z_2 + z_3 + z_4 + z_5 = n$. The number of non-negative solutions to this equation is simply the coefficient of x^n in the generating function

$$A(x) = (1 + x + x^2 + \cdots)^5.$$

(12b) In this case, $z_1 > 0$, so the number of 5-digit positive integers, the digits sum of which is n, is simply the coefficient of x^n in the generating function

$$A(x) = (x + x^2 + \cdots)(1 + x + x^2 + \cdots)^4.$$

(13a) The number of non-negative solutions to this equation is simply the coefficient of x^n in the generating function

$$A(x) = (1 + x + x^2 + \cdots)^3.$$

(13b) The number of non-negative solutions to this equation is simply the coefficient of x^n in the generating function

$$A(x) = (1 + x + x^2 + \cdots)^2(1 + x^2 + x^4 + \cdots).$$

(14) The number of non-negative solutions to this equation is simply the coefficient of x^n in the generating function

$$A(x) = (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots).$$

6.9. Recurrence relations and generating functions

(1) Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ be the generating function for (a_k). Then

$$xf(x) = a_0 x + a_1 x^2 + a_2 x^3 + \cdots,$$
$$\frac{3}{1-x} = 3 + 3x + 3x^2 + \cdots.$$

So

$$\begin{aligned} f(x) - xf(x) - \frac{3}{1-x} &= (a_0 - 3) + (a_1 - a_0 - 3)x + (a_2 - a_1 - 3)x^2 + \cdots \\ &= a_0 - 3 \\ &= 2. \end{aligned}$$

Hence,

$$f(x)(1-x) = 2 + \frac{3}{1-x},$$
$$f(x) = \frac{2}{1-x} + \frac{3}{(1-x)^2}.$$

Decompose the second term using partial fractions:

$$\frac{3}{(1-x)^2} = \frac{A}{1-x} + \frac{B}{(1-x)^2},$$

which gives

$$3 = A(1-x)^2 + B,$$
$$3 = A - Ax + B,$$
$$3 = -Ax + (A + B).$$

Hence,

$$-A = 0 \text{ and}$$
$$A + B = 3,$$

so $A = 0$ and $B = 3$. We thus have

$$\begin{aligned} f(x) &= \frac{2}{1-x} + \frac{3}{(1-x)^2} \\ &= 2\sum_{k=0}^{\infty} x^k + 3\sum_{k=0}^{\infty} \binom{k+1}{k} x^k \\ &= \sum_{k=0}^{\infty} (3k+5)x^k, \end{aligned}$$

and so $a_k = 3k + 5$.

(2) Answer: $a_k = \frac{1}{5}(6 \cdot 3^k - (-2)^k)$.

(3) Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ be the generating function for (a_k). Then

$$2xf(x) = 2a_0x + 2a_1x^2 + 2a_2x^3 + \cdots,$$
$$\frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + \cdots.$$

Therefore

$$\begin{aligned} f(x) - 2xf(x) - \frac{x}{(1-x)^2} &= a_0 + (a_1 - 2a_0 - 1)x + (a_2 - 2a_1 - 2)x^2 + \cdots \\ &= 3 + 0x + 0x^2 + \cdots \\ &= 3. \end{aligned}$$

Hence,

$$f(x)(1-2x) = 3 + \frac{x}{(1-x)^2},$$
$$f(x) = \frac{3}{1-2x} + \frac{x}{(1-x)^2}.$$

Decompose the second term using partial fractions:

$$\frac{x}{(1-x)^2(1-2x)} = \frac{A}{1-2x} + \frac{B}{1-x} + \frac{C}{(1-x)^2},$$

which gives

$$\begin{aligned} x &= A(1-x)^2 + B(1-2x)(1-x) + C(1-2x), \\ x &= A - 2Ax + Ax^2 + B - 3Bx + 2Bx^2 + C - 2Cx, \\ x &= (A + 2B)x^2 + (-2A - 3B - 2C)x + (A + B + C). \end{aligned}$$

Hence,

$$\begin{gathered} A + 2B = 0, \\ -2A - 3B - 2C = 1 \text{ and} \\ A + B + C = 0, \end{gathered}$$

so $A = 2$, $B = -1$ and $C = -1$. We thus have

$$\begin{aligned} f(x) &= \frac{3}{1-2x} + \frac{2}{1-2x} - \frac{1}{1-x} - \frac{1}{(1-x)^2} \\ &= \frac{5}{1-2x} - \frac{1}{1-x} - \frac{1}{(1-x)^2} \\ &= 5\sum_{k=0}^{\infty} 2^k x^k - \sum_{k=0}^{\infty} x^k - \sum_{k=0}^{\infty} \binom{k+1}{k} x^k, \end{aligned}$$

and so $a_k = 5 \cdot 2^k - 1 - (k+1) = 5 \cdot 2^k - k - 2$.

(4) Answer: $a_k = -2^{k+1} + 3^{k+1}$.

(5) Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ be the generating function for (a_n). Then

$$xf(x) = a_0x + a_1x^2 + a_2x^3 + \cdots,$$
$$\frac{x}{1-3x} = x + 3x^2 + 3^2x^3 + \cdots.$$

Threfore we get

$$\begin{aligned} f(x) - xf(x) - \frac{x}{1-3x} &= a_0 + (a_1 - a_0 - 1)x + (a_2 - a_1 - 3)x^2 + \cdots \\ &= 0 + 0x + 0x^2 + \cdots \\ &= 0. \end{aligned}$$

Hence,

$$f(x) = \frac{x}{(1-3x)(1-x)}.$$

Decompose $f(x)$ using partial fractions:

$$\frac{x}{(1-3x)(1-x)} = \frac{A}{1-3x} + \frac{B}{1-x},$$

which gives

$$\begin{aligned} x &= A(1-x) + B(1-3x), \\ x &= A - Ax + B - 3Bx, \\ x &= (-A-3B)x + (A+B). \end{aligned}$$

Hence,

$$\begin{aligned} -A - 3B &= 1 \text{ and} \\ A + B &= 0, \end{aligned}$$

so $A = \frac{1}{2}$ and $B = -\frac{1}{2}$. We thus have

$$\begin{aligned} f(x) &= \frac{1}{2}\left(\frac{1}{1-3x}\right) - \frac{1}{2}\left(\frac{1}{1-x}\right) \\ &= \frac{1}{2}\sum_{n=0}^{\infty} 3^n x^n - \frac{1}{2}\sum_{n=0}^{\infty} x^n, \end{aligned}$$

and so $a_n = \frac{3^n-1}{2}$.

(6) Answer: $a_n = \frac{3^n+5^n}{2}$.

(7) Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ be the generating function for (a_n). Then

$$\begin{aligned} 4xf(x) &= 4a_0 x + 4a_1 x^2 + 4a_2 x^3 + \cdots, \\ \frac{2x}{(1-x)^2} &= 2x + 4x^2 + 6x^3 + \cdots. \end{aligned}$$

Therefore we get

$$\begin{aligned} f(x) - 4xf(x) - \frac{2x}{(1-x)^2} &= a_0 + (a_1 - 4a_0 - 2)x + (a_2 - 4a_1 - 4)x^2 + \cdots \\ &= 3 + 0x + 0x^2 + \cdots \\ &= 3. \end{aligned}$$

Hence,

$$f(x) = \frac{3}{1-4x} + \frac{2x}{(1-4x)(1-x)^2}.$$

Decompose the second term using partial fractions:

$$\frac{2x}{(1-4x)(1-x)^2} = \frac{A}{1-4x} + \frac{B}{1-x} + \frac{C}{(1-x)^2},$$

which gives

$$\begin{aligned} 2x &= A(1-x)^2 + B(1-x)(1-4x) + C(1-4x), \\ 2x &= A - 2Ax + Ax^2 + B - 5Bx + 4Bx^2 + C - 4Cx, \\ 2x &= (A+4B)x^2 + (-2A-5B-4C)x + (A+B+C). \end{aligned}$$

Hence,

$$\begin{aligned} A + 4B &= 0, \\ -2A - 5B - 4C &= 2 \text{ and} \\ A + B + C &= 0, \end{aligned}$$

so $A = \frac{8}{9}$, $B = -\frac{2}{9}$ and $C = -\frac{6}{9}$. We thus have

$$\begin{aligned} f(x) &= \frac{3}{1-4x} + \frac{8}{9}\left(\frac{1}{1-4x}\right) - \frac{2}{9}\left(\frac{1}{1-x}\right) - \frac{6}{9}\left(\frac{1}{(1-x)^2}\right) \\ &= \frac{35}{9}\left(\frac{1}{1-4x}\right) - \frac{2}{9}\left(\frac{1}{1-x}\right) - \frac{6}{9}\left(\frac{1}{(1-x)^2}\right) \\ &= \frac{35}{9}\sum_{n=0}^{\infty} 4^n x^n - \frac{2}{9}\sum_{n=0}^{\infty} x^n - \frac{6}{9}\sum_{n=0}^{\infty}\binom{n+1}{n} x^n, \end{aligned}$$

and so $a_n = \frac{35\cdot 4^n - 6n - 8}{9}$.

(8) Answer: $a_n = \frac{1}{3}(5^n + 2^{n+1})$.

