

Solutions:
A Book of Abstract Algebra (2e)
by Charles C. Pinter

Mark Watson

July 3, 2018

Many of these solutions are incorrect. Please let me know if you find an error!

Chapter 2 Operations

A. Examples of Operations

1.

$$a * b = \sqrt{|ab|}, \text{ on the set } \mathbb{Q}$$

This is not an operation because many roots are irrational

2.

$$a * b = \ln b, \text{ on the set } \{x \in \mathbb{R} : x > 0\}$$

This is an operation

3.

$$a * b \text{ is a root of the equation } x^2 - a^2b^2 = 0, \text{ on the set } \mathbb{R}$$

This is not an operation because it is not uniquely defined for any $a \neq 0$
 $b \neq 0$ because $x = a * b = \pm ab$

4.

Subtraction, on the set \mathbb{Z}

This is an operation.

5.

Subtraction, on the set $\{n \in \mathbb{Z} \geq 0\}$

This is not an operation when $a - b \leq 0$

6.

$a * b = |a - b|$, on the set $\{n \in \mathbb{Z} \geq 0\}$

This is an operation

B. Properties of Operations

1.

$$x * y = x + 2y + 4$$

i $y * x = y + 2x + 4 \neq x + 2y + 4$

Not commutative

ii $x * (y * z) = x(y + 2z + 4) = xy + 2xz + 4x \neq$
 $(x * y) * z = (x + 2y + 4)z = xz + 2yz + 4z$

Not associative

iii $x * e = x$ for $e : x * e = x + 2e + 4 = x$; therefore $e = 2 \neq$
 $e * y = y$ for $e : e * y = e + 2y + 4 = y$; therefore $e = -y - 4$

Identity does not exist

iiii Inverse can't exist without an identity

2.

$$x * y = x + 2y - xy$$

i $y * x = y + 2x - yx \neq x + 2y - xy = x * y$

Not commutative

ii $x * (y * z) = x * (y + 2z - yz) = x + 2(y + 2z - yz) - x(y + 2z - yz) =$
 $x + 2y + 4z - 2yz - xy - 2xz + xyz \neq$
 $(x * y) * z = (x + 2y - xy) * z = (x + 2y - xy) + 2z - (x + 2y - xy)z =$
 $x + 2y - xy + 2z - xz - 2yz + xyz$

Not associative

iii $x * e = x + 2e - xe = x$, therefore $e = 0$

$e * y = e + 2y - ey = y$, therefore $e = \frac{-y}{1-y}$

No identity

iiii No inverse

3.

$$x * y = |x + y|$$

i $y * x = |y + x| = |x + y| = x + y$

Commutative

ii $x * (y * z) = x * |y + z| = |x + |y + z|| =$
 $(x * y) * z = |x + y| * z = ||x + y| + z|$

Not associative (for example let $x = 2, y = -3, z = 5$)

iii $x * e = |x + e| = x$

No identity

iiii No inverse

4.

$$x * y = |x - y|$$

i $y * x = |y - x| = |x - y| = x * y$

Commutative

ii $x * (y * z) = x * |y - z| = |x - |y - z||$
 $(x * y) * z = |x - y| * z = ||x - y| - z|$

Not associative (for example let $x = 2, y = -3, z = 5$)

iii $x * e = |x - e| = x$

No identity

iiii No inverse

5.

$$x * y = xy + 1$$

i $y * x = yx + 1 = xy + 1 = x * y$

Commutative

ii $x * (y * z) = x * (yz + 1) = x(yz + 1) + 1 = xyz + x + 1 \neq$
 $(x * y) * z = (xy + 1) * z = (xy + 1)z + 1 = xyz + z + 1$

Not associative

iii $x * e = xe + 1 = x$, therefore $e = \frac{x-1}{x}$

No identity

iiii No inverse

6.

$$x * y = \max\{x, y\}$$

i $y * x = \max\{y, x\} = \max\{x, y\} = x * y$
Commutative

ii $x * (y * z) = x * \max\{y, z\} = \max\{x, \max\{y, z\}\} = \max\{x, y, z\} =$
 $(x * y) * z = \max\{x, y\} * z = \max\{\max\{x, y\}, z\} = \max\{x, y, z\}$
Associative

iii $x * e = \max\{x, e\} = x$, therefore $e = -\infty$
No identity

iiii No inverse

7.

