Section 6.4

Sterling Jeppson

January 10, 2021

In 1-3 assume that B is a Boolean algebra with operations $+$ and $\cdot$. Give the reasons needed to fill in the blanks of the proofs, but do not use any parts of theorem 6.4.1 unless they have already been proved. You may use any part of the definition of a Boolean algebra and the results of previous exercises, however.

Problem 1 and Solution

For all a in B, $a \cdot a = a$.

Proof. Let a be any element of B. Then

$$\begin{aligned} a &= a \cdot 1 && \text{because 1 is an identity for } \cdot \\ &= a \cdot (a + \overline{a}) && \text{by the complement law for } + \\ &= (a \cdot a) + (a \cdot \overline{a}) && \text{by the distributive law for } \cdot \text{ over } + \\ &= (a \cdot a) + 0 && \text{by the complement law for } \cdot \\ &= a \cdot a && \text{because 0 is an identity for } + \end{aligned}$$

□

Problem 2 and Solution

For all a in B, $a + 1 = 1$.

Proof. Let a be any element of B. Then

$$\begin{aligned} a + 1 &= a + (a + \overline{a}) && \text{by the complement law for } + \\ &= (a + a) + \overline{a} && \text{by the associative law for } + \\ &= a + \overline{a} && \text{by example 6.4.2} \\ &= 1 && \text{by the complement law for } + \end{aligned}$$

□

Problem 3 and Solution

For all a and b in B, $(a + b) \cdot a = a$.

Proof. Let a and b be any element of B. Then

$$
\begin{aligned}
(a+b)\cdot a &= a\cdot(a+b) && \text{by the commutative law for } \cdot\\
&= a\cdot a + a\cdot b && \text{by the distributive law for } \cdot \text{ over } +\\
&= a + a\cdot b && \text{by exercise 1}\\
&= a\cdot 1 + a\cdot b && \text{because 1 is an identity for } \cdot\\
&= a\cdot(1+b) && \text{by the distributive law for } \cdot \text{ over } +\\
&= a\cdot(b+1) && \text{by commutative law for } +\\
&= a\cdot 1 && \text{by exercise 2}\\
&= a && \text{because 1 is an identity for } \cdot \qquad \square
\end{aligned}
$$

In 4-10 assume that B is a Boolean algebra with operations $+$ and $\cdot$. Prove each statement without using any parts of theorem 6.4.1 unless they have already been proved. You may use any part of the definition of a Boolean algebra and the results of previous exercises, however.

Problem 4 and Solution

For all a in B, $a \cdot 0 = 0$.

Proof. Let a be any element of B. Then

$$
\begin{aligned}
a\cdot 0 &= a\cdot(a\cdot\overline{a}) && \text{by the complement law for } \cdot\\
&= (a\cdot a)\cdot\overline{a} && \text{by the associative law for } \cdot\\
&= a\cdot\overline{a} && \text{by exercise 1}\\
&= 0 && \text{by the complement law for } \cdot \qquad \square
\end{aligned}
$$

Problem 5 and Solution

For all a and b in B, $(a \cdot b) + a = a$.

Proof. Let a and b be any elements of B. Then

$$
\begin{aligned}
(a\cdot b)+a &= a+(a\cdot b) && \text{by the commutative law for } +\\
&= a+(a\cdot(b+0)) && \text{by the complement law for } +\\
&= a+((a\cdot b)+(a\cdot 0)) && \text{by the distributive law for } \cdot \text{ over } +\\
&= a+((a\cdot b)+0) && \text{by exercise 4}\\
&= (a+(a\cdot b))+0 && \text{by the associative law for } +\\
&= ((a\cdot 1)+(a\cdot b))+0 && \text{because 1 is an identity for } \cdot\\
&= (a\cdot(1+b))+0 && \text{by the distributive law for } \cdot \text{ over } +\\
&= (a\cdot(b+1))+0 && \text{by the commutative law for } +\\
&= (a\cdot 1)+0 && \text{by exercise 2}\\
&= a+0 && \text{because 1 is an identity for } \cdot\\
&= a && \text{because 0 is an identity for } + \qquad \square
\end{aligned}
$$

Problem 6 and Solution

a. $\overline{0} = 1$.

Proof. $0 \cdot 1 = 0$ because 1 is an identity for $\cdot$, and $0+1 = 1+0 = 1$ because $+$ is commutative and 0 is an identity for $+$. Thus, by the uniqueness of the complement law, $\overline{0} = 1$. $\square$

b. $\overline{1} = 0$.

Proof. $1 \cdot 0 = 0 \cdot 1 = 0$ because $\cdot$ is commutative and 1 is an identity for $\cdot$. Also $1 + 0 = 1$ because 0 is an identity for $+$. Thus, by the uniqueness of the complement law, $\overline{1} = 0$. $\square$

Problem 7 and Solution

a. There is only one element of B that is an identity for $+$.