(9) Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ be the generating function for (a_n). Then

$$\begin{aligned} 2xf(x) &= 2a_0 x + 2a_1 x^2 + 2a_2 x^3 + \cdots, \\ x^2 f(x) &= a_0 x^2 + a_1 x^3 + a_2 x^4 + \cdots, \\ \frac{x^2}{1-2x} &= x^2 + 2x^3 + 4x^4 + 8x^5 \cdots. \end{aligned}$$

Therefore,

$$\begin{aligned} f(x) - 2xf(x) + x^2 f(x) - \frac{x^2}{1-2x} &= a_0 + (a_1 - 2a_0)x + (a_2 - 2a_1 + a_0 - 1)x^2 + \cdots \\ &= 1 + (2-2)x \\ &= 1. \end{aligned}$$

Hence,

$$\begin{aligned} f(x)(1 - 2x + x^2) &= 1 + \frac{x^2}{1-2x}, \\ f(x) &= \frac{1}{1-2x+x^2} + \frac{x^2}{(1-2x)(1-2x+x^2)}, \\ f(x) &= \frac{1-2x+x^2}{(1-2x)(1-2x+x^2)}, \\ f(x) &= \frac{1}{1-2x}, \\ f(x) &= \sum_{n=0}^{\infty} 2^n x^n, \end{aligned}$$

so $a_n = 2^n$.

(10) Answer: $a_k = 4 \cdot 2^k + (k-1)\cdot 3^{k+1}$.

6.10. Application: classical discrete probability

(1a) $\binom{49}{6} = \frac{49!}{43!\ 6!} = 13\ 983\ 816$.

(1b) Let n be the number of lottery tickets. Then

$$\frac{n}{13\ 983\ 816} \geq \frac{1}{1000\ 000}$$
$$n \geq 13.983\ 816.$$

Hence, we have to buy at least 14 tickets.

(1c)
$$\binom{6}{6} + \binom{6}{5}\binom{43}{1} + \binom{6}{4}\binom{43}{2} + \binom{6}{3}\binom{43}{3} = 260\ 624.$$

(1d) Let n be the number of lottery tickets. Then

$$\frac{n}{260\ 624} \geq \frac{1}{1\ 000\ 000}$$
$$n \geq 0.260\ 624.$$

Hence, 1 ticket is enough.

(1e) There are 43 numbers to choose from. Hence, there are $\binom{43}{6} = \frac{43!}{37!\ 6!} = 6\ 096\ 454$ combinations in which no number matches any of the numbers in the draw.

(2a) $E \cap F$ is the event "the patient is deficient in at least two vitamins and has no deficiencies". This is empty, which means that E and F are mutually exclusive events.

(2b) $E \cup F$ is the event "the patient is deficient in at least two vitamins or has no deficiencies".

(2c) $\overline{E} \cap \overline{F}$ is the event "the patient has no deficiencies and is deficient in at least two vitamins", which is again empty.

(3) We must first count the number of integers between 1 and 9999 that have exactly one 4 and one 5 among their digits. Choose a position for the 4 and one for the 5: $P(4, 2)$ ways. Fill the two remaining positions: 8×8 ways. Thus there are $P(4, 2) \times 8^2 = 768$ such integers. Hence, the probability that an integer between 1 and 10 000 has exactly one 4 and one 5 among its digits is $\frac{768}{10\ 000} = 0.0768$.
The sample space is the set of all integers between 1 and 10 000.

(4) The total number of sample points is 2^n, while the number of sequences in which there are no pairs of consecutive digits that are the same is only 2. Hence, the probability that in a random n-digit binary sequence there are no pairs of consecutive digits that are the same is $\frac{2}{2^n} = 2^{1-n}$.

(5a) Here the sample space is the set of all possible five-card hands, which has $C(52, 5) = \frac{52!}{47!5!} = 2\ 598\ 960$ sample points. Now, there are 4 Royal Flushes, so the probability that a five-card hand has a Royal Flush is $\frac{4}{2\ 598\ 960} = 0.00\ 000\ 154$

(5b) The number of five-card hands that are Flushes is

$$4 \times C(13, 5) = 4 \times \frac{13!}{5!8!} = 5148,$$

so the probability that a five-card hand has a Flush is $\frac{5148}{2\ 598\ 960} \approx 0.002$.

(5c) To calculate the number of five-card hands with four aces, put all 4 aces in the hand in 1 way and then choose one more card from the remaining 48 cards. Hence, there are $C(48, 1) = 48$ five-card hands with 4 aces, which means that the probability that a five-card hand has four aces is $\frac{48}{2\ 598\ 960} \approx 0.000\ 019$.

(5d) To calculate the number of five-card hands with four of a kind, first choose 4 of a kind to put in the hand. There are 13 ways to do this. Then choose one more card from the remaining 48 cards in 48 ways. Hence, there are $13 \times 48 = 624$ five-card hands with four of a kind, so the probability that a five-card hand has four of a kind is $\frac{624}{2\ 598\ 960} \approx 0.000\ 24$.

(5e) There are $10 \times 4^5 = 10\ 240$ possible Straights, so the probability that a five-card has a Straight is $\frac{10\ 240}{2\ 598\ 960} \approx 0.003\ 94$.

(5f) There are $10\,240 - 40 = 10\,200$ possible Straights that are not Flushes, so the probability that a five-card hand is a Straight that is not a Flush is $\frac{10\,200}{2\,598\,960} \approx 0.003\,93$.

(5g) To calculate the number of five-card hands that have the same number of hearts and diamonds, we consider the following cases:

Case 1: The hand has no hearts and no diamonds.

In this case, there are $C(26, 5) = \frac{26!}{5!21!} = 65\,780$ possible hands.

Case 2: The hand has one heart and one diamond.

Here there are $C(13, 1) \times C(13, 1) \times C(26, 3) = 439\,400$ possible hands.

Case 3: The hand contains two hearts and two diamonds.

In this case, there are $C(13, 2) \times C(13, 2) \times C(26, 1) = 158\,184$ possible hands.

Hence, in total there are $65\,780 + 439\,400 + 158\,184 = 663\,364$ possible five-card hands with the same number of hearts and diamonds, so the probability that a five-card hand has the same number of hearts and diamonds is $\frac{663\,364}{2\,598\,960} \approx 0.26$.

(5h) To calculate the number of five-card hands with more spades than hearts, consider the following cases:

Case 1: The hand contains no hearts and at least one spade.

In this case, there are $C(39, 5) - C(26, 5) = 575\,757 - 65\,780 = 509\,977$ possible hands.

Case 2: The hand contains one heart and at least two spades.

Here there are

$$\binom{13}{1}\binom{13}{2}\binom{26}{2} + \binom{13}{1}\binom{13}{3}\binom{26}{1} + \binom{13}{1}\binom{13}{4} = 435\,513$$

possible hands.

Case 3: The hand contains two hearts and three spades.

Then there are $C(13, 2) \times C(13, 3) = 22\,308$ possible hands.

Hence, in total, there are $509\,977 + 433\,513 + 22\,308 = 965\,798$ five-card hands with more spades than hearts, which means the probability of a five-card hand containing more spades than hearts is $\frac{965\,798}{2\,598\,960} \approx 0.37$.

(6) There are 365 possible birthdays (ignoring leap years), so there are 365^{30} ways to assign a birthday to each person. If no two have the same birthday, the first person can have any of the 365 birthdays, which means that the second person can have any of the remaining 364 birthdays, and so on. Hence, the probability of everybody having different birthdays is $\frac{P(365, 30)}{365^{30}}$. This means that the probability of two people in the group having the same birthday is $1 - \frac{P(365, 30)}{365^{30}} \approx 0.71$. In other words, it is more likely than not that in a group of 30 people there are two that have the same birthday.

(7a) First, the total number of arrangements is $\frac{8!}{2} = 20\,160$, so there are 20 160 sample points in the sample space. Now, think of the consonants as separators and arrange them first. There are $\frac{4!}{2} = 12$ arrangements of the consonants. We then have 5 possible spaces for the vowels. Choose 4 spaces for the 4 vowels in $C(5, 4) = 5$ ways and then arrange the vowels in the chosen spaces in $4! = 24$ ways. Hence, in total, there are $12 \times 5 \times 24 = 1440$ arrangements with no consecutive vowels. This means that the probability of an arrangement containing no consecutive vowels is $\frac{1440}{20\,160} = \frac{1}{14}$.

(7b) The event that an arrangement contains at least two consecutive vowels is the complement of the event that an arrangement contains no consecutive vowels, so the probability that an arrangement contains at least two consecutive vowels is $1 - \frac{1440}{20\ 160} = \frac{13}{14}$.