$$x * y = \frac{xy}{x + y + 1} \text{ (on the set of positive real numbers)}$$

i $y * x = \frac{yx}{y+x+1} = \frac{xy}{x+y+1} = x * y$
Commutative

ii

$$x * (y * z) = x * \frac{yz}{y + z + 1} = \frac{x \frac{yz}{y+z+1}}{x + \frac{yz}{y+z+1} + 1} = \frac{xyz}{1 + x + y + z + xy + xz + yz} =$$

$$(x * y) * z = \frac{xy}{x + y + 1} * z = \frac{\frac{xy}{x+y+1} z}{\frac{xy}{x+y+1} + z + 1} = \frac{xyz}{1 + x + y + z + xy + xz + yz}$$

Associative

iii $x * e = \frac{xe}{x+e+1} = x$, therefore $x = -1$
No identity

iiii No inverse

C. Operations on a Two-Element Set

1		2		3	
(x,y)	x*y	(x,y)	x*y	(x,y)	x*y
(a,a)	a	(a,a)	a	(a,a)	a
(a,b)	a	(a,b)	a	(a,b)	a
(b,b)	a	(b,b)	a	(b,b)	b
(b,a)	a	(b,a)	b	(b,a)	b

4		5		6	
(x,y)	x*y	(x,y)	x*y	(x,y)	x*y
(a,a)	a	(a,a)	a	(a,a)	a
(a,b)	a	(a,b)	b	(a,b)	b
(b,b)	b	(b,b)	b	(b,b)	b
(b,a)	a	(b,a)	a	(b,a)	b

7		8		9	
(x,y)	x*y	(x,y)	x*y	(x,y)	x*y
(a,a)	a	(a,a)	a	(a,a)	b
(a,b)	b	(a,b)	b	(a,b)	b
(b,b)	a	(b,b)	a	(b,b)	a
(b,a)	b	(b,a)	a	(b,a)	a

10		11		12	
(x,y)	x*y	(x,y)	x*y	(x,y)	x*y
(a,a)	b	(a,a)	b	(a,a)	b
(a,b)	b	(a,b)	b	(a,b)	b
(b,b)	a	(b,b)	b	(b,b)	b
(b,a)	b	(b,a)	b	(b,a)	a

13		14		15	
(x,y)	x*y	(x,y)	x*y	(x,y)	x*y
(a,a)	b	(a,a)	b	(a,a)	b
(a,b)	a	(a,b)	a	(a,b)	a
(b,b)	b	(b,b)	b	(b,b)	a
(b,a)	a	(b,a)	b	(b,a)	b

16	
(x,y)	x*y
(a,a)	b
(a,b)	a
(b,b)	a
(b,a)	a

- 1.
2. Commutative: 1, 4, 6, 7, 10, 11, 13, 16
For all of these $(a, b) = (b, a)$

3. Associative: 1, 3, 4, 5, 6, 7, 11, 13

I used the following Clojure code to solve:

```
(def tables
  (for [aa ['a 'b]
        ab ['a 'b]
        bb ['a 'b]
        ba ['a 'b]]
    {[ 'a 'a] aa
     [ 'a 'b] ab
     [ 'b 'b] bb
     [ 'b 'a] ba}))

(defn assoc?
  [table]
  (every? identity
    (for [x ['a 'b]
          y ['a 'b]
          z ['a 'b]]
      (= (table [(table [x y]) z])
         (table [x (table [y z])])))))

(->> tables
  (map (fn [table] [table (assoc? table)]))
  (filter second))
```

2. Have identity: 4, 6, 7, 13

I used the following Clojure code to solve:

$$((a, a) = a \cap (a, b) = b \cap (b, a) = b) \cup ((b, b) = b \cap (a, b) = a \cap (b, a) = a)$$

```
(for [aa ['a 'b]
      ab ['a 'b]
      bb ['a 'b]
      ba ['a 'b]
      :when (or (and (= aa 'a)
                      (= ab 'b))
                 (and (= aa 'b)
                      (= ab 'a)))]
  [aa ab bb ba])
```

```

                                (= ba 'b))
      (and (= bb 'b)
            (= ab 'a)
            (= ba 'a))))]
  {[ 'a 'a] aa
    [ 'a 'b] ab
    [ 'b 'b] bb
    [ 'b 'a] ba})