Proof. Suppose that 0 and $0'$ are elements of B which are both identities for $+$. Then both 0 and $0'$ satisfy the identity, complement, and universal bound laws. By the identity law for $+$, for all $a \in B$,

$$a + 0 = a \quad \text{and} \quad a + 0' = a$$

It follows that

$$\begin{aligned}
a + 0 &= a + 0' && \text{because both are equal to } a \\
\overline{a} \cdot (a + 0) &= \overline{a} \cdot (a + 0') && \cdot \text{ both sides by } a \\
(\overline{a} \cdot a) + (\overline{a} \cdot 0) &= (\overline{a} \cdot a) + (\overline{a} \cdot 0') && \text{by the distributive law for } \cdot \text{ over } + \\
(a \cdot \overline{a}) + 0 &= (a \cdot \overline{a}) + 0' && \text{by the universal bound law for } \cdot \\
0 \cdot 0 &= 0' \cdot 0' && \text{by the complement law for } \cdot \\
0 &= 0' && \text{by the universal bound law for } \cdot
\end{aligned}$$

$\square$

b. There is only one element of B that is an identity for $\cdot$.

Proof. Suppose that 1 and $1'$ are elements of B which are both identities for $\cdot$. Then both 1 and $1'$ satisfy the identity, complement, and universal bound laws. By the identity law for $\cdot$, for all $a \in B$,

$$a \cdot 1 = a \quad \text{and} \quad a \cdot 1' = a$$

It follows that

$$\begin{aligned}
a \cdot 1 &= a \cdot 1' && \text{because both are equal to } a \\
\overline{a} + (a \cdot 1) &= \overline{a} + (a \cdot 1') && + \ a \text{ to both sides} \\
(\overline{a} + a) \cdot (\overline{a} + 1) &= (\overline{a} + a) \cdot (\overline{a} + 1') && \text{by the distributive law for } + \text{ over } \cdot \\
(\overline{a} + a) \cdot 1 &= (\overline{a} + a) \cdot 1' && \text{by exercise 2} \\
(a + \overline{a}) \cdot 1 &= (a + \overline{a}) \cdot 1' && \text{by the commutative law for } + \\
1 \cdot 1 &= 1' \cdot 1' && \text{by the complement law for } + \\
1 &= 1' && \text{by exercise 1}
\end{aligned}$$

$\square$

Problem 8 and Solution

For all a and b in B, $\overline{a \cdot b} = \overline{a} + \overline{b}$.

Proof. Let a and b be any elements in B.

Proof that $(a \cdot b) + (\overline{a} + \overline{b}) = 1$:

$$
\begin{aligned}
(a \cdot b) + (\overline{a} + \overline{b}) &= (\overline{a} + \overline{b}) + (a \cdot b) && \text{by the commutative law for } + \\
&= ((\overline{a} + \overline{b}) + a) \cdot ((\overline{a} + \overline{b}) + b) && \text{by the distributive law for } + \text{ over } \cdot \\
&= ((\overline{b} + \overline{a}) + a) \cdot (\overline{a} + (\overline{b} + b)) && \text{by the commutative and associative laws for } + \\
&= (\overline{b} + (\overline{a} + a)) \cdot (\overline{a} + (b + \overline{b})) && \text{by the associative and commutative laws for } + \\
&= (\overline{b} + (a + \overline{a})) \cdot (\overline{a} + 1) && \text{by the commutative and complement laws for } + \\
&= (\overline{b} + 1) \cdot 1 && \text{by the complement and universal bound laws for } + \\
&= 1 \cdot 1 && \text{by universal bound law for } + \\
&= 1 && \text{by the identity law for } \cdot
\end{aligned}
$$

Proof that $(a \cdot b) \cdot (\overline{a} + \overline{b}) = 0$:

$$
\begin{aligned}
(a \cdot b) \cdot (\overline{a} + \overline{b}) &= ((a \cdot b) \cdot \overline{a}) + ((a \cdot b) \cdot \overline{b}) && \text{by the distributive law for } \cdot \text{ over } + \\
&= ((b \cdot a) \cdot \overline{a}) + (a \cdot (b \cdot \overline{b})) && \text{by the commutative and associative laws for } \cdot \\
&= (b \cdot (a \cdot \overline{a})) + (a \cdot 0) && \text{by the associative and complement laws for } \cdot \\
&= (b \cdot 0) + 0 && \text{by the complement and universal bound laws for } \cdot \\
&= 0 + 0 && \text{by the universal bound law for } \cdot \\
&= 0 && \text{by the identity law for } +
\end{aligned}
$$

Because both $(a \cdot b) + (\overline{a} + \overline{b}) = 1$ and $(a \cdot b) \cdot (\overline{a} + \overline{b}) = 0$, it follows, by the uniqueness of the complement law, that $\overline{a \cdot b} = \overline{a} + \overline{b}$. □

Problem 9 and Solution

For all a and b in B, $\overline{a + b} = \overline{a} \cdot \overline{b}$.

Proof. Let a and b be any elements in B.