(7c) We first count the number of arrangements containing exactly 3 consecutive vowels and then the number of arrangements that contain 4 consecutive vowels. Again, think of the consonants as separators and arrange them in $\frac{4!}{2} = 12$ ways. We then have 5 possible spaces for the vowels and one of these spaces must contain 3 of the 4 vowels and another space the remaining vowel. Choose 3 vowels from the 4 vowels in $C(4, 3) = 4$ ways and then choose 2 spaces from the 5 spaces for the vowels in $C(5, 2) = 10$ ways. The three vowels can be arranged in $3! = 6$ ways, so the total number of arrangements of the vowels is $6 \times 2 = 12$ ways. Hence, the total number of arrangements containing three consecutive vowels is $12 \times 4 \times 10 \times 12 = 5760$. Similarly, the number of arrangements containing exactly four consecutive vowels is $12 \times C(5, 1) \times 4! = 1440$. Thus, the total number of arrangements containing at least three consecutive vowels is $1440 + 5760 = 7200$, which means the probability that an arrangement contains at least three consecutive vowels is $\frac{7200}{20\ 160} = \frac{5}{14}$.

(9a) Let U be the set of butterflies in the sample and let Sp, St and D be the set of butterflies that have spots, stripes and dots, respectively. Then $|U| = 50$, $|Sp| = 31$, $|St| = 20$, $|D| = 14$, $|Sp \cap St| = 16$, $|Sp \cap D| = 9$, $|St \cap St \cap D| = 5$ and $|\overline{Sp \cup St \cup D}| = 12$. Hence, the number of butterflies that have at least one of these features is

$$|Sp \cup St \cup D| = 50 - 12 = 38.$$

This means that the number of butterflies that have stripes and dots is

$$\begin{aligned}
&|St \cap D| \\
&= |St| + |Sp| + |D| - |Sp \cap St| - |Sp \cap D| + |St \cap St \cap D| - |Sp \cup St \cup D| \\
&= 20 + 31 + 14 - 16 - 9 + 5 - 38 \\
&= 7.
\end{aligned}$$

Thus, the probability that a butterfly has stripes and spots is $\frac{7}{50} = 0.14$.

(9b) The number of butterflies that have at least two of these features is

$$\begin{aligned}
&|(Sp \cap St) \cup (St \cap D) \cup (Sp \cap D)| \\
&= |Sp \cap St| + |St \cap D| + |Sp \cap D| - 2|St \cap St \cap D| \\
&= 16 + 7 + 9 - 10 \\
&= 22.
\end{aligned}$$

Hence, the probability that a butterfly has at least two of these features is $\frac{22}{50} = 0.44$.

(10a) The number of sample points in the sample space is 12^{12}. If no box must be empty, each box must contain exactly one object. There are 12! ways in which the objects can be distributed into the 12 boxes. Hence, the probability that no box is empty is $\frac{12!}{12^{12}}$.

(10b) In this case there will be one empty box and one box that contains two objects. Choose which box must be empty in $C(12, 1) = 12$ ways. Then choose which box must contain 2 objects in $C(11, 1) = 11$ ways. Next, choose two objects that must go into this box in $C(12, 2) = 66$ ways. Finally, distribute the remaining 10 objects to the remaining 10 boxes in 10! ways. Hence, in total there are $12 \times 11 \times 66 \times 10!$ distributions, which means that the probability that exactly one box is empty is $\frac{12 \times 11 \times 66 \times 10!}{12^{12}}$.

(10c) We subtract the number distributions in which no box is empty from the total number of distributions: $12^{12} - 12!$. Hence, the probability that at least one box is empty is $\frac{12^{12} - 12!}{12^{12}}$.

(10d) Choose which two boxes are empty in $C(12, 2) = 66$ ways. Then there are two cases:

Case 1: one box gets three objects.

Choose the box in $C(10, 1) = 10$ ways and then pick which three objects go into this box in $C(12, 3) = 220$ ways. Now distribute the remaining 9 objects into the remaining 9 boxes in 9! ways. Hence, in this case, there are $10 \times 66 \times 220 \times 9!$ distributions.

Case 2: two boxes get two objects each.

Choose these two boxes in $C(10, 2) = 45$ ways. Then choose two objects that go into the first of these two boxes and another two objects that go into the second of these two boxes in $C(12, 2) \times C(10, 2) = 2970$ ways. Finally, distribute the remaining 8 objects into the remaining 8 boxes in 8! ways. In this case, there are $66 \times 45 \times 2970 \times 8!$ distributions.

Hence, in total, there are $10 \times 66 \times 220 \times 9! + 66 \times 45 \times 2970 \times 8!$ distributions, which means the probability that there are two empty boxes is $\frac{10 \times 66 \times 220 \times 9! + 66 \times 45 \times 2970 \times 8!}{12^{12}}$.

(15a) Let E_i, $1 \leq i \leq 3$, be the event that the first archer hits the target with shot i and let F_j, $1 \leq j \leq 2$, be the event that the second archer hits the target with shot j. Then $P(E_1) = P(E_2) = P(E_3) = 0.6$ and $P(F_1) = P(F_2) = 0.75$. Hence, the probability that all five shots hit the target is

$$\begin{aligned} P(E_1 \cap E_2 \cap E_3 \cap F_1 \cap F_2) &= P(E_1) \times P(E_2) \times P(E_3) \times P(F_1) \times P(F_2) \\ &= (0.6)^3 \times (0.75)^2 \\ &= 0.1215. \end{aligned}$$

(15b) The event that an archer misses the target is the complement of the event of him hitting it, so the probability that the first archer misses the target is 0.4, while the probability that the second archer misses the shot is 0.25. Hence, the probability that all five shots miss the target is

$$\begin{aligned} P(\overline{E_1} \cap \overline{E_2} \cap \overline{E_3} \cap \overline{F_1} \cap \overline{F_2}) &= P(\overline{E_1}) \times P(\overline{E_2}) \times P(\overline{E_3}) \times P(\overline{F_1}) \times P(\overline{F_2}) \\ &= (0.4)^3 \times (0.25)^2 \\ &= 0.004. \end{aligned}$$

(15c) The event that at least one shot hits the target is the complement of the event that no shot hits the target, so the probability that at least one shot hits the target is $1 - 0.004 = 0.996$.

(17) The sample space contains 20! sample points and there is only one arrangement that is in numerical order, so the probability that an arrangement is in numerical order is $\frac{1}{20!}$.

7

Graph Theory

7.1. Introduction to graphs and digraphs

(1a) $n(G) = 12$ and $m(G) = 12$.

(1b) We have the following degrees:

$\deg a = 3$	$\deg b = 2$	$\deg c = 2$	$\deg d = 3$
$\deg e = 1$	$\deg f = 1$	$\deg g = 1$	$\deg h = 1$
$\deg i = 1$	$\deg j = 2$	$\deg k = 1$	$\deg l = 6$

Vertex a is adjacent to b, c and d, while it is incident with ab, ac and ad. Vertex b is adjacent to a and d, while it is incident with ab and bd. Vertex c is adjacent to a and l, while it is incident with ac and cl. Vertex d is adjacent to a, b and l, while it is incident with ad, bd and dl. Vertex e, f, g and h are all adjacent to l and incident with el, fl, gl and hl, respectively. Vertex i is adjacent to j and incident with ij. Vertex j is adjacent to i and k, while it is incident with ij and jk. Vertex k is adjacent to j and incident with jk. Finally, vertex l is adjacent to c, d, e, f, g and h, while it is incident with cl, dl, el, fl, gl and hl.
The vertices b, c, j and l are even, while a, d, e, f, g, h, i and k are odd.
There are no isolated vertices, while e, f, g, h, i and k are end vertices.

(1c) $\delta(G) = 1$ and $\Delta(G) = 6$.

(1d) $H = (V, E)$, where $V = \{a, b, d\}$ and $E = \{ab, ad, bd\}$.

(1e) No, it contains K_3 as a subgraph and hence any partition of the three vertices of the triangle into two sets will have at least two of the three vertices in one of these sets. However, any two of the three vertices are adjacent.

(1f) The path h, l, d, b, a, c has maximum length.

(1g) $d(a, f) = 3$

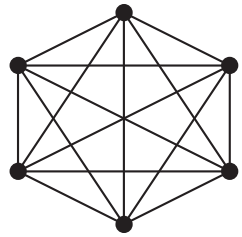
(1h) No, there is no path from a to i.

(1i) 2

Logic and Discrete Mathematics: A Concise Introduction, Solutions Manual, First Edition.
Willem Conradie, Valentin Goranko and Claudette Robinson.
© 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.
Companion Website: www.wiley.com/go/conradie/logic

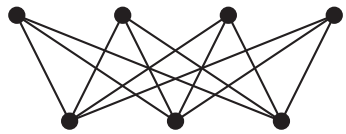
(2) $K_{4,4}$

(3) K_6; see the figure below:



The graph K_6

$K_{4,3}$ K_6; see the figure below:



The graph $K_{4,3}$

(4a) Yes, the cycle C_6 has 6 vertices and 6 edges.

(4b) Yes, K_6 has 6 vertices and 15 edges.

(4c) No. The maximum degree of each vertex is 5, so $5 \cdot 6 = 30 = 2m$. Hence, the maximum number of edges in a graph with 6 vertices is $m = 15$.

(5) No. To have every vertex incident with at least one edge, we must pair up the vertices since each edge is incident with two vertices. Then each pair cannot be joined to any other pair since we want no two edges to be adjacent. However, 5 is odd, so that leaves one vertex out.

(6) No. The subgraph K_1 of the bipartite graph $K_{1,2}$ is not biparite. However, a nontrivial subgraph of a bipartite graph is bipartite.

