Solutions to Chapter 7, Susanna Epp Discrete Math 5th Edition

https://github.com/spamegg1

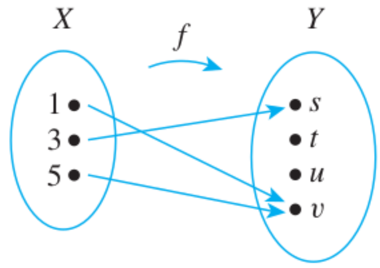
September 5, 2023

Contents

1 Exercise Set 7.1

1.1 Exercise 1

Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$. Define $f : X \to Y$ by the following arrow diagram.



1.1.1 (a)

Write the domain of f and the co-domain of f.

Proof. domain of $f = \{1, 3, 5\}$, co-domain of $f = \{s, t, u, v\}$ □

1.1.2 (b)

Find $f(1), f(3)$, and $f(5)$.

Proof. $f(1) = v, f(3) = s, f(5) = v$ □

1.1.3 (c)

What is the range of f?

Proof. range of $f = \{s, v\}$ □

1.1.4 (d)

Is 3 an inverse image of s? Is 1 an inverse image of u?

Proof. yes, no □

1.1.5 (e)

What is the inverse image of s? of u? of v?

Proof. inverse image of $s = \{3\}$, inverse image of $u = \varnothing$, inverse image of $v = \{1, 5\}$ □

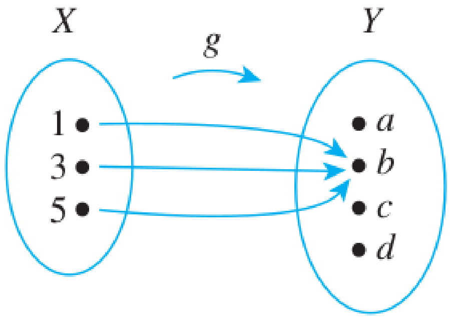
1.1.6 (f)

Represent f as a set of ordered pairs.

Proof. $\{(1, v), (3, s), (5, v)\}$ □

1.2 Exercise 2

Let $X = \{1, 3, 5\}$ and $Y = \{a, b, c, d\}$. Define $g : X \to Y$ by the following arrow diagram.



1.2.1 (a)

Write the domain of g and the co-domain of g.

Proof. domain: $\{1, 3, 5\}$ co-domain: $\{a, b, c, d\}$ □

1.2.2 (b)

Find $g(1), g(3)$, and $g(5)$.

Proof. $g(1) = b, g(3) = b, g(5) = b$ □

1.2.3 (c)

What is the range of g?

Proof. $\{b\}$ □

1.2.4 (d)

Is 3 an inverse image of a? Is 1 an inverse image of b?

Proof. no, yes □

1.2.5 (e)

What is the inverse image of b? of c?

Proof. $\{1, 3, 5\}$ and $\varnothing$ □

1.2.6 (f)

Represent g as a set of ordered pairs.

Proof. $\{(1, b), (3, b), (5, b)\}$ □

1.3 Exercise 3

Indicate whether the statements in parts (a)–(d) are true or false for all functions. Justify your answers.

1.3.1 (a)

If two elements in the domain of a function are equal, then their images in the co-domain are equal.

Proof. True. The definition of function says that for any input there is one and only one output, so if two inputs are equal, their outputs must also be equal. □

1.3.2 (b)

If two elements in the co-domain of a function are equal, then their preimages in the domain are also equal.

Proof. Not necessarily true. A function can have the same output for more than one input. □

1.3.3 (c)

A function can have the same output for more than one input.

Proof. True. The definition of function does not prohibit this occurrence. □

1.3.4 (d)

A function can have the same input for more than one output.

Proof. False, this is ruled out by the definition of a function. Functions are single valued. Every input corresponds to only one output. □

1.4 Exercise 4

1.4.1 (a)

Find all functions from $X = \{a, b\}$ to $Y = \{u, v\}$.

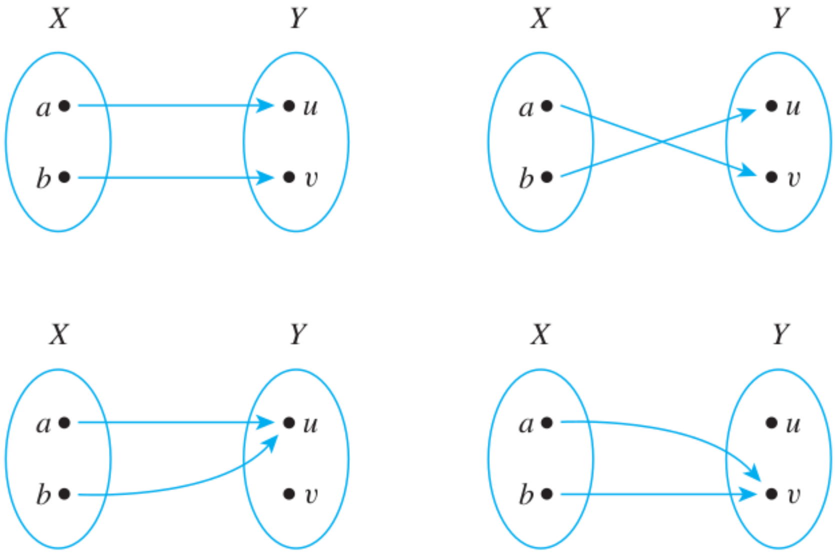
Proof. There are four functions from X to Y as shown *on the next page.*

□

1.4.2 (b)

Find all functions from $X = \{a, b, c\}$ to $Y = \{u\}$.

Proof. There is only one function $f : X \to Y$ given by the set $\{(a, u), (b, u), (c, u)\}$. □



1.4.3 (c)

Find all functions from $X = \{a, b, c\}$ to $Y = \{u, v\}$.