Proof that $(a + b) + (\overline{a} \cdot \overline{b}) = 1$:

$$
\begin{aligned}
(a + b) + (\overline{a} \cdot \overline{b}) &= ((a + b) + \overline{a}) \cdot ((a + b) + \overline{b}) && \text{by the distributive law for } + \text{ over } \cdot \\
&= ((b + a) + \overline{a}) \cdot (a + (b + \overline{b})) && \text{by the commutative and associative laws for } + \\
&= (b + (a + \overline{a})) \cdot (a + 1) && \text{by the associative and complement laws for } + \\
&= (b + 1) \cdot (a + 1) && \text{by the complement law for } + \\
&= 1 \cdot 1 && \text{by exercise 2} \\
&= 1 && \text{by the identity law for } +
\end{aligned}
$$

Proof that $(a+b)\cdot(\overline{a}\cdot\overline{b})=0$:

$$\begin{aligned}
(a+b)\cdot(\overline{a}\cdot\overline{b}) &= (\overline{a}\cdot\overline{b})\cdot(a+b) && \text{by commutative law for } \cdot \\
&= ((\overline{a}\cdot\overline{b})\cdot a)+((\overline{a}\cdot\overline{b})\cdot b) && \text{by the distributive law for } \cdot \text{ over } + \\
&= (a\cdot(\overline{a}\cdot\overline{b}))+(\overline{a}\cdot(\overline{b}\cdot b)) && \text{by the commutative and associative laws for } \cdot \\
&= (a\cdot\overline{a})\cdot\overline{b})+(\overline{a}\cdot(b\cdot\overline{b})) && \text{by the associative and commutative laws for } \cdot \\
&= (0\cdot\overline{b})+(\overline{a}\cdot 0) && \text{by the complement law for } \cdot \\
&= 0+0 && \text{by exercise 4} \\
&= 0 && \text{by the identity law for } +
\end{aligned}$$

Because both $(a+b)+(\overline{a}\cdot\overline{b})=1$ and $(a+b)\cdot(\overline{a}\cdot\overline{b})=0$, it follows by the uniqueness of the complement law, that $\overline{a+b}=\overline{a}\cdot\overline{b}$. □

Problem 10 and Solution

For all x, y, and z in B, if $x+y=x+z$ and $x\cdot y=x\cdot z$, then $y=z$.

Proof. Let x, y, and z be any elements in B. Then

$$\begin{aligned}
y &= (y+x)\cdot y && \text{by exercise 3} \\
&= y\cdot(x+y) && \text{by the commutative laws for } \cdot \text{ and } + \\
&= y\cdot(x+z) && x+y=x+z \\
&= (y\cdot x)+(y\cdot z) && \text{by the distributive law for } \cdot \text{ on } + \\
&= (x\cdot y)+(z\cdot y) && \text{by the commutative law for } \cdot \\
&= (x\cdot z)+(y\cdot z) && x\cdot y=x\cdot z \\
&= (z\cdot x)+(z\cdot y) && \text{by the commutative law for } \cdot \\
&= z\cdot(x+y) && \text{by the distributive law for } \cdot \text{ over } + \\
&= z\cdot(x+z) && x+y=x+z \\
&= (z+x)\cdot z && \text{by the commutative laws for } \cdot \text{ and } + \\
&= z && \text{by exercise 3}
\end{aligned}$$

□

Problem 11

Let $S=\{0,1\}$, and define operations $+$ and $\cdot$ on S be the following tables:

$+$	**0**	**1**
0	0	1
1	1	1

$\cdot$	**0**	**1**
0	0	0
1	0	1

a. Show that the elements of S satisfy the following properties:

(i) the commutative law for $+$
(ii) the commutative law for $\cdot$
(iii) the associative law for $+$

(iv) the associative law for $\cdot$

(v) the distributive law for $+$ over $\cdot$

(vi) the distributive law for $\cdot$ over $+$

b. Show that 0 is an identity element for $+$ and that 1 is an identity element for $\cdot$.

c. Define $\overline{0} = 1$ and $\overline{1} = 0$. Show that for all a in S, $a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$. It follows from parts (a)-(c) that S is a Boolean algebra with the operations $+$ and $\cdot$.

Solution

a. (i) Because S only has 2 elements, we only need to show that $0 + 1 = 1 + 0$. But this is true as they both $+$ to 1.

(ii) Because S only has 2 elements, we only need to show that $0 \cdot 1 = 1 \cdot 0$. But this is true as they both $\cdot$ to 0.

(iii)
$$\begin{array}{lcl}
0+(0+0)=0+0=0 & \text{and} & (0+0)+0=0+0=0 \\
0+(0+1)=0+1=1 & \text{and} & (0+0)+1=0+1=1 \\
0+(1+0)=0+1=1 & \text{and} & (0+1)+0=1+0=1 \\
0+(1+1)=0+1=1 & \text{and} & (0+1)+1=1+1=1 \\
1+(0+0)=1+0=1 & \text{and} & (1+0)+0=1+0=1 \\
1+(0+1)=1+1=1 & \text{and} & (1+0)+1=1+1=1 \\
1+(1+0)=1+1=1 & \text{and} & (1+1)+0=1+0=1 \\
1+(1+1)=1+1=1 & \text{and} & (1+1)+1=1+1=1
\end{array}$$

(iv)
$$\begin{array}{lcl}
0\cdot(0\cdot 0)=0\cdot 0=0 & \text{and} & (0\cdot 0)\cdot 0=0\cdot 0=0 \\
0\cdot(0\cdot 1)=0\cdot 0=0 & \text{and} & (0\cdot 0)\cdot 1=0\cdot 1=0 \\
0\cdot(1\cdot 0)=0\cdot 0=0 & \text{and} & (0\cdot 1)\cdot 0=0\cdot 0=0 \\
0\cdot(1\cdot 1)=0\cdot 1=0 & \text{and} & (0\cdot 1)\cdot 1=0\cdot 1=0 \\
1\cdot(0\cdot 0)=1\cdot 0=0 & \text{and} & (1\cdot 0)\cdot 0=0\cdot 0=0 \\
1\cdot(0\cdot 1)=1\cdot 0=0 & \text{and} & (1\cdot 0)\cdot 1=0\cdot 1=0 \\
1\cdot(1\cdot 0)=1\cdot 0=0 & \text{and} & (1\cdot 1)\cdot 0=1\cdot 0=0 \\
1\cdot(1\cdot 1)=1\cdot 1=1 & \text{and} & (1\cdot 1)\cdot 1=1\cdot 1=1
\end{array}$$