(7) No. Take K_3 and remove two of its edges. The resulting graph is a subgraph but it is not connected.

(8) If n is odd, then there are $C(n,1) + C(n,2) + \cdots + C\left(n, \frac{n-1}{2}\right)$ complete bipartite graphs. If n is even, there are $C(n,1) + C(n,2) + \cdots + \frac{1}{2}C\left(n, \frac{n}{2}\right)$ complete bipartite graphs.

(9) Since

$$\sum_{i=1}^{n} \deg\, v_i = 2m,$$

we have

$$\begin{aligned} 3n &\le 2m \\ 3n &\le 2 \cdot 35 \\ 3n &\le 70 \\ n &\le 23\frac{1}{3} \end{aligned}$$

Therefore, the largest number of vertices of this graph is 23.

(10a) The indegrees and outdegrees are listed below:

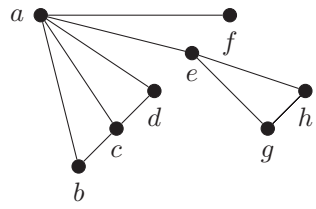
$\text{out}(a) = 5$	$\text{in}(a) = 0$	$\text{out}(b) = 1$	$\text{in}(b) = 1$
$\text{out}(c) = 0$	$\text{in}(c) = 3$	$\text{out}(d) = 1$	$\text{in}(d) = 1$
$\text{out}(e) = 2$	$\text{in}(e) = 1$	$\text{out}(f) = 0$	$\text{in}(f) = 1$
$\text{out}(g) = 1$	$\text{in}(g) = 2$	$\text{out}(h) = 1$	$\text{in}(h) = 2$

Therefore, a is a source while c and f are sinks.

(10b) $n(D) = 8$ and $m(D) = 11$.

(10c) The path a, e, g, h has maximum length.

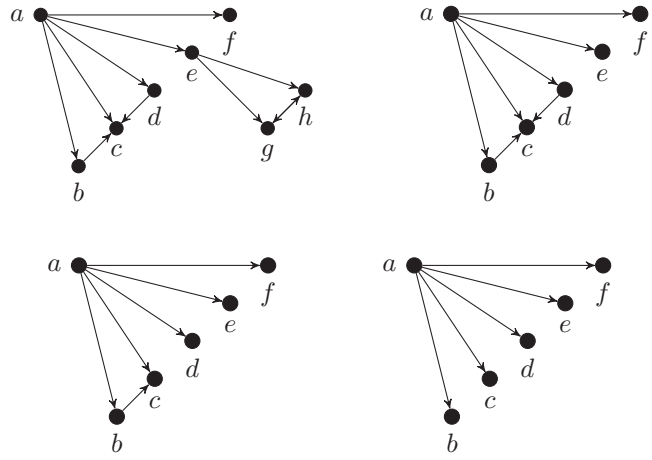
(10d) The underlying graph:



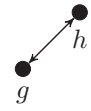
(10e) Yes, its underlying graph is connected.

(10f) No, there is no directed path from f to h.

(10g) Possible subdigraphs:



(10h) $H = (V, E)$, where $V = \{g, h\}$ and $E = \{(g, h), (h, g)\}$:



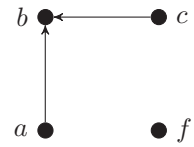
(11a) The maximum indegree is $n - 1$.

(11b) The maximum outdegree is $n - 1$.

(11c) The maximum number of arcs is $(n-1)n = n^2 - n$.

(12a) No, the maximum number of arcs a digraph of order 5 can have is 20.

(12b) Yes.



(13) When outdegrees of vertices are summed, each arc is counted once since every arc is incident from exactly one vertex. Similarly, when indegrees are summed, each arc is counted exactly once.

(14) A directed cycle in digraph D is a sequence of vertices $u_0, u_1, u_2, \ldots, u_n, u_0$ starting and ending at the same vertex u_0 such that (u_{i-1}, u_i), $i = 1, \ldots, n$ and (u_n, u_0) are arcs of D, and no vertex other that u_0 is repeated in the sequence.

7.2. Incidence and adjacency matrices

(1a) Incidence matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccccc} ab & af & ac & bc & bf & cd & de & df \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

(1b) Incidence matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ i \end{array} \begin{array}{c} \begin{array}{ccccccccc} ab & af & be & bg & de & dh & di & fg & fh \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ i \end{array} \begin{array}{c} \begin{array}{ccccccccc} a & b & c & d & e & f & g & h & i \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

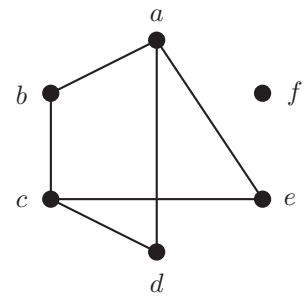
(1c) Incidence matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{cccccc} ab & ad & ae & bc & cd & ce \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

(2a) Sketch:



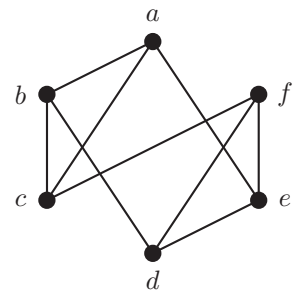
Incidence matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

(2c) Sketch:



Incidence matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{ccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

(3a) Change the entries on the diagonal of the matrix in Exercise(2a) to 1's:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Consider the first column. There is a 1 in rows 2, 4 and 5. Add row 1 to these rows:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Consider the second column. There is a 1 in rows 1, 3, 4 and 5. Add row 2 to these rows:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Continuing this process for the remaining columns will yield the same matrix.

(3c) Change the entries on the diagonal of the matrix in Exercise (2c) to 1's:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Add row 1 to rows 2, 3 and 5:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Add row 2 to rows 1, 3, 4 and 5:

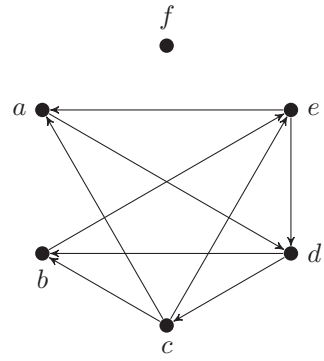
$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Add row 3 to rows 1, 2, 4, 5 and 6:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

(4) The Warshall algorithm computes the existence of walks between vertices, and a graph is connected if there exists a path/walk between every two vertices. If the end result of the application of the Warshall algorithm gives a matrix containing only 1's, we know that there is a walk between every pair of vertices in the graph, which therefore means that the graph is connected. The graphs in Exercise (2b) and (2c) are connected, while the graphs in (2a) and (2d) are not connected.

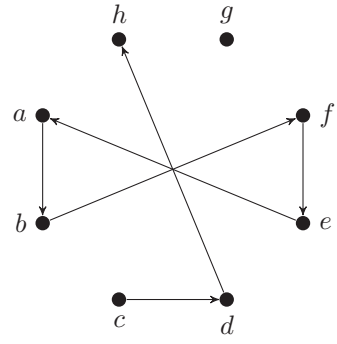
(5a) Sketch:



Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

(5c) Sketch:



Adjacency matrix:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

(6a) Change the entries on the diagonal of the matrix in Exercise (5a) to 1's:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 1 to rows 3 and 5:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 2 to rows 3 and 4:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 3 to row 4:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 4 to rows 1, 3 and 5:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 5 to rows 1, 2, 3 and 4:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

We cannot add row 6 to any of the other rows, so we are done.

(6c) Change all the entries on the diagonal of the matrix in (5c) to 1's:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 1 to row 5:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 2 to rows 1 and 5:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 4 to row 3:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 5 to row 6:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Add row 6 to rows 1, 2 and 5:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Adding row 8 to rows 3 and 4 yields the same matrix.

(7) A digraph is strongly connected if there exists a direct connection from every vertex to every vertex. If the end result of the application of the Warshall algorithm gives a matrix containing only 1's, we know that this is the case. None of the digraphs in the previous question are strongly connected.

(8) To determine the order of a graph from its adjacency matrix, count the number of rows or columns in the matrix. To determine its size, count the 1 and divide the result by 2.

(9) To determine the order of a digraph from its adjacency matrix, count the number of rows or columns in the matrix, and to detemine its size, add the 1's together.

(11) Check that the matrix is symmetric about its main diagonal and that the number of 1's occurring as entries is even. Specifically there should be $2m$ entries that are 1's, where m is the size of the graph.

7.3. Weighted graphs and path algorithms

(1a) Dijkstra's algorithm; see Table 7.1. Reading off from the table, the shortest path from p to q is p, b, c, g, d, q.