Proof. There are 8 functions:

$\{(a, u), (b, u), (c, u)\}$

$\{(a, u), (b, u), (c, v)\}$

$\{(a, u), (b, v), (c, u)\}$

$\{(a, u), (b, v), (c, v)\}$

$\{(a, v), (b, u), (c, u)\}$

$\{(a, v), (b, u), (c, v)\}$

$\{(a, v), (b, v), (c, u)\}$

$\{(a, v), (b, v), (c, v)\}$ $\square$

1.5 Exercise 5

Let $I_{\mathbb{Z}}$ be the identity function defined on the set of all integers, and suppose that $e, b_i^{jk}, K(t)$, and u_{kj} all represent integers. Find the following:

1.5.1 (a)

$I_{\mathbb{Z}}(e)$

Proof. e (because $I_{\mathbb{Z}}$ is the identity function). $\square$

1.5.2 (b)

$I_{\mathbb{Z}}(b_i^{jk})$

Proof. b_i^{jk} (because $I_{\mathbb{Z}}$ is the identity function). $\square$

1.5.3 (c)

$I_{\mathbb{Z}}(K(t))$

Proof. $K(t)$ (because $I_{\mathbb{Z}}$ is the identity function). $\square$

1.5.4 (d)

$I_{\mathbb{Z}}(u_{kj})$

Proof. u_{kj} (because $I_{\mathbb{Z}}$ is the identity function). $\square$

1.6 Exercise 6

Find functions defined on the set of nonnegative integers that can be used to define the sequences whose first six terms are given below.

1.6.1 (a)

$1, -\frac{1}{3}, \frac{1}{5}, -\frac{1}{7}, \frac{1}{9}, -\frac{1}{11}$

Proof. The sequence is given by the function $f : \mathbb{Z}^{nonneg} \to \mathbb{R}$ defined by the rule $f(n) = \frac{(-1)^n}{2n+1}$ for each nonnegative integer n. $\square$

1.6.2 (b)

$0, -2, 4, -6, 8, -10$

Proof. The sequence is given by the function $f : \mathbb{Z}^{nonneg} \to \mathbb{Z}$ defined by the rule $f(n) = (-1)^n \cdot (2n)$ for each nonnegative integer n. $\square$

1.7 Exercise 7

Let $A = \{1, 2, 3, 4, 5\}$, and define a function $F : \mathscr{P}(A) \to \mathbb{Z}$ as follows: For each set X in $\mathscr{P}(A)$,

$$F(x) = \begin{cases} 0 & \text{if } X \text{ has an even number of elements} \\ 1 & \text{if } X \text{ has an odd number of elements} \end{cases}$$

Find the following:

1.7.1 (a)

$F(\{1,3,4\})$

Proof. $F(\{1,3,4\}) = 1$ *[because* $\{1,3,4\}$ *has an odd number of elements]* ☐

1.7.2 (b)

$F(\varnothing)$

Proof. $F(\{\varnothing\}) = 0$ *[because* $\{\varnothing\}$ *has an even number of elements]* ☐

1.7.3 (c)

$F(\{2,3\})$

Proof. $F(\{2,3\}) = 0$ *[because* $\{2,3\}$ *has an even number of elements]* ☐

1.7.4 (d)

$F(\{2,3,4,5\})$

Proof. $F(\{2,3,4,5\}) = 0$ *[because* $\{2,3,4,5\}$ *has an even number of elements]* ☐

1.8 Exercise 8

Let $J_5 = \{0,1,2,3,4\}$, and define a function $F : J_5 \to J_5$ as follows: For each $x \in J_5, F(x) = (x^3 + 2x + 4) \mod 5$. Find the following:

1.8.1 (a)

$F(0)$

Proof. $F(0) = (0^3 + 2 \cdot 0 + 4) \mod 5 = 4 \mod 5 = 4$ ☐

1.8.2 (b)

$F(1)$

Proof. $F(1) = (1^3 + 2 \cdot 1 + 4) \mod 5 = 7 \mod 5 = 2$ ☐

1.8.3 (c)

$F(2)$

Proof. $F(2) = (2^3 + 2 \cdot 2 + 4) \mod 5 = 16 \mod 5 = 1$ ☐

1.8.4 (d)

$F(3)$

Proof. $F(3) = (3^3 + 2 \cdot 3 + 4) \mod 5 = 37 \mod 5 = 2$ $\square$

1.8.5 (e)

$F(4)$

Proof. $F(4) = (4^3 + 2 \cdot 4 + 4) \mod 5 = 76 \mod 5 = 1$ $\square$

1.9 Exercise 9

Define a function $S : \mathbb{Z}^+ \to \mathbb{Z}^+$ as follows: For each positive integer $n, S(n) =$ the sum of the positive divisors of n. Find the following:

1.9.1 (a)

$S(1)$

Proof. $S(1) = 1$

$\square$

1.9.2 (b)

$S(15)$

Proof. $S(15) = 1 + 3 + 5 + 15 = 24$ $\square$

1.9.3 (c)

$S(17)$

Proof. $S(15) = 1 + 17 = 18$ $\square$

1.9.4 (d)

$S(5)$

Proof. $S(5) = 1 + 5 = 6$ $\square$

1.9.5 (e)

$S(18)$

Proof. $S(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39$ $\square$

1.9.6 (f)

$S(21)$

Proof. $S(21) = 1 + 3 + 7 + 21 = 32$ □

1.10 Exercise 10

Let D be the set of all finite subsets of positive integers. Define a function $T : \mathbb{Z}^+ \to D$ as follows: For each positive integer $n, T(n) =$ the set of positive divisors of n. Find the following:

1.10.1 (a)

$T(1)$

Proof. $T(1) = \{1\}$

□

1.10.2 (b)

$T(15)$

Proof. $T(15) = \{1, 3, 5, 15\}$ □

1.10.3 (c)

$T(17)$

Proof. $T(17) = \{1, 17\}$ □

1.10.4 (d)

$T(5)$

Proof. $T(1) = \{1\}$ □

1.10.5 (e)

$T(18)$

Proof. $T(18) = \{1, 2, 3, 6, 9, 18\}$ □

1.10.6 (f)

$T(21)$

Proof. $T(21) = \{1, 3, 7, 21\}$ □

1.11 Exercise 11

Define $F : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ as follows: For every ordered pair (a, b) of integers, $F(a, b) = (2a + 1, 3b - 2)$. Find the following:

1.11.1 (a)

$F(4, 4)$

Proof. $F(4, 4) = (2 \cdot 4 + 1, 3 \cdot 4 - 2) = (9, 10)$ □

1.11.2 (b)

$F(2, 1)$

Proof. $F(2, 1) = (2 \cdot 2 + 1, 3 \cdot 1 - 2) = (5, 1)$ □

1.11.3 (c)

$F(3, 2)$

Proof. $F(3, 3) = (2 \cdot 3 + 1, 3 \cdot 3 - 2) = (7, 7)$ □

1.11.4 (d)