(v)
$$\begin{array}{lcl}
0+(0\cdot 0)=0+0=0 & \text{and} & (0+0)\cdot(0+0)=0\cdot 0=0 \\
0+(0\cdot 1)=0+0=0 & \text{and} & (0+0)\cdot(0+1)=0\cdot 1=0 \\
0+(1\cdot 0)=0+0=0 & \text{and} & (0+1)\cdot(0+0)=1\cdot 0=0 \\
0+(1\cdot 1)=0+1=1 & \text{and} & (0+1)\cdot(0+1)=1\cdot 1=1 \\
1+(0\cdot 0)=1+0=1 & \text{and} & (1+0)\cdot(1+0)=1\cdot 1=1 \\
1+(0\cdot 1)=1+0=1 & \text{and} & (1+0)\cdot(1+1)=1\cdot 1=1 \\
1+(1\cdot 0)=1+0=1 & \text{and} & (1+1)\cdot(1+0)=1\cdot 1=1 \\
1+(1\cdot 1)=1+1=1 & \text{and} & (1+1)\cdot(1+1)=1\cdot 1=1
\end{array}$$

(vi) $0 \cdot (0+0) = 0 \cdot 0 = 0$ and $(0 \cdot 0) + (0 \cdot 0) = 0 + 0 = 0$
$0 \cdot (0+1) = 0 \cdot 1 = 0$ and $(0 \cdot 0) + (0 \cdot 1) = 0 + 0 = 0$
$0 \cdot (1+0) = 0 \cdot 1 = 0$ and $(0 \cdot 1) + (0 \cdot 0) = 0 + 0 = 0$
$0 \cdot (1+1) = 0 \cdot 1 = 0$ and $(0 \cdot 1) + (0 \cdot 1) = 0 + 0 = 0$
$1 \cdot (0+0) = 1 \cdot 0 = 0$ and $(1 \cdot 0) + (1 \cdot 0) = 0 + 0 = 0$
$1 \cdot (0+1) = 1 \cdot 1 = 1$ and $(1 \cdot 0) + (1 \cdot 1) = 0 + 1 = 1$
$1 \cdot (1+0) = 1 \cdot 1 = 1$ and $(1 \cdot 1) + (1 \cdot 0) = 1 + 0 = 1$
$1 \cdot (1+1) = 1 \cdot 1 = 1$ and $(1 \cdot 1) + (1 \cdot 1) = 1 + 1 = 1$

b. We must show that $0 + x = x$ and that $1 \cdot x = x$ for all $x \in S$. But this is so as $S = \{0, 1\}$ and $0 + 0 = 0$, $0 + 1 = 1$, $1 \cdot 0 = 0$ and $1 \cdot 1 = 1$.

c. Let $\overline{0} = 1$ and $\overline{1} = 0$. Then

$$0 + \overline{0} = 0 + 1 = 1 \quad \text{and} \quad 0 \cdot \overline{0} = 0 \cdot 1 = 0$$
$$1 + \overline{1} = 1 + 0 = 1 \quad \text{and} \quad 1 \cdot \overline{1} = 1 \cdot 0 = 0$$

Problem 12

Prove that the associative laws for a Boolean algebra can be omitted from the definition. That is, prove that the associative laws can be derived from the other laws in the definition.

Solution

We will derive the associative laws from the commutative, distributive, identity, and complement laws. To do this we must first use these laws to derive the universal bound laws and absorption laws.

Lemma 1. *For all a in B, $a + 1 = 1$.*

Proof. Let a be any element in B. Then

$$\begin{aligned}
(a+1) &= (a+1) \cdot 1 && \text{by the identity law for } \cdot \\
&= (a+1) \cdot (a + \overline{a}) && \text{by the complement law for } + \\
&= ((a+1) \cdot a) + ((a+1) \cdot \overline{a}) && \text{by the distributive law for } \cdot \text{ over } + \\
&= (a \cdot (a+1)) + (\overline{a} \cdot (a+1)) && \text{by the commutative law for } \cdot \\
&= ((a \cdot a) + (a \cdot 1)) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the distributive law for } \cdot \text{ over } + \\
&= (a + (a \cdot 1)) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by exercise 1} \\
&= (a + a) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the identity law for } \cdot \\
&= ((a + a) \cdot 1) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the identity law for } \cdot \\
&= ((a + a) \cdot (a + \overline{a})) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the complement law for } + \\
&= (a + a \cdot \overline{a}) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the distributive law for } + \text{ over } \cdot \\
&= (a + 0) + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the complement law for } \cdot
\end{aligned}$$

$$
\begin{aligned}
&= a + ((\overline{a} \cdot a) + (\overline{a} \cdot 1)) && \text{by the identity law for } + \\
&= a + ((\overline{a} \cdot a) + \overline{a}) && \text{by the identity law for } \cdot \\
&= a + ((a \cdot \overline{a}) + \overline{a}) && \text{by the commutative law for } \cdot \\
&= a + (0 + \overline{a}) && \text{by the complement law for } \cdot \\
&= a + (\overline{a} + 0) && \text{by the commutative law for } + \\
&= a + \overline{a} && \text{by the identity law for } + \\
&= 1 && \text{by the complement law for } + \qquad \square
\end{aligned}
$$