```

2. Have inverse: 7 and 13
 4 has identity b : there exists no x where $a * x = b$
 6 has identity a : there exists no x where $b * x = a$
 7 has identity b : $a * b = b = e$ and $b * a = b = e$
 13 has identity a : $a * b = a = e$ and $b * a = a = e$

D. Automata: The Algebra of Input/Output Sequences

1. Let $\mathbf{a} = a_1..a_n$, $\mathbf{b} = b_1..b_m$, $\mathbf{c} = c_1..c_k$
 $\mathbf{a} * (\mathbf{b} * \mathbf{c}) = \mathbf{a} * (b_1..b_m c_1..c_k) = a_1..a_n b_1..b_m c_1..c_k$
 $(\mathbf{a} * \mathbf{b}) * \mathbf{c} = (a_1..a_n b_1..b_m) * \mathbf{c} = a_1..a_n b_1..b_m c_1..c_k$
2. Concatenation is not commutative because placing elements on to the beginning versus the end of a sequence leads to different sequences.
3. Let $\mathbf{a} = a_1..a_n$
 $\mathbf{a}\lambda = \lambda\mathbf{a} = \mathbf{a}$

Chapter 3 The Definition of Groups

A. Examples of Abelian Groups

1. $x * y = x + y + k$ (k is a fixed constant), on the set \mathbb{R}

- i $y * x = y + x + k = x + y + k = x * y$
Commutative
- ii $x * (y * z) = x * (y + z + k) = x + (y + z + k) + k = x + y + z + 2k =$
 $(x * y) * z = (x + y + k) * z = (x + y + k) + z + k = x + y + z + 2k$
Associative
- iii $x * e = x + e + k = x$, therefore $e = -k$
 $e * y = e + y + k = y$, therefore $e = -k$
Identity is $-k$
- iiii $x * a = x + a + k = e = -k$, therefore $a = -x - 2k$
 $a * x = a + x + k = e = -k$, therefore $a = -x - 2k$
Inverse is $-x - 2k$

2.

$$x * y = \frac{xy}{2}, \text{ on the set } \{x \in \mathbb{R} : x \neq 0\}$$

- i $y * x = \frac{yx}{2} = \frac{xy}{2} = x * y$
Commutative
- ii $x * (y * z) = x * \frac{yz}{2} = \frac{x \frac{yz}{2}}{2} = \frac{xyz}{4} =$
 $(x * y) * z = \frac{xy}{2} * z = \frac{\frac{xy}{2} z}{2} = \frac{xyz}{4}$
Associative
- iii $x * e = \frac{xe}{2} = x$, therefore $e = 2$
 $e * y = \frac{ey}{2} = x$, therefore $e = 2$
Identity is 2
- iiii $x * a = \frac{xa}{2} = e = 2$, therefore $a = \frac{4}{x}$
 $a * x = \frac{ax}{2} = e = 2$, therefore $a = \frac{4}{x}$
Inverse is $\frac{4}{x}$

3.

$$x * y = x + y + xy, \text{ on the set } \{x \in \mathbb{R} : x \neq -1\}$$

- i $y * x = y + x + yx = x + y + xy = x * y$ Commutative
- ii $x * (y * z) = x * (y + z + yz) = x + (y + z + yz) + x(y + z + yz) =$
 $x + y + z + xy + xz + yz + xyz =$
 $(x * y) * z = (x + y + xy) * z = (x + y + xy) + z + (x + y + xy)z =$
 $x + y + z + xy + xz + yz + xyz$
Associative

- iii $x * e = x + e + xe = x$, therefore $e = 0$
 $e * y = e + y + ey = y$, therefore $e = 0$
 Identity is 0
- iiii $x * a = x + a + xa = e = 0$, therefore $a = \frac{-x}{1+x}$
 $a * x = a + x + ax = \frac{-x}{1+x} + x + \frac{-x}{1+x}x = 0 = 3$
 Inverse is $\frac{-x}{1+x}$

4.

$$x * y = \frac{x+y}{xy+1}, \text{ on the set } \{x \in \mathbb{R} : -1 < x < 1\}$$