$F(1, 5)$

Proof. $F(1, 5) = (2 \cdot 1 + 1, 3 \cdot 5 - 2) = (3, 13)$ □

1.12 Exercise 12

Let $J_5 = \{0, 1, 2, 3, 4\}$, and define $G : J_5 \times J_5 \to J_5 \times J_5$ as follows: For each $(a, b) \in J_5 \times J_5, G(a, b) = ((2a + 1) \mod 5, (3b - 2) \mod 5)$. Find the following:

1.12.1 (a)

$G(4, 4)$

Proof. $G(4, 4) = ((2 \cdot 4 + 1) \mod 5, (3 \cdot 4 - 2) \mod 5) = (9 \mod 5, 10 \mod 5) = (4, 0)$ □

1.12.2 (b)

$G(2, 1)$

Proof. $G(2, 1) = ((2 \cdot 2 + 1) \mod 5, (3 \cdot 1 - 2) \mod 5) = (5 \mod 5, 1 \mod 5) = (0, 1)$ □

1.12.3 (c)

$G(3, 2)$

Proof. $G(3,2) = ((2 \cdot 3 + 1) \mod 5, (3 \cdot 2 - 2) \mod 5) = (7 \mod 5, 4 \mod 5) = (2, 4)$ □

1.12.4 (d)

$G(1, 5)$

Proof. $G(1,5) = ((2 \cdot 1 + 1) \mod 5, (3 \cdot 5 - 2) \mod 5) = (3 \mod 5, 13 \mod 5) = (3, 3)$ □

1.13 Exercise 13

Let $J_5 = \{0, 1, 2, 3, 4\}$, and define functions $f : J_5 \to J_5$ and $g : J_5 \to J_5$ as follows: For each $x \in J_5, f(x) = (x+4)^2 \mod 5$ and $g(x) = (x^2 + 3x + 1) \mod 5$. Is $f = g$? Explain.

Proof.

x	$f(x)$	$g(x)$
0	$4^2 \mod 5 = 1$	$(0^2 + 3 \cdot 0 + 1) \mod 5 = 1$
1	$5^2 \mod 5 = 0$	$(1^2 + 3 \cdot 1 + 1) \mod 5 = 0$
2	$6^2 \mod 5 = 1$	$(2^2 + 3 \cdot 2 + 1) \mod 5 = 1$
3	$7^2 \mod 5 = 4$	$(3^2 + 3 \cdot 3 + 1) \mod 5 = 4$
4	$8^2 \mod 5 = 4$	$(4^2 + 3 \cdot 4 + 1) \mod 5 = 4$

The table shows that $f(x) = g(x)$ for every x in J_5. Thus, by definition of equality of functions, $f = g$. □

1.14 Exercise 14

Define functions H and K from $\mathbb{R}$ to $\mathbb{R}$ by the following formulas: For every $x \in \mathbb{R}, H(x) = \lfloor x \rfloor + 1$ and $K(x) = \lceil x \rceil$. Does $H = K$? Explain.

Proof. No, because $H(2) = \lfloor 2 \rfloor + 1 = 3 \neq 2 = \lceil 2 \rceil = K(2)$. □

1.15 Exercise 15

Let F and G be functions from the set of all real numbers to itself. Define new functions $F \cdot G : \mathbb{R} \to \mathbb{R}$ and $G \cdot F : \mathbb{R} \to \mathbb{R}$ as follows: For every $x \in \mathbb{R}$, $(F \cdot G)(x) = F(x) \cdot G(x)$, $(G \cdot F)(x) = G(x) \cdot F(x)$. Does $F \cdot G = G \cdot F$? Explain.

Proof.

$$\begin{aligned} (F \cdot G)(x) &= F(x) \cdot G(x) && \text{by definition of } F \cdot G \\ &= G(x) \cdot F(x) && \text{by commutative law for real numbers} \\ &= (G \cdot F)(x) && \text{by definition of } G \cdot F \end{aligned}$$

for every real number x. Therefore $F \cdot G$ and $G \cdot F$ are equal. $\square$

1.16 Exercise 16

Let F and G be functions from the set of all real numbers to itself. Define new functions $F - G : \mathbb{R} \to \mathbb{R}$ and $G - F : \mathbb{R} \to \mathbb{R}$ as follows: For every $x \in \mathbb{R}$, $(F - G)(x) = F(x) - G(x)$, $(G - F)(x) = G(x) - F(x)$. Does $F - G = G - F$? Explain.

Proof. Counterexample: Let $F(x) = 2x, G(x) = 3x$. Then

$$(F - G)(1) = F(1) - G(1) = 2 - 3 = -1 \neq 1 = 3 - 2 = G(1) - F(1) = (G - F)(1).$$

Therefore $F - G$ does not equal $G - F$. $\square$

1.17 Exercise 17

Use the definition of logarithm to fill in the blanks below.

1.17.1 (a)

$\log_2 8 = 3$ because ____ .

Proof. $2^3 = 8$ $\square$

1.17.2 (b)

$\log_5(\frac{1}{25}) = -2$ because ____ .

Proof. $5^{-2} = \dfrac{1}{25}$ $\square$

1.17.3 (c)

$\log_4 4 = 1$ because ____ .

Proof. $4^1 = 4$ $\square$

1.17.4 (d)

$\log_3(3^n) = n$ because ____ .

Proof. $3^n = 3^n$ $\square$

1.17.5 (e)

$\log_4 1 = 0$ because ____ .

Proof. $4^0 = 1$ $\square$

1.18 Exercise 18

Find exact values for each of the following quantities without using a calculator.

1.18.1 (a)

$\log_3 81$

Proof. 4 $\square$

1.18.2 (b)

$\log_2 1024$

Proof. 10 $\square$

1.18.3 (c)

$\log_3 \frac{1}{27}$

Proof. -3 $\square$

1.18.4 (d)

$\log_2 1$

Proof. 0 $\square$

1.18.5 (e)

$\log_{10}(\frac{1}{10})$

Proof. -1 $\square$

1.18.6 (f)

$\log_3 3$

Proof. 1 $\square$

1.18.7 (g)

$\log_2 2^k$

Proof. k $\square$

1.19 Exercise 19

Use the definition of logarithm to prove that for any positive real number b with $b \neq 1, \log_b b = 1$.

Proof. Let b be any positive real number with $b \neq 1$. Since $b^1 = b$, then $\log_b b = 1$ by definition of logarithm. $\square$

1.20 Exercise 20

Use the definition of logarithm to prove that for any positive real number b with $b \neq 1, \log_b 1 = 0$.