Lemma 2. *For all a in B, $a \cdot 0 = 0$*

Proof. Let a be any element in B. Then

$$
\begin{aligned}
a \cdot 0 &= (a \cdot 0) + 0 && \text{by the identity law for } + \\
&= (a \cdot 0) + (a \cdot \overline{a}) && \text{by the complement law for } \cdot \\
&= ((a \cdot 0) + a) \cdot ((a \cdot 0) + \overline{a}) && \text{by the distributive law for } + \text{ over } \cdot \\
&= ((a \cdot 0) + (a \cdot 1)) \cdot ((a \cdot 0) + \overline{a}) && \text{by the identity law for } \cdot \\
&= (a \cdot (0 + 1)) \cdot ((a \cdot 0) + \overline{a}) && \text{by the distributive law for } \cdot \text{ over } + \\
&= (a \cdot (1 + 0)) \cdot ((a \cdot 0) + \overline{a}) && \text{by the commutative law for } + \\
&= (a \cdot 1) \cdot ((a \cdot 0) + \overline{a}) && \text{by the identity law for } + \\
&= a \cdot ((a \cdot 0) + \overline{a}) && \text{by the identity law for } \cdot \\
&= a \cdot (\overline{a} + (a \cdot 0)) && \text{by the commutative law for } + \\
&= a \cdot ((\overline{a} + a) \cdot (\overline{a} + 0)) && \text{by the distributive law for } + \text{ over } \cdot \\
&= a \cdot ((\overline{a} + a) \cdot \overline{a}) && \text{by the identity law for } + \\
&= a \cdot ((a + \overline{a}) \cdot \overline{a}) && \text{by the commutative law for } + \\
&= a \cdot (1 \cdot \overline{a}) && \text{by the complement law for } + \\
&= a \cdot (\overline{a} \cdot 1) && \text{by the commutative law for } \cdot \\
&= a \cdot \overline{a} && \text{by the identity law for } \cdot \\
&= 0 && \text{by the complement law for } \cdot \qquad \square
\end{aligned}
$$

Lemma 3. *For all a and b in B, $a + (a \cdot b) = a$.*

Proof. Let a and b be any elements in B. Then

$$
\begin{aligned}
a + (a \cdot b) &= (a \cdot 1) + (a \cdot b) && \text{by the identity law for } \cdot \\
&= a \cdot (1 + b) && \text{by the distributive law for } \cdot \text{ over } + \\
&= a \cdot (b + 1) && \text{by the commutative law for } + \\
&= a \cdot 1 && \text{by lemma 1} \\
&= a && \text{by the identity law for } \cdot \qquad \square
\end{aligned}
$$

Lemma 4. *For all a and b in B, $a \cdot (a + b) = a$.*

Proof. Let a and b be any elements in B. Then

$$
\begin{aligned}
a \cdot (a+b) &= (a+0) \cdot (a+b) && \text{by the identity law for } + \\
&= a + (0 \cdot b) && \text{by the distributive law for } + \text{ over } \cdot \\
&= a + (b \cdot 0) && \text{by the commutative law for } \cdot \\
&= a + 0 && \text{by lemma 2} \\
&= a && \text{by the identity law}
\end{aligned}
$$
□

Lemma 5. *For all $x, y,$ and z in B, $(x + (y + z)) \cdot x = x$.*

Proof. Let $x, y,$ and z be any elements in B. Then

$$
\begin{aligned}
(x + (y + z)) \cdot x &= x \cdot (x + (y + z)) && \text{by the commutative property for } \cdot \\
&= x && \text{by lemma 4}
\end{aligned}
$$
□

Lemma 6. *For all $x, y,$ and z in B, $((x + y) + z) \cdot x = x$.*

Proof. Let $x, y,$ and z be any elements in B. Then

$$
\begin{aligned}
((x + y) + z) \cdot x &= x \cdot ((x + y) + z) && \text{by the commutative property for } \cdot \\
&= (x \cdot (x + y)) + (x \cdot z) && \text{by the distributive law for } \cdot \text{ over } + \\
&= ((x \cdot x) + (x \cdot y)) + (x \cdot z) && \text{by the distributive law for } \cdot \text{ over } + \\
&= (x + (x \cdot y)) + (x \cdot z) && \text{by exercise 1} \\
&= x + (x \cdot z) && \text{by lemma 3} \\
&= x && \text{by lemma 3}
\end{aligned}
$$
□

Theorem. *For all $a, b,$ and c in B, $a + (b + c) = (a + b) + c$.*

Proof. Let $a, b,$ and c be any elements in B.