Table 7.1 Exercise 1(a)

Step	p	a	b	c	d	e	f	g	q	Last transfer	Perm
Initial	$(-,0)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	p	$\{p\}$
1	$(-,0)$	$(p,4)$	$(p,1)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	b	$\{p,b\}$
2	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	c	$\{p,b,c\}$
3	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(c,5)$	$(-,\infty)$	a	$\{p,b,c,a\}$
4	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(-,\infty)$	$(-,\infty)$	$(-,\infty)$	$(c,5)$	$(-,\infty)$	g	$\{p,b,c,a,g\}$
5	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(g,6)$	$(-,\infty)$	$(g,7)$	$(c,5)$	$(-,\infty)$	d	$\{p,b,c,a,g,d\}$
6	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(g,6)$	$(d,13)$	$(g,7)$	$(c,5)$	$(d,9)$	f	$\{p,b,c,a,g,d,f\}$
7	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(g,6)$	$(f,8)$	$(g,7)$	$(c,5)$	$(d,9)$	e	$\{p,b,c,a,g,d,f,e\}$
8	$(-,0)$	$(p,4)$	$(p,1)$	$(b,3)$	$(g,6)$	$(f,8)$	$(g,7)$	$(c,5)$	$(d,9)$	q	$\{p,b,c,a,g,d,f,e,q\}$

Floyed – Warshall algorithm:
Steps 1 and 2 produce the matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & \infty & \infty & \infty & \infty & \infty & \infty \\ 4 & 0 & \infty & 3 & \infty & \infty & \infty & \infty & \infty \\ 1 & \infty & 0 & 2 & \infty & \infty & \infty & \infty & \infty \\ \infty & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & \infty & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & \infty & 4 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 & 2 & 2 \\ \infty & \infty & \infty & 2 & 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & \infty & 0 \end{pmatrix} \end{array}$$

In the first iteration, checking for shorter paths via vertex p yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & \infty & \infty & \infty & \infty & \infty & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & \infty & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & \infty & \infty \\ \infty & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & \infty & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & \infty & 4 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 & 2 & 2 \\ \infty & \infty & \infty & 2 & 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & \infty & 0 \end{pmatrix} \end{array}$$

In the second iteration, checking for shorter paths via vertex a yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 7 & \infty & \infty & \infty & \infty & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & \infty & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & \infty & \infty \\ 7 & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & \infty & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & \infty & 4 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 & 2 & 2 \\ \infty & \infty & \infty & 2 & 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & \infty & 0 \end{pmatrix} \end{array}$$

In the third iteration, checking for shorter paths via vertex b yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 3 & \infty & \infty & \infty & \infty & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & \infty & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & \infty & \infty \\ 3 & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & \infty & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & \infty & 4 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 & 2 & 2 \\ \infty & \infty & \infty & 2 & 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & \infty & 0 \end{pmatrix} \end{array}$$

In the fourth iteration, checking for shorter paths via vertex c yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 3 & \infty & \infty & \infty & 5 & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & 5 & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & 4 & \infty \\ 3 & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & \infty & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & \infty & 4 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 & 2 & 2 \\ 5 & 5 & 4 & 2 & 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & \infty & 0 \end{pmatrix} \end{array}$$

In the fifth iteration, checking for shorter paths via vertex d yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 3 & \infty & \infty & \infty & 5 & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & 5 & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & 4 & \infty \\ 3 & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & \infty & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & 8 & 4 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 & 2 & 2 \\ 5 & 5 & 4 & 2 & 1 & 8 & 2 & 0 & 4 \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & 4 & 0 \end{pmatrix} \end{array}$$

In the sixth iteration, checking for shorter paths via vertex e yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 3 & \infty & \infty & \infty & 5 & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & 5 & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & 4 & \infty \\ 3 & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & 8 & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & 8 & 4 \\ \infty & \infty & \infty & \infty & 8 & 1 & 0 & 2 & 2 \\ 5 & 5 & 4 & 2 & 1 & 8 & 2 & 0 & 4 \\ \infty & \infty & \infty & \infty & 3 & 4 & 2 & 4 & 0 \end{pmatrix} \end{array}$$

In the seventh iteration, checking for shorter paths via vertex f yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 3 & \infty & \infty & \infty & 5 & \infty \\ 4 & 0 & 5 & 3 & \infty & \infty & \infty & 5 & \infty \\ 1 & 5 & 0 & 2 & \infty & \infty & \infty & 4 & \infty \\ 3 & 3 & 2 & 0 & \infty & \infty & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & 0 & 7 & 8 & 1 & 3 \\ \infty & \infty & \infty & \infty & 7 & 0 & 1 & 3 & 3 \\ \infty & \infty & \infty & \infty & 8 & 1 & 0 & 2 & 2 \\ 5 & 5 & 4 & 2 & 1 & 3 & 2 & 0 & 4 \\ \infty & \infty & \infty & \infty & 3 & 3 & 2 & 4 & 0 \end{pmatrix} \end{array}$$

In the eighth iteration, checking for shorter paths via vertex g yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ q \end{array} \begin{array}{c} \begin{array}{ccccccccc} p & a & b & c & d & e & f & g & q \end{array} \\ \begin{pmatrix} 0 & 4 & 1 & 3 & 6 & 6 & 7 & 5 & 9 \\ 4 & 0 & 5 & 3 & 6 & 8 & 7 & 5 & 9 \\ 1 & 5 & 0 & 2 & 5 & 7 & 6 & 4 & 8 \\ 3 & 3 & 2 & 0 & 3 & 5 & 4 & 2 & 6 \\ 6 & 6 & 5 & 3 & 0 & 4 & 3 & 1 & 3 \\ 6 & 8 & 7 & 5 & 4 & 0 & 1 & 3 & 3 \\ 7 & 7 & 6 & 4 & 3 & 1 & 0 & 2 & 2 \\ 5 & 5 & 4 & 2 & 1 & 3 & 2 & 0 & 4 \\ 9 & 9 & 8 & 6 & 3 & 3 & 2 & 4 & 0 \end{pmatrix} \end{array}$$

Checking for shorter paths via q yields the same matrix.

(1b) Dijkstra's algorithm; see Table 7.2.
Reading off from the table, the shortest path from p to q is: p, c, b, q.
Floyed-Warshall algorithm:
Steps 1 and 2 produce the matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 2 & \infty & 1 & \infty & \infty \\ 2 & 0 & 4 & \infty & \infty & \infty \\ \infty & 4 & 0 & 2 & \infty & 1 \\ 1 & \infty & 2 & 0 & 4 & \infty \\ \infty & \infty & \infty & 4 & 0 & 2 \\ \infty & \infty & 1 & \infty & 2 & 0 \end{pmatrix} \end{array}$$

Table 7.2 Exercise 1(b)

Step	p	a	b	c	d	q	Last transfer	Perm
Initial	$(-, 0)$	$(-, \infty)$	$(-, \infty)$	$(-, \infty)$	$(-, \infty)$	$(-, \infty)$	p	$\{p\}$
1	$(-, 0)$	$(p, 2)$	$(-, \infty)$	$(p, 1)$	$(-, \infty)$	$(-, \infty)$	c	$\{p, c\}$
2	$(-, 0)$	$(p, 2)$	$(c, 3)$	$(p, 1)$	$(c, 5)$	$(-, \infty)$	a	$\{p, c, a\}$
3	$(-, 0)$	$(p, 2)$	$(c, 3)$	$(p, 1)$	$(c, 5)$	$(-, \infty)$	b	$\{p, c, a, b\}$
4	$(-, 0)$	$(p, 2)$	$(c, 3)$	$(p, 1)$	$(c, 5)$	$(b, 4)$	q	$\{p, c, a, b, q\}$

In the first iteration, checking for shorter paths via vertex p yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 2 & \infty & 1 & \infty & \infty \\ 2 & 0 & 4 & 3 & \infty & \infty \\ \infty & 4 & 0 & 2 & \infty & 1 \\ 1 & 3 & 2 & 0 & 4 & \infty \\ \infty & \infty & \infty & 4 & 0 & 2 \\ \infty & \infty & 1 & \infty & 2 & 0 \end{pmatrix} \end{array}$$

In the second iteration, checking for shorter paths via vertex a yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 2 & 6 & 1 & \infty & \infty \\ 2 & 0 & 4 & 3 & \infty & \infty \\ 6 & 4 & 0 & 2 & \infty & 1 \\ 1 & 3 & 2 & 0 & 4 & \infty \\ \infty & \infty & \infty & 4 & 0 & 2 \\ \infty & \infty & 1 & \infty & 2 & 0 \end{pmatrix} \end{array}$$

In the third iteration, checking for shorter paths via vertex b yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 2 & 6 & 1 & \infty & 7 \\ 2 & 0 & 4 & 3 & \infty & 5 \\ 6 & 4 & 0 & 2 & \infty & 1 \\ 1 & 3 & 2 & 0 & 4 & 3 \\ \infty & \infty & \infty & 4 & 0 & 2 \\ 7 & 5 & 1 & 3 & 2 & 0 \end{pmatrix} \end{array}$$

In the fourth iteration, checking for shorter paths via vertex c yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 2 & 3 & 1 & 5 & 4 \\ 2 & 0 & 4 & 3 & 7 & 5 \\ 3 & 4 & 0 & 2 & 6 & 1 \\ 1 & 3 & 2 & 0 & 4 & 3 \\ 5 & 7 & 6 & 4 & 0 & 2 \\ 4 & 5 & 1 & 3 & 2 & 0 \end{pmatrix} \end{array}$$