Proof. Let b be any positive real number with $b \neq 1$. Since $b^0 = 1$, then $\log_b 1 = 0$ by definition of logarithm. $\square$

1.21 Exercise 21

If b is any positive real number with $b \neq 1$ and x is any real number, b^{-x} is defined as follows: $b^{-x} = \dfrac{1}{b^x}$. Use this definition and the definition of logarithm to prove that $\log_b \left(\dfrac{1}{u}\right) = -\log_b(u)$ for all positive real numbers u and b, with $b \neq 1$.

Proof. Suppose b and u are any positive real numbers with $b \neq 1$. *[We must show that $\log_b(\frac{1}{u}) = -\log_b(u)$.]* Let $v = \log_b(\frac{1}{u})$. By definition of logarithm, $b^v = \frac{1}{u}$. Multiplying both sides by u and dividing by b^v gives $u = b^{-v}$, and thus, by definition of logarithm, $-v = \log_b(u)$. When both sides of this equation are multiplied by -1, the result is $v = -\log_b(u)$. Therefore, $\log_b(\frac{1}{u}) = -\log_b(u)$ because both expressions equal v. *[This is what was to be shown.]* $\square$

1.22 Exercise 22

Use the unique factorization for the integers theorem (Section 4.4) and the definition of logarithm to prove that $\log_3(7)$ is irrational.

Proof. 1. Argue by contradiction and assume $r = \log_3(7)$ is rational.

2. By 1 and definition of rational, $r = a/b$ for some integers a, b where $b \neq 0$.

3. We may assume $b > 0$. (If $b < 0$ then $a/b = (-a)/(-b)$ therefore we can replace a/b with $-a/(-b)$ where $-b > 0$.)

4. By 1, 2 and definition of logarithm, $7 = 3^{a/b}$.

5. By 4, taking the bth powers of both sides, we get $7^b = 3^a$.

6. Since b is a positive integer, 7^b is a positive integer. Therefore 3^a is the same positive integer.

7. By 6, we have two different prime factorizations of the same positive integer. By the uniqueness part of the prime factorization theorem, this is only possible if the positive integer is equal to 1.

8. By 7, $7^b = 3^a = 1$ so $a = b = 0$. This is a contradiction since $b > 0$.

9. So our supposition in 1 is false by 8, thus $\log_3(7)$ is irrational. □

1.23 Exercise 23

If b and y are positive real numbers such that $\log_b y = 3$, what is $\log_{1/b}(y)$? Explain.

Proof. By definition of logarithm with base b, $b^3 = y$. So

$$y = b^3 = \frac{1}{\frac{1}{b^3}} = \frac{1}{\left(\frac{1}{b}\right)^3} = \left(\frac{1}{b}\right)^{-3}$$

So by definition of logarithm with base $1/b$, $\log_{1/b}(y) = -3$. □

1.24 Exercise 24

If b and y are positive real numbers such that $\log_b y = 2$, what is $\log_{b^2}(y)$? Explain.

Proof. By definition of logarithm with base b, $b^2 = y$. So by definition of logarithm with base b^2, $\log_{b^2}(y) = 1$ because $(b^2)^1 = y$. □

1.25 Exercise 25

Let $A = \{2, 3, 5\}$ and $B = \{x, y\}$. Let p_1 and p_2 be the projections of $A \times B$ onto the first and second coordinates. That is, for each pair $(a, b) \in A \times B, p_1(a, b) = a$ and $p_2(a, b) = b$.

1.25.1 (a)

Find $p_1(2, y)$ and $p_1(5, x)$. What is the range of p_1?

Proof. $p_1(2, y) = 2, p_1(5, x) = 5$, range of $p_1 = \{2, 3, 5\}$ □

1.25.2 (b)

Find $p_2(2, y)$ and $p_2(5, x)$. What is the range of p_2?

Proof. $p_2(2, y) = y, p_2(5, x) = x$, range of $p_2 = \{x, y\}$ □

1.26 Exercise 26

Observe that mod and div can be defined as functions from $\mathbb{Z}^{nonneg} \times \mathbb{Z}^+$ to $\mathbb{Z}$. For each ordered pair (n, d) consisting of a nonnegative integer n and a positive integer d, let

$mod(n, d) = n \mod d$ (the nonnegative remainder obtained when n is divided by d).

$div(n, d) = n$ div d (the integer quotient obtained when n is divided by d).

Find each of the following:

1.26.1 (a)

$mod(67, 10)$ and $div(67, 10)$

Proof. $mod(67, 10) =, div(67, 10) =$ □

1.26.2 (b)

$mod(59, 8)$ and $div(59, 8)$

Proof. $mod(67, 10) = 7, div(67, 10) = 6$ □

1.26.3 (c)

$mod(30, 5)$ and $div(30, 5)$

Proof. $mod(30, 5) = 0, div(30, 5) = 6$ □

1.27 Exercise 27

Let S be the set of all strings of a's and b's.

1.27.1 (a)

Define $f : S \to \mathbb{Z}$ as follows: For each string s in S

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left most } a \text{ in } s & \text{if } s \text{ contains some } a\text{'s} \\ 0 & \text{if } s \text{ contains no } a\text{'s} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

Proof. $f(aba) = 0$ *[because there are no b's to the left of the leftmost a in aba]*

$f(bbab) = 2$ *[because there are two b's to the left of the leftmost a in bbab]*

$f(b) = 0$ *[because the string b contains no a's]*

range of $f = \mathbb{Z}^{nonneg}$ □

1.27.2 (b)

Define $g : S \to S$ as follows: For each string s in S, $g(s)$ = the string obtained by writing the characters of s in reverse order. Find $g(aba), g(bbab)$, and $g(b)$. What is the range of g?

Proof. $g(aba) = aba, g(bbab) = babb, g(b) = b$, range of $g = S$ □

1.28 Exercise 28

Consider the coding and decoding functions E and D defined in Example 7.1.9.

1.28.1 (a)

Find $E(0110)$ and $D(111111000111)$.

Proof. $E(0110) = 000111111000$ and $D(111111000111) = 1101$ □

1.28.2 (b)

Find $E(1010)$ and $D(000000111111)$.

Proof. $E(1010) = 111000111000$ and $D(000000111111) = 0011$ □

1.29 Exercise 29

Consider the Hamming distance function defined in Example 7.1.10.

1.29.1 (a)

Find $H(10101, 00011)$.