Proof that $\boldsymbol{a + (b + c) = ((a + b) + c) \cdot (a + (b + c))}$:

$$
\begin{aligned}
&((a + b) + c) \cdot (a + (b + c)) \\
&\quad = (((a + b) + c) \cdot a) + (((a + b) + c) \cdot (b + c)) && \text{by the distributive law for } \cdot \text{ over } + \\
&\quad = a + (((a + b) + c) \cdot (b + c)) && \text{by lemma 6} \\
&\quad = a + ((((a + b) + c) \cdot b) + (((a + b) + c) \cdot c)) && \text{by the distributive law for } \cdot \text{ over } + \\
&\quad = a + ((((b + a) + c) \cdot b) + ((c + (a + b)) \cdot c)) && \text{by the commutative law for } + \\
&\quad = a + (b + ((c + (a + b)) \cdot c)) && \text{by lemma 6} \\
&\quad = a + (b + c) && \text{by lemma 5}
\end{aligned}
$$

Proof that $\boldsymbol{(a + b) + c = ((a + b) + c) \cdot (a + (b + c))}$:

$$
\begin{aligned}
&((a + b) + c) \cdot (a + (b + c)) \\
&\quad = (a + (b + c)) \cdot ((a + b) + c) && \text{by the commutative law for } \cdot \\
&\quad = ((a + (b + c)) \cdot (a + b)) + ((a + (b + c)) \cdot c) && \text{by the distributive law for } \cdot \text{ over } + \\
&\quad = ((a + (b + c)) \cdot (a + b)) + (((c + b) + a) \cdot c) && \text{by the commutative law for } + \text{ applied twice} \\
&\quad = ((a + (b + c)) \cdot (a + b)) + c && \text{by lemma 6} \\
&\quad = (((a + (b + c)) \cdot a) + ((a + (b + c)) \cdot b)) + c && \text{by the distributive law for } \cdot \text{ over } + \\
&\quad = (a + ((a + (b + c)) \cdot b)) + c && \text{by lemma 5} \\
&\quad = (a + (((b + c) + a) \cdot b)) + c && \text{by the commutative law for } + \\
&\quad = (a + b) + c && \text{by lemma 6}
\end{aligned}
$$

Since $a+(b+c) = ((a+b)+c)\cdot(a+(b+c))$ and $(a+b)+c = ((a+b)+c)\cdot(a+(b+c))$ we can conclude from the transitivity of equality that $a+(b+c) = (a+b)+c$. $\square$

Lemma 7. *For all x, y, and z in B, $(x \cdot (y \cdot z)) + x = x$.*

Proof. Let x, y, and z be any elements in B. Then,

$$\begin{aligned} (x \cdot (y \cdot z)) + x &= x + (x \cdot (y \cdot z)) && \text{by the commutative law for } + \\ &= x && \text{by lemma 3} \end{aligned}$$

$\square$

Lemma 8. *For all x, y, and z in B, $((x \cdot y) \cdot z) + x = x$.*

Proof. Let x, y, and z be any elements in B. Then,

$$\begin{aligned} ((x \cdot y) \cdot z) + x &= x + ((x \cdot y) \cdot z) && \text{by the commutative law for } + \\ &= (x + (x \cdot y)) \cdot (x + z) && \text{by the distributive law for } + \text{ over } \cdot \\ &= x \cdot (x + z) && \text{by lemma 3} \\ &= x && \text{by lemma 4} \end{aligned}$$

$\square$

Theorem. *For all a, b, and c in B, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

Proof. Let x, y, and z be any elements in B.

Proof that $\boldsymbol{a \cdot (b \cdot c) = ((a \cdot b) \cdot c) + (a \cdot (b \cdot c))}$:

$$\begin{aligned} &((a \cdot b) \cdot c) + (a \cdot (b \cdot c)) \\ &\quad = (((a \cdot b) \cdot c) + a) \cdot (((a \cdot b) \cdot c) + (b \cdot c)) && \text{by the distributive law for } + \text{ over } \cdot \\ &\quad = a \cdot (((a \cdot b) \cdot c) + (b \cdot c)) && \text{by lemma 8} \\ &\quad = a \cdot ((((a \cdot b) \cdot c) + b) \cdot (((a \cdot b) \cdot c) + c)) && \text{by the distributive law for } + \text{ over } \cdot \\ &\quad = a \cdot ((((b \cdot a) \cdot c) + b) \cdot ((c \cdot (a \cdot b)) + c)) && \text{by the commutative law for } \cdot \text{ applied twice} \\ &\quad = a \cdot (b \cdot ((c \cdot (a \cdot b)) + c)) && \text{by lemma 8} \\ &\quad = a \cdot (b \cdot c) && \text{by lemma 7} \end{aligned}$$

Proof that $\boldsymbol{(a \cdot b) \cdot c = ((a \cdot b) \cdot c) + (a \cdot (b \cdot c))}$:

$$\begin{aligned} &((a \cdot b) \cdot c) + (a \cdot (b \cdot c)) \\ &\quad = (a \cdot (b \cdot c)) + ((a \cdot b) \cdot c) && \text{by the commutative property for } + \\ &\quad = ((a \cdot (b \cdot c)) + (a \cdot b)) \cdot ((a \cdot (b \cdot c)) + c) && \text{by the distributive law for } + \text{ over } \cdot \\ &\quad = ((a \cdot (b \cdot c)) + (a \cdot b)) \cdot (((c \cdot b) \cdot a) + c) && \text{by the commutative law for } \cdot \text{ applied twice} \\ &\quad = ((a \cdot (b \cdot c)) + (a \cdot b)) \cdot c && \text{by lemma 8} \\ &\quad = (((a \cdot (b \cdot c)) + a) \cdot ((a \cdot (b \cdot c)) + b)) \cdot c && \text{by the distributive law for } + \text{ over } \cdot \\ &\quad = (a \cdot ((a \cdot (b \cdot c)) + b)) \cdot c && \text{by lemma 7} \\ &\quad = (a \cdot (((b \cdot c) \cdot a) + b)) \cdot c && \text{by the commutative law for } \cdot \\ &\quad = (a \cdot b) \cdot c && \text{by lemma 8} \end{aligned}$$