- i $y * x = \frac{y+x}{yx+1} = \frac{x+y}{xy+1} = x * y$
 Commutative
- ii $x * (y * z) = x * \frac{y+z}{yz+1} = \frac{x + \frac{y+z}{yz+1}}{x \frac{y+z}{yz+1} + 1} = \frac{xyz+x+y+z}{xy+xz+yz+1} =$
 $(x * y) * z = \frac{x+y}{xy+1} * z = \frac{\frac{x+y}{xy+1} + z}{\frac{x+y}{xy+1}z + 1} = \frac{xyz+x+y+z}{xy+xz+yz+1}$
 Associative
- iii $x * e = \frac{x+e}{xe+1} = x$, therefore $e = 0$
 $e * y = \frac{e+y}{ey+1} = y$, therefore $e = 0$
 Identity is 0
- iiii $x * a = \frac{x+a}{xa+1} = e = 0$, therefore $a = -x$
 $a * x = \frac{a+x}{ax+1} = \frac{-x+x}{-x^2+1} = 0$
 Inverse is $-x$

B. Groups on the Set $\mathbb{R} \times \mathbb{R}$

1.

$$(a, b) * (c, d) = (ad + bc, bd), \text{ on the set } \{(x, y) \in \mathbb{R} \times \mathbb{R} : y \neq 0\}$$

- i $(c, d) * (a, b) = (cb + da, db) = (ad + bc, bd) = (a, b) * (c, d)$
 Commutative
- ii $(a, b) * ((c, d) * (e, f)) = (a, b) * (cf + de, df) = (adf + b(cf + de), bdf) = (adf + bcf + bde, bdf) =$
 $((a, b) * (c, d)) * (e, f) = (ad + bc, bd) * (e, f) = ((ad + bc)f + bde, bdf) = (adf + bcf + bde, bdf)$
 Associative

- iii $(a, b) * (e_1, e_2) = (ae_2 + be_1, be_2) = (a, b)$, therefore $(e_1, e_2) = (0, 1)$
 $(e_1, e_2) * (a, b) = (e_1b + e_2a, e_2b) = (a, b)$, therefore $(e_1, e_2) = (0, 1)$
Identity is $(0, 1)$
- iiii $(a, b) * (a', b') = (ab' + ba', bb') = (0, 1)$, therefore $(a', b') = (\frac{-a}{b^2}, \frac{1}{b})$
 $(a', b') * (a, b) = (a'b + b'a, b'b) = (0, 1)$, therefore $(a', b') = (\frac{-a}{b^2}, \frac{1}{b})$
Inverse is $(\frac{-a}{b^2}, \frac{1}{b})$

2.

$(a, b) * (c, d) = (ac, bc + d)$, on the set $\{(x, y) \in \mathbb{R}x\mathbb{R} : x \neq 0\}$

- i $(c, d) * (a, b) = (ca, da + b) \neq (ac, bc + d) = (a, b) * (c, d)$
Not commutative
- ii $(a, b) * ((c, d) * (e, f)) = (a, b) * (ce, de + f) = (ace, bce + de + f) =$
 $((a, b) * (c, d)) * (e, f) = (ac, bc + d) * (e, f) = (ace, (bc + d)e + f)$
Associative
- iii $(a, b) * (e_1, e_2) = (ae_1, be_1 + e_2) = (a, b)$, therefore $(e_1, e_2) = (1, 0)$
 $(e_1, e_2) * (a, b) = (e_1a, e_2a + b) = (a, b)$, therefore $(e_1, e_2) = (1, 0)$
Identity is $(1, 0)$
- iiii $(a, b) * (a', b') = (aa', ba' + b') = (1, 0)$, therefore $(a', b') = (\frac{1}{a}, \frac{-b}{b})$
 $(a', b') * (a, b) = (a'a, b'a + b) = (1, 0)$, therefore $(a', b') = (\frac{1}{a}, \frac{-b}{b})$
Inverse is $(\frac{1}{a}, \frac{-b}{b})$
A (non-Abelian) group

3.

$(a, b) * (c, d) = (ac, bc + d)$, on the set $\{(x, y) \in \mathbb{R}x\mathbb{R}\}$

- i $(c, d) * (a, b) = (ca, da + b) \neq (ac, bc + d) = (a, b) * (c, d)$
Not commutative
- ii $(a, b) * ((c, d) * (e, f)) = (a, b) * (ce, de + f) = (ace, bce + de + f) =$
 $((a, b) * (c, d)) * (e, f) = (ac, bc + d) * (e, f) = (ace, (bc + d)e + f)$
Associative
- iii $(a, b) * (e_1, e_2) = (ae_1, be_1 + e_2) = (a, b)$, therefore $e_1 = \frac{a}{a}$
Since we can't divide by 0, there is no general identity
- iiii No inverse without an identity element

4.