Proof. $H(10101, 00011) = 3$ □

1.29.2 (b)

Find $H(00110, 10111)$.

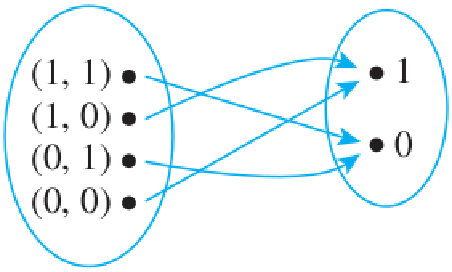
Proof. $H(00110, 10111) = 2$ □

1.30 Exercise 30

Draw arrow diagrams for the Boolean functions defined by the following input/output tables.

1.30.1 (a)

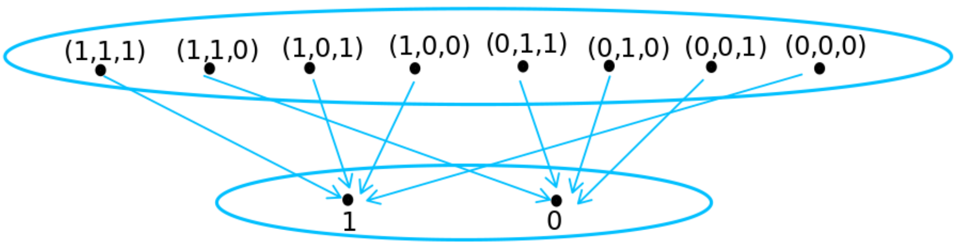
Input		Output
P	Q	R
1	1	0
1	0	1
0	1	0
0	0	1



Proof. □

1.30.2 (b)

Input			Output
P	Q	R	S
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1



Proof. □

1.31 Exercise 31

Fill in the following table to show the values of all possible two-place Boolean functions.

Proof.

Input	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1 1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1 0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0 1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0 0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

□

1.32 Exercise 32

Consider the three-place Boolean function f defined by the following rule: For each triple (x_1, x_2, x_3) of 0's and 1's,

$$f(x_1, x_2, x_3) = (4x_1 + 3x_2 + 2x_3) \mod 2.$$

1.32.1 (a)

Find $f(1,1,1)$ and $f(0,0,1)$.

Proof. $f(1,1,1) = (4 \cdot 1 + 3 \cdot 1 + 2 \cdot 1) \mod 2 = 9 \mod 2 = 1$

$f(0,0,1) = (4 \cdot 0 + 3 \cdot 0 + 2 \cdot 1) \mod 2 = 2 \mod 2 = 0$ □

1.32.2 (b)

Describe f using an input/output table.

Proof.

Input			Output
x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

□

1.33 Exercise 33

Student A tries to define a function $g : \mathbb{Q} \to \mathbb{Z}$ by the rule

$$g\left(\frac{m}{n}\right) = m - n \text{ for all integers } m \text{ and } n \text{ with } n \neq 0.$$

Student B claims that g is not well defined. Justify student B's claim.

Proof. If g were well defined, then $g(1/2) = g(2/4)$ because $1/2 = 2/4$. However, $g(1/2) = 1 - 2 = -1$ and $g(2/4) = 2 - 4 = -2$. Since $-1 \neq -2, g(1/2) \neq g(2/4)$. Thus g is not well defined. □

1.34 Exercise 34

Student C tries to define a function $h : \mathbb{Q} \to \mathbb{Q}$ by the rule

$$h\left(\frac{m}{n}\right) = \frac{m^2}{n} \text{ for all integers } m \text{ and } n \text{ with } n \neq 0.$$

Student D claims that h is not well defined. Justify student D's claim.

Proof.

$$h(2) = h\left(\frac{4}{2}\right) = \frac{4^2}{2} = 8 \neq 4 = \frac{2^2}{1} = h\left(\frac{2}{1}\right) = h(2).$$

□

1.35 Exercise 35

Let $U = \{1, 2, 3, 4\}$. Student A tries to define a function $R : U \to \mathbb{Z}$ as follows: For each $x \in U$, $R(x)$ is the integer y so that $(xy) \mod 5 = 1$. Student B claims that R is not well defined. Who is right: student A or student B? Justify your answer.

Proof. Student B is correct. If R were well defined, then $R(3)$ would have a uniquely determined value. However, on the one hand, $R(3) = 2$ because $(3 \cdot 2) \mod 5 = 1$, and, on the other hand, $R(3) = 7$ because $(3 \cdot 7) \mod 5 = 1$. Hence $R(3)$ does not have a uniquely determined value, and so R is not well defined. □

1.36 Exercise 36

Let $V = \{1, 2, 3\}$. Student C tries to define a function $S : V \to V$ as follows: For each $x \in V$, $S(x)$ is the integer y in V so that $(xy) \mod 4 = 1$. Student D claims that S is not well defined. Who is right: student C or student D? Justify your answer.

Proof. Student D is right, because $S(2)$ is not defined. $2 \cdot 1 \mod 4 = 2, 2 \cdot 2 \mod 4 = 0$, and $2 \cdot 3 \mod 4 = 2$. So when $x = 2$ there is no y in V such that $xy \mod 4 = 1$. □

1.37 Exercise 37

On certain computers the integer data type goes from -2,147,483,648 to 2,147,483,647. Let S be the set of all integers from -2,147,483,648 through 2,147,483,647. Try to define a function $f : S \to S$ by the rule $f(n) = n^2$ for each n in S. Is f well defined? Explain.

Proof. No, $2,147,483,647 = 2^{31} - 1$ so for values of n greater than, say, 2^{16}, $f(n) = n^2$ will be greater than 2^{32} which falls outside of S.

Computers handle this by using 2's complement and looping the overshoot around back to -2^{31} and onward toward the positive values again. Here is an example from Scala:

```
$ scala
// Welcome to Scala 3.3.0 (17.0.7, Java OpenJDK 64-Bit Server VM).
// Type in expressions for evaluation. Or try :help.
scala> def f(n: Int): Int = n*n
def f(n: Int): Int
scala> f(2147483647)
val res0: Int = 1
scala>
```

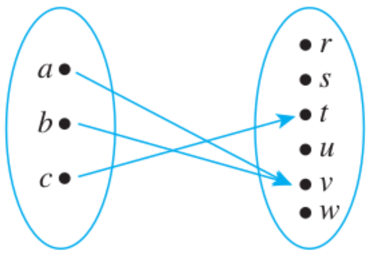
$\square$

1.38 Exercise 38

Let $X = \{a, b, c\}$ and $Y = \{r, s, t, u, v, w\}$. Define $f : X \to Y$ as follows: $f(a) = b, f(b) = v, f(c) = t$.