Since $a \cdot (b \cdot c) = ((a \cdot b) \cdot c) + (a \cdot (b \cdot c))$ and $(a \cdot b) \cdot c = ((a \cdot b) \cdot c) + (a \cdot (b \cdot c))$ we can conclude from the transitivity of equality that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. $\square$

In 13-18 determine whether each sentence is a statement. Explain your answers.

Problem 13

This sentence is false.

Solution

The sentence is not a statement because it is neither true nor false. If the sentence were true then it would be true that the sentence is false which is a contradiction. Hence the sentence is not true. If the sentence were false then it would be false that the sentence is false and so the sentence would be true which is a contradiction. Hence the sentence is not false.

Problem 14

If $1 + 1 = 3$, then $1 = 0$.

Solution

This sentence is a statement because it is true. Since the hypothesis $1 + 1 = 3$ is never true the conclusion will always be true. This is an example of a statement that is vacuously true.

Problem 15

The sentence in this box is a lie.

Solution

The sentence is not a statement because it is neither true nor false. If the sentence in the box were true then it would be true that the sentence in the box is a lie or false which is a contradiction. If the sentence in the box were false then it would be false that the sentence in the box is false and so the sentence in the box would be true. This is a contradiction and so the sentence in the box is not false.

Problem 16

All positive integers with negative squares are prime.

Solution

The sentence is false if, and only if, its negation is true. The negation of the sentence is that there exists a positive integer with a negative square that is not prime. Since no such integers exist the negation is false and the sentence is true. Hence the sentence is a statement.

Problem 17

This sentence is false or $1 + 1 = 3$.

Solution

The sentence is not a statement because it is neither true nor false. If the sentence were true then it would be true that the sentence is false or $1 + 1 = 3$. But $1 + 1 \neq 3$ and so it must be that the sentence is false which is a contradiction. If the sentence were false then it would be false that the sentence is false or $1 + 1 = 3$. But this means that both sub sentences on both sides of the or must be false. Then it must be the false that the sentence is false and so the sentence is true which is a contradiction.

Problem 18

This sentence is false and $1 + 1 = 2$.

Solution

The sentence is not a statement because it is neither true nor false. If the sentence were true then it would be true that the sentence is false and $1 + 1 = 2$ which is a contradiction. If the sentence were false then it would be false that the sentence is false and $1 + 1 = 2$. This would mean that the the sentence is true or $1 + 1 \neq 2$. But $1 + 1 = 2$ and so it would have to be that the sentence is true which is a contradiction.

Problem 19

a. Assuming that the following sentence is a statement, prove that $1 + 1 = 3$:

   If this sentence is true, then $1 + 1 = 3$.

b. What can you deduce from part (a) about the status of "this sentence is true"? Why?

Solution

a. If the sentence is a statement then it is either true or false.

   Case 1, the sentence is true: In this case when the statement asks "If this sentence is true", the answer will be yes. Now by definition of an if then statement, if the hypothesis is true and the statement is true, then the conclusion is also true. It follows that $1 + 1 = 3$.

   Case 2, the sentence is false: In this case when the statement asks "If this sentence is true", the answer will be no. Now by definition of an if then statement, if the hypothesis is false then the conclusion is always true vacuously. Hence $1 + 1 = 3$.

b. Since no truth value of the sentence leads to a contradiction and since both truth values of the sentence lead to the same result we can not conclude anything about the truth of the sentence "this sentence is true".

Problem 20

The following two sentences were devised by the logician Saul Kripke. While not intrinsically paradoxical, they could be paradoxical under certain circumstances. Describe such circumstances.

1. Most of Nixon's assertions about Watergate are false.
2. Everything Jones says about Watergate is true.

Solution

Suppose that Nixon says 2 and the only utterance that Jones makes about Watergate is 1. Further suppose that apart from 2, all of Nixon's other assertions about Watergate are evenly split between true and false.

Case 1, 2 is true: Since 2 is true, it follows that the majority of claims that Nixon has made about Watergate are true. Furthermore, the truth of 2 implies that everything Jones says about Watergate is true. Since Jones says 1, it is true that most of Nixon's assertions about Watergate are false. We now have that most of Nixon's assertions about Watergate are true and that most of Nixon's assertions about Watergate are false which is a contradiction.

Case 2, 2 is false: Since 2 is false, it follows that the majority of claims that Nixon has made about Watergate are false. Furthermore the falsity of 2 implies that there exists some statement made by Jones about Watergate which is false. Since Jones only says 1, it must be that 1 is that false statement. But now, by the falsity of 1, most of Nixon's assertions about Watergate are true. This is a contradiction as we previously obtained that the majority of Nixon's assertions about Watergate are false.

Conclusion: Since our suppositions lead to a contradiction in the case that 2 is true and in the case that 2 is false we conclude that the simple sentence that "Everything Jones says about Watergate is true" is neither true not false. Thus we obtain a paradox.