In the fifth iteration, we obtain the same matrix as above. Finally, checking for shorter paths via vertex q yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 2 & 3 & 1 & 5 & 4 \\ 2 & 0 & 4 & 3 & 7 & 5 \\ 3 & 4 & 0 & 2 & 3 & 1 \\ 1 & 3 & 2 & 0 & 4 & 3 \\ 5 & 7 & 3 & 4 & 0 & 2 \\ 4 & 5 & 1 & 3 & 2 & 0 \end{pmatrix} \end{array}$$

(2) Steps 1 and 2 produce the matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 4 & \infty & \infty \\ 1 & 0 & 3 & \infty & 1 & 6 \\ 2 & 3 & 0 & 1 & \infty & 3 \\ 4 & \infty & 1 & 0 & \infty & 1 \\ \infty & 1 & \infty & \infty & 0 & 4 \\ \infty & 6 & 3 & 1 & 4 & 0 \end{pmatrix} \end{array}$$

In the first iteration, checking for shorter paths via vertex p yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 4 & \infty & \infty \\ 1 & 0 & 3 & 5 & 1 & 6 \\ 2 & 3 & 0 & 1 & \infty & 3 \\ 4 & 5 & 1 & 0 & \infty & 1 \\ \infty & 1 & \infty & \infty & 0 & 4 \\ \infty & 6 & 3 & 1 & 4 & 0 \end{pmatrix} \end{array}$$

In the second iteration, checking for shorter paths via vertex a yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 4 & 2 & 7 \\ 1 & 0 & 3 & 5 & 1 & 6 \\ 2 & 3 & 0 & 1 & 4 & 3 \\ 4 & 5 & 1 & 0 & 6 & 1 \\ 2 & 1 & 4 & 6 & 0 & 4 \\ 7 & 6 & 3 & 1 & 4 & 0 \end{pmatrix} \end{array}$$

In the third iteration, checking for shorter paths via vertex b yields the following matrix:

$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 3 & 2 & 5 \\ 1 & 0 & 3 & 4 & 1 & 6 \\ 2 & 3 & 0 & 1 & 4 & 3 \\ 3 & 4 & 1 & 0 & 5 & 1 \\ 2 & 1 & 4 & 5 & 0 & 4 \\ 5 & 6 & 3 & 1 & 4 & 0 \end{pmatrix} \end{array}$$

In the fourth iteration, checking for shorter paths via vertex b yields the following matrix:

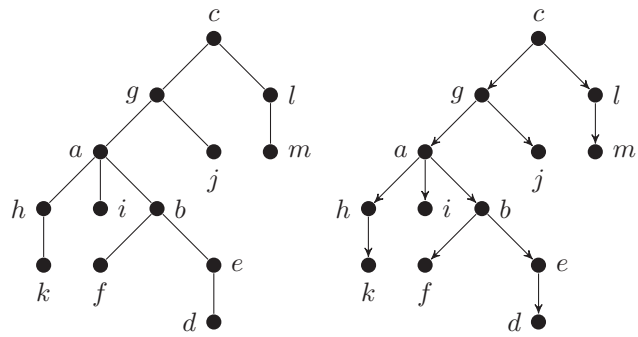
$$\begin{array}{c} \\ p \\ a \\ b \\ c \\ d \\ q \end{array} \begin{array}{c} \begin{array}{cccccc} p & a & b & c & d & q \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 3 & 2 & 4 \\ 1 & 0 & 3 & 4 & 1 & 5 \\ 2 & 3 & 0 & 1 & 4 & 2 \\ 3 & 4 & 1 & 0 & 5 & 1 \\ 2 & 1 & 4 & 5 & 0 & 4 \\ 4 & 5 & 2 & 1 & 4 & 0 \end{pmatrix} \end{array}$$

Checking for shorter paths via c, d and q does not change the matrix.

7.4. Trees

(1a.i) Yes, it is a tree.

(1a.ii) Rooted tree and derived rooted directed tree:



(1a.iii) Height of the rooted tree: 5.

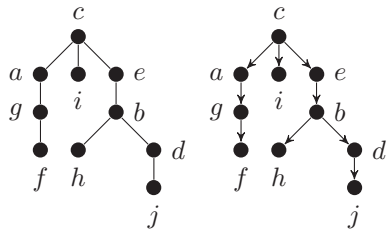
(1a.iv) Level of vertex e: 4.

(1b) The graph contains a cycle, namely b, c, d, e, h, g, f, b, so it is not a tree.

(1c) The graph contains a cycle, namely c, a, d, b, c, so it is not a tree.

(1d.i) Yes, it is a tree.

(1d.ii) Rooted tree and derived rooted directed tree:



(1d.iii) Height of rooted tree: 4.

(1d.iv) Level of vertex e: 1.

(2a.i) $a, b, c, d, g, h, e, l, i, j, k, f$

(2a.ii) $a, b, d, e, k, f, c, g, l, i, h, j$

(2a.iii) $k, e, f, d, b, a, l, g, i, c, h, j$

(2a.iv) $k, f, e, d, b, l, i, g, j, h, c, a$

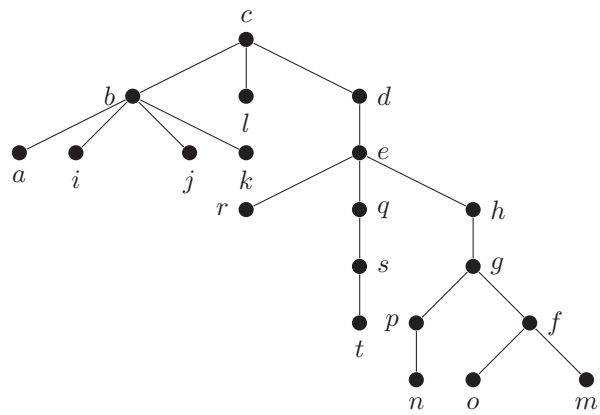
(2b.i) $a, b, c, d, e, f, g, l, m, h, i, n, o, j, k$

(2b.ii) $a, b, d, l, m, e, h, j, c, f, i, k, g, n, o$

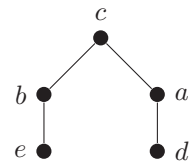
(2b.iii) $l, d, m, b, e, j, h, i, k, f, c, n, g, o$

(2b.iv) $l, m, d, j, h, e, b, k, i, f, n, o, g, c, a$

(3b)



(3c)



(4a) See Table 7.3 for the run of the algorithm.

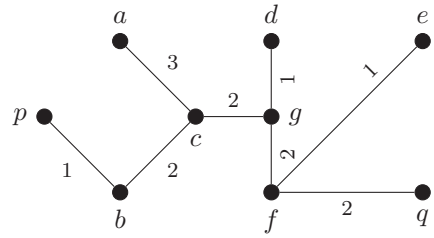


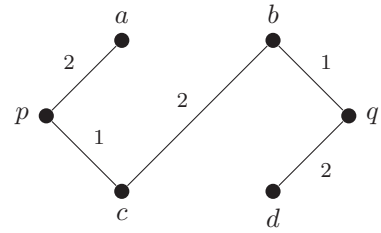
Table 7.3 Exercise 4(a)

Step	e	S	X	$V(\langle X\rangle_X) = V(G)$
0	–	$\{pa, pb, ac, bc, cg, gd, gf, fq, dq, de, ef, eq\}$	$\varnothing$	*NO*
1	pb	$\{pa, ac, bc, cg, gd, gf, fq, dq, de, ef, eq\}$	$\{pb\}$	*NO*
2	gd	$\{pa, ac, bc, cg, gf, fq, dq, de, ef, eq\}$	$\{pb, gd\}$	*NO*
3	ef	$\{pa, ac, bc, cg, gf, fq, dq, de, eq\}$	$\{pb, gd, ef\}$	*NO*
4	bc	$\{pa, ac, cg, gf, fq, dq, de, eq\}$	$\{pb, gd, ef, bc\}$	*NO*
5	cg	$\{pa, ac, gf, fq, dq, de, eq\}$	$\{pb, gd, ef, bc, cg\}$	*NO*
6	fq	$\{pa, ac, gf, dq, de, eq\}$	$\{pb, gd, ef, bc, cg, fq\}$	*NO*
7	gf	$\{pa, ac, dq, de, eq\}$	$\{pb, gd, ef, bc, cg, fq, gf\}$	*NO*
8	ac	$\{pa, dq, de, eq\}$	$\{pb, gd, ef, bc, cg, fq, gf, ac\}$	*YES*

Table 7.4 Exercise 4(b)

Step	e	S	X	$V(\langle X\rangle_X) = V(G)$
0	–	$\{pa, pc, ab, cd, cb, bq, dq\}$	$\varnothing$	*NO*
1	pc	$\{pa, ab, cd, cb, bq, dq\}$	$\{pc\}$	*NO*
2	bq	$\{pa, ab, cd, cb, dq\}$	$\{pc, bq\}$	*NO*
3	dq	$\{pa, ab, cd, cb\}$	$\{pc, bq, dq\}$	*NO*
4	cb	$\{pa, ab, cd\}$	$\{pc, bq, dq, cb\}$	*NO*
5	pa	$\{ab, cd\}$	$\{pc, bq, dq, cb, pa\}$	*YES*

(4b) See Table 7.4 for the run of the algorithm.