1.38.1 (a)

Draw an arrow diagram for f.



Proof. $\square$

1.38.2 (b)

Let $A = \{a, b\}, C = \{t\}, D = \{u, v\}, E = \{r, s\}$.

Find $f(A), f(X), f^{-1}(C), f^{-1}(D), f^{-1}(E), f^{-1}(Y)$.

Proof. $f(A) = \{v\}, f(X) = \{t, v\}, f^{-1}(C) = \{c\}, f^{-1}(D) = \{a, b\}, f^{-1}(E) = \varnothing$,

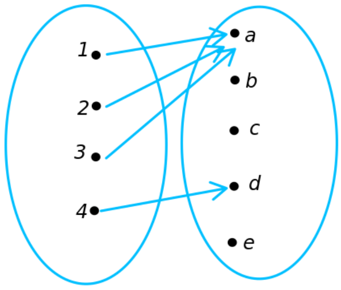
$f^{-1}(Y) = \{a, b, c\}$ $\square$

1.39 Exercise 39

Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$. Define $g : X \to Y$ as follows: $g(1) = a, g(2) = a, g(3) = a, g(4) = d$.

1.39.1 (a)

Draw an arrow diagram for g.



Proof. □

1.39.2 (b)

Let $A = \{2,3\}, C = \{a\}$, and $D = \{b,c\}$. Find $g(A), g(X), g^{-1}(C), g^{-1}(D)$, and $g^{-1}(Y)$.

Proof. $g(A) = \{a\}, g(X) = \{a,d\}, g^{-1}(C) = \{1,2,3\}, g^{-1}(D) = \varnothing, g^{-1}(Y) = \{1,2,3,4\}$. □

1.40 Exercise 40

Let X and Y be sets, let A and B be any subsets of X, and let F be a function from X to Y. Fill in the blanks in the following proof that $F(A) \cup F(B) \subseteq F(A \cup B)$.

Proof: Let y be any element in $F(A) \cup F(B)$. *[We must show that y is in $F(A \cup B)$.]* By definition of union, (i) ____ .

Case 1, $y \in F(A)$: In this case, by definition of $F(A)$, $y = F(x)$ for (ii) ____ $x \in A$. Since $A \subseteq A \cup B$, it follows from the definition of union that $x \in$ (iii) ____ . Hence, $y = F(x)$ for some $x \in A \cup B$, and thus, by definition of $F(A \cup B), y \in$ (iv) ____ .

Case 2, $y \in F(B)$: In this case, by definition of $F(B)$, (v) ____ for some $x \in B$. Since $B \subseteq A \cup B$ it follows from the definition of union that (vi) ____ . Thus $y \in F(A \cup B)$.

Therefore, regardless of whether $y \in F(A)$ or $y \in F(B)$, we have that $y \in F(A \cup B)$ *[as was to be shown]*.

Proof. (i) $y \in F(A)$ or $y \in F(B)$ (ii) some (iii) $A \cup B$ (iv) $F(A \cup B)$ (v) $y = F(x)$ (vi) $x \in A \cup B$ □

In $41 - 49$ let X and Y be sets, let A and B be any subsets of X, and let C and D be any subsets of Y. Determine which of the properties are true for every function F from X to Y and which are false for at least one function F from X to Y. Justify your answers.

1.41 Exercise 41

If $A \subseteq B$ then $F(A) \subseteq F(B)$.

Proof. Let F be a function from X to Y, and suppose $A \subseteq X, B \subseteq X$, and $A \subseteq B$. Let $y \in F(A)$. *[We must show that $y \in F(B)$.]* By definition of image of a set, $y = F(x)$ for some $x \in A$. Thus since $A \subseteq B, x \in B$, and so $y = F(x)$ for some $x \in B$. Hence $y \in F(B)$ *[as was to be shown]*. □

1.42 Exercise 42

$F(A \cap B) \subseteq F(A) \cap F(B)$

Proof. 1. Assume $y \in F(A \cap B)$. *[We want to show $y \in F(A) \cap F(B)$.]*

2. By 1 and definition of $F(A \cap B)$, $y = F(x)$ for some $x \in A \cap B$.

3. By 2 and definition of intersection, $x \in A$ and $x \in B$.

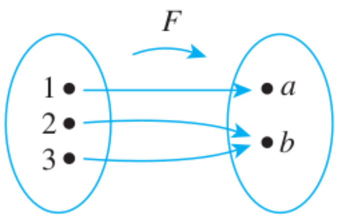
4. By 3 and definition of $F(A)$ and $F(B)$, $y = F(x)$ is in $F(A)$ and in $F(B)$.

5. By 4 and definition of intersection, $y \in F(A) \cap F(B)$.

6. By 1, 5 and definition of subset, $F(A \cap B) \subseteq F(A) \cap F(B)$. □

1.43 Exercise 43

$F(A) \cap F(B) \subseteq F(A \cap B)$



Proof. Counterexample: Let $X = \{1, 2, 3\}$, let $Y = \{a, b\}$, and define a function $F : X \to Y$ by the arrow diagram shown above.

Let $A = \{1, 2\}$ and $B = \{1, 3\}$. Then $F(A) = \{a, b\} = F(B)$, and so $F(A) \cap F(B) = \{a, b\}$. But $F(A \cap B) = F(\{1\}) = \{a\} \neq \{a, b\}$. And so $F(A) \cap F(B) \not\subseteq F(A \cap B)$. (This is just one of many possible counterexamples.) □

1.44 Exercise 44

For all subsets A and B of X, $F(A - B) = F(A) - F(B)$.

Proof. Counterexample: Let $X = \{1, 2\}, Y = \{a\}, A = \{1\}, B = \{2\}$, define $F : X \to Y$ by $F(1) = F(2) = a$. Then $A - B = \{1\}, F(A) = \{a\}, F(B) = \{a\}$. So $F(A - B) = \{a\} \neq \varnothing = F(A) - F(B)$. □

1.45 Exercise 45

For all subsets C and D of Y, if $C \subseteq D$ then $F^{-1}(C) \subseteq F^{-1}(D)$.