Problem 21

Can there exist a computer program that has as output a list of all the computer programs that do not list themselves in their output? Explain your answer.

Solution

No. Suppose that such a program could exist. Either it would list itself in its output or it would not list itself in its output. If it listed itself in its output then it would fail to be a member of those programs which do not list themselves in their output and yet it would be on the list. Thus the program would fail in performing the task that it supposedly can perform. On the other hand, if it did not list itself in its output then it would be a member of those programs which do not list themselves in their output and yet it would fail to be on the list. Thus the program would fail in performing the task that it supposedly can perform. Since the program fails to perform the desired task in the case that it lists itself in its output and in the case that it does not list itself in its output and since these are the only two possibilities, no such program can exist.

Problem 22

Can there exist a book that refers to all those books and only those books that do not refer to themselves? Explain your answer.

Solution

No. Suppose that such a book could exist. Either it would refer to itself or it would not refer to itself. If it referred to itself then it would not be a member of those books that do not refer to themselves and yet it would be referred to in its pages. Thus the book would fail to fulfill the requirement that it only refers to books that do not refer to themselves. On the other hand, if the book did not refer to itself, then it would be a member of those books that do not refer to themselves and yet it would fail to refer to itself in its pages. Thus the book would fail to fulfill the requirement that it refer to all those books that do not refer to themselves. Since the book fails to satisfy its definition in the case that it refers to itself and in the case that it does not refer to itself and since these two cases are the only cases which are possible, we can conclude that no such book can exist.

Problem 23

Some English adjectives are descriptive of themselves (for instance, the word *polysyllabic* is polysyllabic) whereas others are not (for instance, the word *monosyllabic* is not monosyllabic). The word *heterological* refers to an adjective that does not describe itself. Is *heterological* heterological? Explain you answer.

Solution

It can not be determine whether the word *heterological* is heterological. Suppose that the word *heterological* is heterological. Then the word *heterological* does not describe itself. But this means that the word *heterological* is not heterological which is a contradiction. Now suppose that the word *heterological* is not heterological. Then the word *heterological* describes itself. But this means that the word *heterological* is heterological which is a contradiction.

Problem 24

As strange as it may seem, it is possible to give a precise-looking definition of an integer that, in fact, is not a definition at all. The following was devised by and English librarian, G. G. Berry, and reported by Bertrand Russell. Explain how it leads to a contradiction. Let n be "the smallest integer not describable in fewer that 12 English words". (Note that the total number of strings consisting of 11 or fewer English words is finite.)

Solution

Suppose that n is "the smallest integer not describable in fewer that 12 English words". Then n is not describable in fewer than 12 English words and n is describable in 11 English words as the phrase "the smallest integer not describable in fewer that 12 English words" contains only 11 English words. Thus a contradiction is reached and so n is not the smallest integer describable in fewer than 12 English words.

Problem 25

Is there an algorithm which, for a fixed quantity a and any input algorithm X and data set D, can determine whether X prints a when run with data set D? Explain. (This problem is called the printing problem.)

Solution

Theorem. *There is no computer algorithm that will accept any algorithm X, data set D, and fixed quantity a as input and then will output "prints a" or "does not print a" to indicate whether or not X prints a in a finite number of steps when X is run with data set D.*

Proof. Suppose there is an algorithm, Prints, such that if an algorithm X, a data set D, and a fixed quantity a are input, then

Prints(X, D, a) prints

"prints a"	if X prints a in a finite number of steps when run with data set D

or

"does not print a"	if X prints a in a finite number of steps when run with data set D

Define a new algorithm, Test, as follows: For any input algorithm X, input data D, and fixed quantity a,

Test(X, D, a)

does not print a if Prints(X, D, a) prints "prints a"

or prints a if Prints(X, D, a) prints "does not print a"

Now run algorithm Test with input Test, D, and a. If Test(Test, D, a) prints a after a finite number of steps, then the value of Prints(Test, D, a) is "prints a" and so Test(Test, D, a) does not print a. On the other hand, if Test(Test, D, a) does not print a after a finite number of steps, then the value of Prints(Test, D, a) is "does not print a" and so Test(Test, D, a) prints a. The reasoning above shows that Test(Test, D, a) prints a and also does not print a. This is a contradiction. But the existence of Test follows logically from the supposition of the existence of an algorithm Prints that can check whether any algorithm and data set prints a. Hence the supposition is false and there is no such algorithm. $\square$

Problem 26

Use a technique similar to that used to derive Russell's paradox to prove that for any set A, $\mathscr{P}(A) \nsubseteq A$.

Solution

Proof. Let A be any set and define another set

$$S = \{B \mid B \subseteq A \text{ and } B \notin B\}.$$

It follows that S is the set of all subsets of A which is the power set of A. Hence $S = \mathscr{P}(A)$. Now suppose that $S \in S$. This supposition implies, by the definition of S, that $S \notin S$ which is a contradiction. Now suppose that $S \notin S$. This supposition implies, by the definition of S, that it is false that $S \subseteq A$ and $S \notin S$. By De Morgan's laws of logic, it is true that $S \nsubseteq A$ or $S \in S$. But we already know that $S \in S$ leads to a contradiction and so it must be true that $S \nsubseteq A$. It now follows from the fact that $S = \mathscr{P}(A)$ that $\mathscr{P}(A) \nsubseteq A$. $\square$