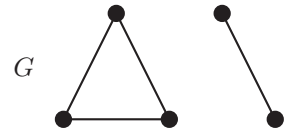


(5) We know that $22 = \sum_{v\in V(T)} deg\,(v) = 2m(T)$, so $m(T) = 11$. Hence, $n(T) = m(T) + 1 = 11 + 1 = 12$.

(6) We have $m(T) = n(T) - 1 = 13 - 1 = 12$, so $\sum_{v\in V(T)} deg\,(v) = 2m(T) = 2(12) = 24$.

(8) Let T be a tree with at least two vertices. To prove that T is bipartite, we have to show that we can divide $V(T)$ into two disjoint subsets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 to a vertex in V_2. Let v be an arbitrary vertex of T and root T at v. Since T has at least two vertices, the rooted tree has at least two levels. Let V_1 consist of all vertices on odd numbered levels and V_2 of all vertices on even numbered levels. It is clear that V_1 and V_2, so defined, form a partition of $V(T)$. Moreover, since there are no edges between vertices on the same level of a rooted tree, all edges in T connect vertices in V_1 with vertices in V_2.

(9) Consider the graph G below:



We have $n = m + 1$, but G is not a tree.

(10) K_1 and K_2 are clearly trees, but for $i \geq 3$, note that $m(K_i) = \frac{i(i-1)}{2} \neq i - 1 = n(K_i) - 1$, so, by Theorem 7.4.10, K_i is not a tree for $i \geq 3$. Alternatively, note that, for $i \geq 3$, $m(K_i)$ contains K_3 as a subgraph and hence it will not be acyclic.

(11) $K_{i,j}$ is a tree for $i = 1$ and $j \geq 1$, or vice versa. To see this, note that if $i = 1$ and $j \geq 1$, we have $n(K_{i,j}) = i + j = 1 + j$ and $m(K_{i,j}) = i \times j = j$, so $n(K_{i,j}) = 1 + j = m(K_{i,j}) + 1$, which means that $K_{i,j}$ is a tree by Theorem 7.4.10. If both $i \geq 2$ and $j \geq 2$, $K_{i,j}$ contains a cycle (of length 4) and is therefore not a tree.

(12) Let F be a forest with k connected components, n vertices and m edges. Now, since each component is a tree, we have that $n_i = m_i + 1$, where n_i is the number of vertices in the ith component and m_i the

number of edges in the ith component, $i = 1, 2, \ldots, k$. This means that

$$n = \sum_{i=1}^{k} n_i = \sum_{i=1}^{k} (m_i + 1) = m + k,$$

and therefore $m = n - k$, as required.

7.5. Eulerian graphs and Hamiltonian graphs

(1a) The graph is not Eulerian since it contains odd vertices; however, it contains an Eulerian trail.

(1b) Since all vertices are even, the graph contains an Eulerian circuit and hence it is Eulerian.

(1c) The graph is not Eulerian since it contains odd vertices. It also does not contain an Eulerian trail since it contains four odd vertices.

(1d) The graph is not Eulerian since it contains two odd vertices; however, it contains an Eulerian trail.

(1e) Since all vertices are even, the graph contains an Eulerian circuit and hence it is Eulerian.

(1f) The graph contains 4 odd vertices, so it does not contain an Eulerian trail and it is also not Eulerian.

(2a) The directed graph is not Eulerian since the indegrees of vertices a and b do not equal their respective outdegrees. However, it contains a directed Eulerian trail, namely a, b, c, d, b.

(2b) The directed graph is not Eulerian since the indegrees of vertices a and c do not equal their respective outdegrees. It also does not contain a directed Eulerian trail.

(2c) The directed graph contains a directed Eulerian circuit, namely a, b, c, a, and hence is Eulerian.

(2d) The directed graph is not Eulerian since the indegrees of vertices a, c, e, f, g and h do not equal their respective outdegrees. It also does not contain a directed Eulerian trail.

(3) The graph of the octahedron is Eulerian. The graphs of all the other solids are not Eulerian and also do not contain Eulerian trails since they all have more than two odd vertices.

(4a) The graph is not Hamiltonian but does contain a Hamiltonian path.

(4b) The graph is Hamiltonian.

(4c) The graph is not Hamiltonian and also does not contain a Hamiltonian path.

(4d) The graph is Hamiltonian.

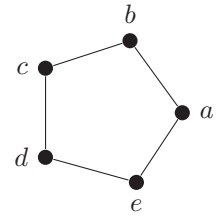
(4e) The graph is Hamiltonian.

(4f) The graph is Hamiltonian.

(5) The graphs of all five solids are Hamiltonian.

(6) Assume G has two connected components, each of which has an Eulerian trail. Denote the initial vertices of each of these trails by u and u', respectively, and the terminal vertices by v and v', respectively. Now add the edges $v'u$ and vu' to G to obtain the graph G'. Clearly, G' then has a Eulerian circuit, namely $u, \ldots, v, u', \ldots, v', u$, so, by definition, G' is Eulerian.

(7) Consider the following graph:



This graph is clearly Hamiltonian, but $\deg a + \deg c = 2 + 2 = 4 \not\geq 5$.

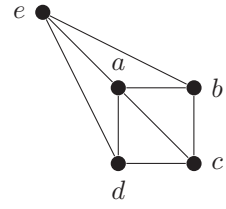
(8) $K_{j,k}$ is Hamiltonian for $j, k \geq 2$ and $j = k$.

(10) There is no relationship between Eulerian and Hamiltonian graphs. To see this, note that the second graph in Example 7.5.2 is Eulerian but not Hamiltonian. On the other hand, the graphs of the solids, except for the cube, in Exercise 3 are Hamiltonian but not Eulerian.

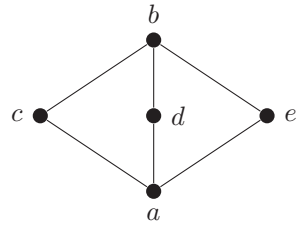
(11) For the left-to-right direction, suppose G contains an Eulerian trail $u - v$. Then $G + uv$ is Eulerian and so, by Theorem 7.5.3, every vertex of $G + uv$ is even. However, this means that every vertex of G different from u and v has even degree, while u and v must be odd. For the right-to-left direction, suppose G is a connected graph having exactly two odd vertices u and v. If G does not contain uv, then $G + uv$ is Eulerian. If uv is removed from the Eulerian circuit of $G + uv$, then we have an Eulerian trail in G. If uv is in G, we can add another vertex w along with edges uw and vw, producing a connected graph H in which every vertex is even. Therefore, H is Eulerian and contains an Eulerian circuit C. This circuit must contain uw and vw as consecutive edges so that we can remove them from C, and so an Eulerian trail remains. This trail begins at u and ends at v.

7.6. Planar graphs

(1a) Yes, it is planar:



(1b) Yes, it is planar:



(1c) The graph is not planar, since the subgraph $H = (V, E)$ with $V = \{a, b, c, d, e\}$ and $E = \{ab, bd, de, ae, bc, cd, ce, ac, be, ad\}$ is a subdivision of K_5.

(1d) The graph is not planar, since the subgraph $H = (V, E)$ with $V = \{a, b, c, d, e, f\}$ and $E = \{ad, ae, af, bd, be, bf, cd, ce, cf\}$ is a subdivision of $K_{3,3}$.

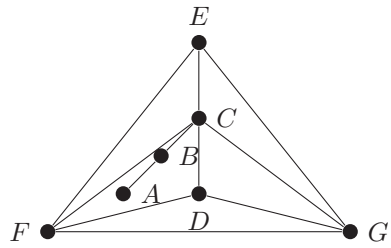
(1e) The graph is not planar, since the subgraph $H = (V, E)$ with $V = \{a, b, c, d, e, g, h, i, j\}$ and $E = \{ad, ae, ah, bd, be, bi, cd, ce, cj, gi, gh, gj\}$ is a subdivision of $K_{3,3}$.

(2) The greatest order a complete planar graph can have is 4, since K_5 is a subgraph of K_n for all $n \geq 5$ and we know that K_4 is planar.

(3) We know that $\sum \deg \ v = 3 \cdot 6 = 18 = 2m$, so we get $m = 9$. Furthermore, $n - m + f = 6 - 9 + f = 2$ and therefore $f = 5$.

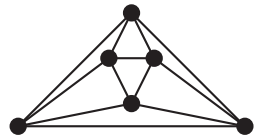
(4) We know that $\sum \deg \ v = 1 \cdot 2 + 4 \cdot 3 + 1 \cdot 4 = 18 = 2m$, so $m = 9$. Furthermore, $n - m + f = 6 - 9 + f = 2$ and therefore $f = 5$.

(5) If we can model this information in a planar graph, the components can be embedded in a single layer on a circuit board. This is indeed the case:



(6a) By Lemma 7.6.4 it must be the case that $3n - m \geq 6$, i.e. $3n - 6 \geq m$. Therefore $3 \cdot 6 - 6 \geq m$, so m can be at most 12.

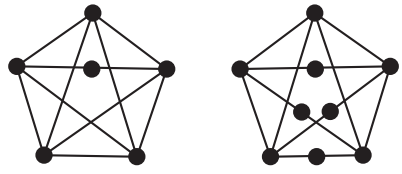
(6b) A connected planar graph of order 6 and size 12:



(7a) $3k - 6$, by Lemma 7.6.4.