Proof. Let F be a function from a set X to a set Y, and suppose $C \subseteq Y, D \subseteq Y$, and $C \subseteq D$. *[We must show that $F^{-1}(C) \subseteq F^{-1}(D)$.]* Suppose $x \in F^{-1}(C)$. Then $F(x) \in C$. Since $C \subseteq D, F(x) \in D$ also. Hence, by definition of inverse image, $x \in F^{-1}(D)$. *[So $F^{-1}(C) \subseteq F^{-1}(D)$.]* □

1.46 Exercise 46

For all subsets C and D of Y, $F^{-1}(C \cup D) = F^{-1}(C) \cup F^{-1}(D)$.

Proof. 1. Assume $x \in F^{-1}(C \cup D)$ and let $y = F(x)$. *[Want to show $x \in F^{-1}(C) \cup F^{-1}(D)$.]*

2. By 1 and definition of $F^{-1}(C \cup D)$, $y \in C \cup D$.

3. By 2 and definition of union, $y \in C$ or $y \in D$.

4. **Case 1 ($\boldsymbol{y \in C}$):** By definition of $F^{-1}(C)$, $x \in F^{-1}(C)$.

By definition of union, $x \in F^{-1}(C) \cup F^{-1}(D)$.

5. **Case 2 ($\boldsymbol{y \in D}$):** By definition of $F^{-1}(D)$, $x \in F^{-1}(D)$.

By definition of union, $x \in F^{-1}(C) \cup F^{-1}(D)$.

6. By 4 and 5, $x \in F^{-1}(C) \cup F^{-1}(D)$.

7. By 1, 6 and definition of subset, $F^{-1}(C \cup D) \subseteq F^{-1}(C) \cup F^{-1}(D)$.

The proof of the reverse direction $F^{-1}(C) \cup F^{-1}(D) \subseteq F^{-1}(C \cup D)$ is similar. □

1.47 Exercise 47

For all subsets C and D of Y, $F^{-1}(C \cap D) = F^{-1}(C) \cap F^{-1}(D)$.

Proof. True, the proof is extremely similar to exercise 46. □

1.48 Exercise 48

For all subsets C and D of Y, $F^{-1}(C - D) = F^{-1}(C) - F^{-1}(D)$.

Proof. 1. Assume $x \in F^{-1}(C - D)$ and let $y = F(x)$. *[Want to show $x \in F^{-1}(C) - F^{-1}(D)$.]*

2. By 1 and definition of $F^{-1}(C - D), y \in C - D$.

3. By 2 and definition of difference, $y \in C$ and $y \notin D$.

4. By 3 and definition of $F^{-1}(C)$, $x \in F^{-1}(C)$. Similarly, since $y = F(x)$ and $y \notin D$, $x \notin F^{-1}(D)$.

5. By 4 and definition of difference, $x \in F^{-1}(C) - F^{-1}(D)$.

6. By 1, 5 and definition of subset, $F^{-1}(C - D) \subseteq F^{-1}(C) - F^{-1}(D)$.

Now the reverse part:

7. Assume $x \in F^{-1}(C) - F^{-1}(D)$ and let $y = F(x)$. *[Want to show $x \in F^{-1}(C - D)$.]*

8. By 7 and definition of difference, $x \in F^{-1}(C)$ and $x \notin F^{-1}(D)$.

9. By 8 and definition of $F^{-1}(C), y \in C$. Similarly $y \notin D$.

10. By 9 and definition of difference $y \in C - D$.

11. Since $y = F(x)$, by 10 and definition of $F^{-1}(C - D)$, $x \in F^{-1}(C - D)$.

12. By 7, 11 and definition of subset, $F^{-1}(C) - F^{-1}(D) \subseteq F^{-1}(C - D)$.

Conclusion:

13. By 6, 12 and definition of set equality $F^{-1}(C) - F^{-1}(D) = F^{-1}(C - D)$. □

1.49 Exercise 49

$F(F^{-1}(C)) \subseteq C$.

Proof. 1. Assume $y \in F(F^{-1}(C))$. *[Want to show $y \in C$.]*

2. By 1 and definition of $F(F^{-1}(C))$, there exists some $x \in F^{-1}(C)$ such that $y = F(x)$.

3. By 2 and definition of $F^{-1}(C)$, $F(x) \in C$. So $y \in C$ because $y = F(x)$.

4. By 1, 3 and definition of subset, $F(F^{-1}(C)) \subseteq C$. □

1.50 Exercise 50

Given a set S and a subset A, the characteristic function of A, denoted χ_A, is the function defined from S to $\mathbb{Z}$ with the property that for each $u \in S$,

$$\chi_A(u) = \begin{cases} 1 & \text{if } u \in A \\ 0 & \text{if } u \notin A \end{cases}$$

Show that each of the following holds for all subsets A and B of S and every $u \in S$.

1.50.1 (a)

$\chi_{A \cap B}(u) = \chi_A(u) \cdot \chi_B(u)$

Proof. Assume A, B are any subsets of S and u is any element in S. There are 4 cases:

Case 1 ($\boldsymbol{u \in A, u \in B}$): Then $\chi_A(u) = 1$ and $\chi_B(u) = 1$.

By definition of intersection $u \in A \cap B$. Thus $\chi_{A \cap B}(u) = 1$ also. Since $1 = 1 \cdot 1$, $\chi_{A \cap B}(u) = \chi_A(u) \cdot \chi_B(u)$.

Case 2 ($\boldsymbol{u \in A, u \notin B}$): Then $\chi_A(u) = 1$ and $\chi_B(u) = 0$.

By definition of intersection $u \notin A \cap B$. Thus $\chi_{A\cap B}(u) = 0$ also. Since $0 = 1 \cdot 0$, $\chi_{A\cap B}(u) = \chi_A(u) \cdot \chi_B(u)$.

Case 3 ($\boldsymbol{u \notin A, u \in B}$): Then $\chi_A(u) = 0$ and $\chi_B(u) = 1$.

By definition of intersection $u \notin A \cap B$. Thus $\chi_{A\cap B}(u) = 0$ also. Since $0 = 0 \cdot 1$, $\chi_{A\cap B}(u) = \chi_A(u) \cdot \chi_B(u)$.

Case 4 ($\boldsymbol{u \notin A, u \notin B}$): Then $\chi_A(u) = 0$ and $\chi_B(u) = 0$.