$(a, b) * (c, d) = (ac - bd, ad + bc)$, on the set $\mathbb{R} \times \mathbb{R}$ with the origin removed

$$\text{i } (c, d) * (a, b) = (ca - db, cb + da) = (ac - bd, ad + bc) = (a, b) * (c, d)$$

Commutative

$$\begin{aligned} \text{ii } (a, b) * ((c, d) * (e, f)) &= (a, b) * (ce - df, cf + de) \\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) = \\ &= ((a, b) * (c, d)) * (e, f) = (ac - bd, ad + bc) * (e, f) \\ &= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e) \\ &= (ace - bde - adf - bcf, acf - bcf + ade + bce) = \end{aligned}$$

Associative

$$\text{iii } (a, b) * (e_1, e_2) = (ae_1 - be_2, ae_2 + be_1) = (a, b), \text{ therefore } (e_1, e_2) = (1, 0)$$

Identity is $(1, 0)$

$$\begin{aligned} \text{iiii } (a, b) * (a', b') &= (aa' - bb', ab' + ba') = (1, 0), \text{ therefore } (a', b') = \\ &= \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \\ (a', b') * (a, b) &= (a, b) * (a', b') \text{ commutativity} \\ \text{Inverse is } &\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) \end{aligned}$$

5. The previous operation on the set $\mathbb{R} \times \mathbb{R}$ is not a group because there is no identity or inverse for $(0, 0)$, we'd have to divide by 0

C. Groups of Subsets of a Set

$$1 \ A + \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$$

$$\emptyset + B = (\emptyset - B) \cup (B - \emptyset) = \emptyset \cup B = B$$

Identity element = \emptyset (the empty set)

$$2 \ A + A^{-1} = (A - A^{-1}) \cup (A^{-1} - A) = \emptyset \cup \emptyset$$

$$\text{so } A - A^{-1} = \emptyset, \ A^{-1} - A = \emptyset$$

$$\text{and } A = A^{-1}$$

3

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

D. A Checkerboard Game

*	I	V	H	D
I	I	V	H	D
V	V	I	D	H
H	H	D	I	V
D	D	H	V	I

E. A Coin Game

*	I	M1	M2	M3	M4	M5	M6	M7
I	I	M1	M2	M3	M4	M5	M6	M7
M1	M1	I	M3	M2	M5	M4	M7	M6
M2	M2	M3	I	M1	M6	M7	M4	M5
M3	M3	M2	M1	I	M7	M6	M5	M4
M4	M4	M6	M5	M7	I	M2	M1	M3
M5	M5	M7	M4	M6	M1	M3	I	M2
M6	M6	M4	M7	M5	M2	I	M3	M1
M7	M7	M6	M6	M4	M3	M3	M2	I

$\langle G, * \rangle$ is a group because it has an identity element I and for every value there is an inverse.

It is not commutative, you can tell because the top right and bottom left of the operation table are not transposes of each other. For example, $M_7 * M_6 = M_2$ but $M_6 * M_7 = M_1$

F. Groups in Binary Codes

1 $a_n + b_n = b_n + a_n$ for every n

2 $1 + (0 + 1) = 1 + 1 = (1 + 0) + 1$
 $1 + (0 + 0) = 1 = (1 + 0) + 0$
 $0 + (1 + 1) = 0 + 0 = 0 = 1 + 1 = (0 + 1) + 1$
 $0 + (1 + 0) = 1 = (0 + 1) + 1$
 $0 + (0 + 1) = 1 = (0 + 0) + 1$
 $0 + (0 + 0) = 0 = (0 + 0) + 0$

3 $(a_1, \dots, a_n) + [(b_1, \dots, b_n) + (c_1, \dots, c_n)]$
 $= (a_1, \dots, a_n) + [(b_1 + c_1), \dots, (b_n + c_n)]$
 $= (a_1 + b_1 + c_1), \dots, (a_n + b_n + c_n)$
 $= [(a_1 + b_1), \dots, (a_n + b_n)] + (c_1, \dots, c_n)$
 $= [(a_1, \dots, a_n) + (b_1, \dots, b_n)] + (c_1, \dots, c_n)$

4 The identity is 0^n , that is a word of length n where each element is 0. This way each element remains unchanged, as does the entire word.