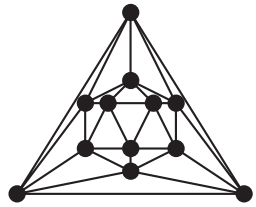
(7b) Note that the shortest length of any cycle is 3, so no face is bounded by less than 3 edges. Now, suppose that at least one face is bounded by more than 3 edges and let N denote the sum of the number of edges bounding a face, summed over all f faces. Then $N > 3f$. Each edge is counted precisely twice as each edge is on the boundary of exactly 2 regions. Furthermore, there are $3k - 6$ edges, so we must have $N = 2(3k - 6) = 6k - 12$. By Theorem 7.6.3, $f = 2 - k + 3k - 6 = 2k - 4$. Therefore, we have $N > 3(2k - 4) = 6k - 12$, a contradiction.

(8)

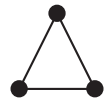


(9) $K_{3,3}$ is a counterexample, since $3(6) - 9 = 9 \geq 6$, yet $K_{3,3}$ is not planar.

(10) The icosahedron:



(11) K_3:



(12a) Let G be a graph with n vertices and m edges, and suppose G has two components. Then $n_1 - m_1 + f_1 = 2$ and $n_2 - m_2 + f_2 = 2$ for the two components of G. Furthermore, note that f_1 and f_2 both include the external face, so $f = f_1 + f_2 - 1$. Hence, $(n_1 + n_2) - (m_1 + m_2) + (f_1 + f_2) = 4$, which means $(n_1 + n_2) - (m_1 + m_2) + (f_1 + f_2 - 1) = 3$. Therefore, we get $n - m + f = 3$.

(12b) With a similar argument as in Exercise 6(a), we have that $n - m + f = 4$.

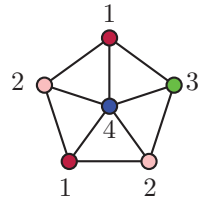
(12c) With a similar argument as in 6(a), we get $n - m + f = 2k - (k - 1) = k + 1$.

(13) Let G be a planar graph and let G' be a subdivision of G. If G is planar it can be drawn as a plane graph. Now subdividing a plane graph does not cause any edges to cross, so the subdivision will also be plane. Hence G' is planar.
Conversely, suppose that G' is planar and a subdivision of G. Then G' can be drawn as a plane graph. Now removing the vertices introduced by the subdivision and restoring the original edges in G', drawn as a plane graph, cannot cause any edges to cross, so G can be drawn as a plane graph and hence is planar.

(14) Let G be a planar (n, m) graph with k components such that each component contains at least 3 vertices. Now, by Lemma 7.6.4, $3n_i - m_i \geq 6$ for each $1 \leq i \leq k$, where n_i is the number of vertices in the ith component and m_i the number of edges in the ith component. Adding these inequalities together, we get $3(n_1 + \cdots + n_k) - (m_1 + \cdots + m_k) \geq 6k$. Hence, $3n - m \geq 6k$.

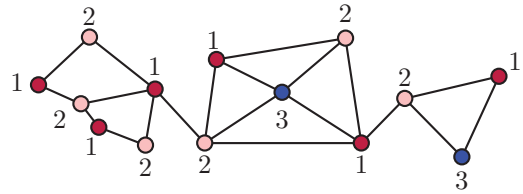
7.7. Graph colourings

(1a) The graph has chromatic number 4. Below is a colouring using 4 colours:



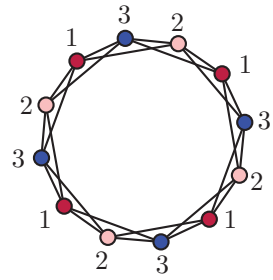
The graph contains C_5 as a subgraph, which means we must use at least 3 colours. Furthermore, the vertex in the middle is adjacent to every other vertex in the cycle, so we need a fourth colour.

(1b) The graph has chromatic number 3. Below is a colouring using 3 colours:



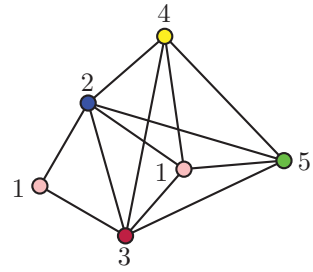
We cannot use fewer than 3 colours since the graph contains K_3 as a subgraph.

(1c) The graph has chromatic number 3. Below is a colouring using 3 colours:



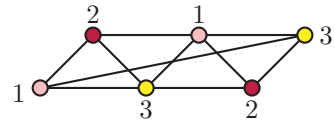
We cannot use fewer than 3 colours since the graph contains K_3 as a subgraph.

(1d) The graph has chromatic number 5. Below is a colouring using 5 colours:



We cannot use fewer than 5 colours since the graph contains K_4 (requiring 4 colours) as a subgraph and another vertex, which is adjacent to each vertex, in this subgraph, thus requires a fifth colour.

(1e) The graph has chromatic number 3. Below is a colouring using 3 colours:

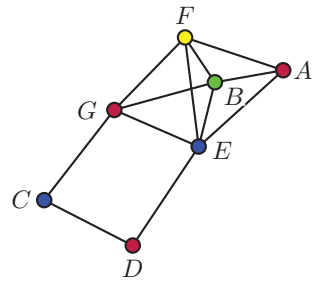


We cannot use fewer than 3 colours since the graph contains K_3 as a subgraph.

(2) A cycle of even length has chromatic number 2 since the vertices can just alternate colour. A cycle of odd length has chromatic number 3, since alternating only 2 colours would leave 2 adjacent vertices of the same colour.

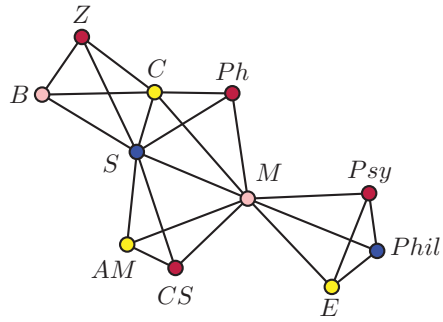
(3) $K_{3,3}$ has chromatic number 2. This is the same for $K_{4,6}$ and $K_{101,98}$. In fact, any complete bipartite graph has chromatic number 2.

(4) The problem is equivalent to finding the chromatic number of the graph in which cities are nodes and cities are adjacent if the corresponding cities are less than 500 km apart. Below is a graph modelling this problem with a colouring using the least number of colours (colours *A*, *D* and *G* purple, *C* and *E* blue, *B* green and *F* yellow):



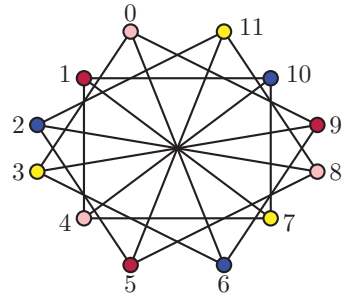
Hence, the chromatic number of this graph is 4, which means that at least 4 frequencies are required.

(5) Below is a colouring using a minimum number of colours (colour *CS*, *Psy*, *Ph* and *Z* purple, *B* and *M* pink, *AM*, *C* and *E* yellow, and *Phil* and *S* blue):



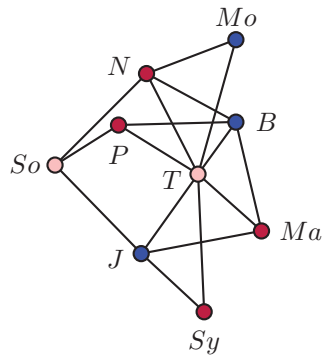
Hence, the minimum number of time slots required is 4.

(6) We can model this problem as a graph colouring problem by representing the integers $0, 1, 2, \ldots, 11$ as vertices and making two vertices adjacent if and only if the corresponding integers are congruent modulo 3. The clusters are then the colours in a colouring of the graph. Below is a graph with a colouring using a minimum number of colours (colours 0, 4 and 8 pink, 1, 5 and 9 purple, 2, 6 and 10 blue and 3, 7 and 11 yellow):



Hence, the minimum number of clusters such a partition can have is 4.

(7) We can model this problem as a graph colouring problem by representing the cats as the vertices and making two vertices adjacent if and only if the corresponding cats fight. The rooms are then the colours in a colouring of the graph. Below is a colouring using a minimum number of colours (colours *Ma*, *N*, *P* and *Sy* purple, *So* and *T* pink and *B*, *J* and *Mo* blue):



Hence, Mrs Winterbottom requires at least 3 rooms for her cats.

(8) False. Take for instance any cycle. A cycle is planar but has chromatic number 2 or 3.

(9) True. If G contains no subdivision of K_5 or $K_{3,3}$ as a subgraph, then G is planar by Kuratowski's theorem, and hence, by the four-colour theorem, G is 4-colourable.

(10) The chromatic number of every nontrivial tree is 2, while the chromatic number of the trivial tree is 1. The chromatic number of any forest with at least one nontrivial connected component is also 2. If all components of the forrest are trivial, then its chromatic number is 1.

(11a) If a graph is 4-colourable, then it is planar.

(11b) No, the graph $K_{3,3}$ is 4-colourable but it is not planar.

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.