By definition of intersection $u \notin A \cap B$. Thus $\chi_{A\cap B}(u) = 0$ also. Since $0 = 0 \cdot 0$, $\chi_{A\cap B}(u) = \chi_A(u) \cdot \chi_B(u)$. $\square$

1.50.2 (b)

$\chi_{A\cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$

Proof. Assume A, B are any subsets of S and u is any element in S. There are 4 cases:

Case 1 ($\boldsymbol{u \in A, u \in B}$): Then $\chi_A(u) = 1$ and $\chi_B(u) = 1$.

By definition of union $u \in A \cup B$. Thus $\chi_{A\cup B}(u) = 1$ also. Since $1 = 1 + 1 - (1 \cdot 1)$, $\chi_{A\cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$.

Case 2 ($\boldsymbol{u \in A, u \notin B}$): Then $\chi_A(u) = 1$ and $\chi_B(u) = 0$.

By definition of union $u \in A \cup B$. Thus $\chi_{A\cup B}(u) = 1$ also. Since $1 = 1 + 0 - (1 \cdot 0)$, $\chi_{A\cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$.

Case 3 ($\boldsymbol{u \notin A, u \in B}$): Then $\chi_A(u) = 0$ and $\chi_B(u) = 1$.

By definition of union $u \in A \cup B$. Thus $\chi_{A\cup B}(u) = 1$ also. Since $1 = 0 + 1 - (0 \cdot 1)$, $\chi_{A\cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$.

Case 4 ($\boldsymbol{u \notin A, u \notin B}$): Then $\chi_A(u) = 0$ and $\chi_B(u) = 0$.

By definition of union $u \notin A \cup B$. Thus $\chi_{A\cup B}(u) = 0$ also. Since $0 = 0 + 0 - (0 \cdot 0)$, $\chi_{A\cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$. $\square$

Each of exercises $51 - 53$ refers to the Euler phi function, denoted ϕ, which is defined as follows: For each integer $n \geq 1$, $\phi(n)$ is the number of positive integers less than or equal to n that have no common factors with n except ± 1. For example, $\phi(10) = 4$ because there are four positive integers less than or equal to 10 that have no common factors with 10 except ± 1, namely, 1, 3, 7, and 9.

1.51 Exercise 51

Find each of the following:

1.51.1 (a)

$\phi(15)$

Proof. $\phi(15) = 8$ *[because* $1, 2, 4, 7, 8, 11, 13,$ *and* 14 *have no common factors with* 15 *other than* ± 1*]* ☐

1.51.2 (b)

$\phi(2)$

Proof. $\phi(2) = 1$ *[because the only positive integer less than or equal to* 2 *having no common factors with* 2 *other than* ± 1 *is* 1*]* ☐

1.51.3 (c)

$\phi(5)$

Proof. $\phi(5) = 4$ *[because* $1, 2, 3,$ *and* 4 *have no common factors with* 5 *other than* ± 1*]* ☐

1.51.4 (d)

$\phi(12)$

Proof. $\phi(12) = 4$ (1, 5, 7, 11) ☐

1.51.5 (e)

$\phi(11)$

Proof. $\phi(11) = 10$ (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) ☐

1.51.6 (f)

$\phi(1)$

Proof. $\phi(1) = 1$ ☐

1.52 Exercise 52

Prove that if p is a prime number and n is an integer with $n \geq 1$, then $\phi(p^n) = p^n - p^{n-1}$.

Proof. Let p be any prime number and n any integer with $n \geq 1$. There are p^{n-1} positive integers less than or equal to p^n that have a common factor other than ± 1 with p^n, namely, $p, 2p, 3p, \ldots, (p^{n-1})p$. Hence, there are $p^n - p^{n-1}$ positive integers less than or equal to p^n that do not have a common factor with p^n except for ± 1. ☐

1.53 Exercise 53

Prove that there are infinitely many integers n for which $\phi(n)$ is a perfect square.

Proof. By exercise 52, for any integer n with $n \geq 1, \phi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$.

So, for all integers k with $k \geq 1$, we have that $\phi(2^{2k+1}) = 2^{2k} = (2^k)^2$ is a perfect square. □

2 Exercise Set 7.2

2.1 Exercise 1

Proof. □

2.2 Exercise 2

Proof. □

2.3 Exercise 3

Proof. □

2.4 Exercise 4

Proof. □

2.5 Exercise 5

Proof. □

2.6 Exercise 6

Proof. □

2.7 Exercise 7

Proof. □

2.8 Exercise 8

Proof. □

2.9 Exercise 9

Proof. □

2.10 Exercise 10

Proof. □

2.11 Exercise 11

Proof. □

2.12 Exercise 12

Proof. □

2.13 Exercise 13

Proof. □

2.14 Exercise 14

Proof. □

2.15 Exercise 15

Proof. □

2.16 Exercise 16

Proof. □

2.17 Exercise 17

Proof. □

2.18 Exercise 18

Proof. □

2.19 Exercise 19

Proof. □

2.20 Exercise 20

Proof. □

2.21 Exercise 21

Proof. □

2.22 Exercise 22

Proof. □

2.23 Exercise 23

Proof. □

2.24 Exercise 24

Proof. □

2.25 Exercise 25

Proof. □

2.26 Exercise 26

Proof. □

2.27 Exercise 27

Proof. □

2.28 Exercise 28

Proof. □

2.29 Exercise 29

Proof. □

2.30 Exercise 30

Proof. □

2.31 Exercise 31

Proof. □

2.32 Exercise 32

Proof. □

2.33 Exercise 33

Proof. □

2.34 Exercise 34

Proof. ☐

2.35 Exercise 35

Proof. ☐

2.36 Exercise 36

Proof. ☐

2.37 Exercise 37

Proof. ☐

2.38 Exercise 38

Proof. ☐

2.39 Exercise 39

Proof. ☐

2.40 Exercise 40

Proof. ☐

2.41 Exercise 41

Proof. ☐

2.42 Exercise 42

Proof. ☐

2.43 Exercise 43

Proof. ☐

2.44 Exercise 44

Proof. ☐

2.45 Exercise 45

Proof. ☐

2.46 Exercise 46

Proof. □

2.47 Exercise 47

Proof. □

2.48 Exercise 48

Proof. □

2.49 Exercise 49

Proof. □

2.50 Exercise 50

Proof. □

2.51 Exercise 51

Proof. □

2.52 Exercise 52

Proof. □

2.53 Exercise 53

Proof. □

2.54 Exercise 54

Proof. □

2.55 Exercise 55

Proof. □

2.56 Exercise 56

Proof. □

2.57 Exercise 57

Proof. □

2.58 Exercise 58

Proof. ∎