5 The inverse of any element is itself. With no differences between the operands, the result of the operation is 0^n

6 $0 + 0 = 0 = 0 - 0$
 $1 + 0 = 1 = 1 - 0$
 $0 + 1 = 1 = 0 - 1$
 $1 + 1 = 0 = 1 - 1$
 $a_n + b_n = a_n - b_n$

7 $1 + 1 = 0, 1 = 1 + 0$
 $1 + 0 = 1, 1 = 0 + 1$
 $0 + 1 = 1, 0 = 1 + 1$
 $0 + 0 = 0, 0 = 0 + 0$

G. Theory of Coding: Maximum-Likelihood Decoding

$$\begin{aligned}
 1 \quad & a_4 = a_1 + a_3, a_5 = a_1 + a_2 + a_3 \\
 & 000 \rightarrow a_4 = 0 + 0 = 0, a_5 = 0 + 0 + 0 = 0 \\
 & 001 \rightarrow a_4 = 0 + 1 = 1, a_5 = 0 + 0 + 1 = 1 \\
 & 010 \rightarrow a_4 = 0 + 0 = 0, a_5 = 0 + 1 + 0 = 1 \\
 & 011 \rightarrow a_4 = 0 + 1 = 1, a_5 = 0 + 1 + 1 = 0 \\
 & 100 \rightarrow a_4 = 1 + 0 = 1, a_5 = 1 + 0 + 0 = 1 \\
 & 101 \rightarrow a_4 = 1 + 1 = 0, a_5 = 1 + 0 + 1 = 0 \\
 & 110 \rightarrow a_4 = 1 + 0 = 1, a_5 = 1 + 1 + 0 = 0 \\
 & 111 \rightarrow a_4 = 1 + 1 = 0, a_5 = 1 + 1 + 1 = 1
 \end{aligned}$$

$$\begin{aligned}
 2 \quad & \text{a } 000000 \\
 & \quad 001001 \\
 & \quad 010111 \\
 & \quad 011110 \\
 & \quad 100011 \\
 & \quad 101010 \\
 & \quad 110100 \\
 & \quad 111101
 \end{aligned}$$

b The minimum distance of C_2 is 2.
For example, $110100 + 111101 = 001001$.

c One error is sure to be detected. Two (or more) errors could lead to another code word.

$$\begin{aligned}
 3 \quad & 0000 \\
 & 1001 \\
 & 1110 \\
 & 0111
 \end{aligned}$$

$$\begin{aligned}
 x[0] &= x[2] \\
 x[1] &= x[2] + x[3]
 \end{aligned}$$

Minimum distance = 2

4 11111 \rightarrow 11101
 00101 \rightarrow 00111
 11000 \rightarrow 11010
 10011 \rightarrow 10011
 10001 \rightarrow 10011
 10111 \rightarrow equidistant from 00111 and 10011

5 Every word will always differ in m bits, so it would take at least m bits to change one code word to another. Therefore, any number of bits smaller than m cannot change a code word into another code word. If a code word has been changed and the result isn't another code word, we can easily detect this.

6 Let's say x is less than $\frac{1}{2}(m-1)$ from both a and b .
 Then, the distance from a to b must be at most the distance from x to a plus the distance from x to b :

$$\overline{ab} \leq \overline{xa} + \overline{xb}$$

Plugging in for the distances from x to a and b :

$$\overline{ab} \leq \frac{1}{2}(m-1) + \frac{1}{2}(m-1) = (m-1)$$

Also, because both are code words we know a and a are at least m distance apart:

$$\overline{ab} > m$$

The distance from a to b can't satisfy both equations simultaneously:

$$\overline{ab} \leq (m-1) \text{ and } \overline{ab} > m$$

7 The above shows that any word x can only belong to one sphere (associated with the closest code word).

8 This claim is not true.

$$t = \frac{1}{2}(m-1) = \frac{1}{2} < 1$$

Therefore, there exist some words that cannot be corrected because they are a distance of 1 from multiple code words.