VE203 Discrete Math
Spring 2022 — HW2 Solutions

March 19, 2022

JOINT INSTITUTE
交大密西根学院

Exercise 2.1

Base Case: (A is a set of order 1)

If $A = \{a\}$ then the largest and smallest elements are both a.

Inductive Step: Suppose all sets of order n have a largest and smallest element. Let A be a set of order $n+1$. Further, since we already proved the base case we can assume that A has at least 2 elements. We need to show that A has a largest and smallest element.

A is nonempty so let $x \in A$. Consider the set $A_0 = A \backslash \{x\}$. This is a set of order n. Thus, by the inductive hypothesis, A_0 has a largest and smallest element.

- Let a be the smallest element of A_0.
- Let b be the largest element of A_0.

Observe that $A = A_0 \cup \{x\}$. We can identify the largest and smallest elements of A as follows.

- If $x < a$ then x is smaller than all other elements of A meaning x is the smallest element of A. Otherwise, a is smaller than all other values of A.
- If $x > b$ then x is larger than all other elements of A meaning x is the largest element of A. Otherwise, b is larger than all other values of A.

End of proof.

Exercise 2.2

In this proof, in order to find $a^k(P(k+1)), a^{k-1}(P(k))$ and $a^{k-2}(P(k-1))$ are used as value 1 . However, for the base case, it only proves that for n $= 1, a^{n-1}(P(1)) = 1$. That is to say, if we check the case n $= 2, a^1 = \frac{a^0 \cdot a^0}{a^{-1}}$, the value of $a^{-1}(P(0))$ is actually unknown and doesn't necessarily equals to 1 . So the proof is invalid.

Exercise 2.3

1) If the "nonempty sorted list" is $\langle x, \langle\rangle\rangle$. Then the statement is vacuously true.

2) If the "nonempty sorted list" is $\langle x, \tilde{L}\rangle$ where $\tilde{L} = \langle y, L\rangle$ and the statement is true, i.e., y is the smallest number in L and $x \leqslant y$. Denote the number of elements in $\langle y, L\rangle\rangle$ as n. Then for the number of elements is $n+1$, say the "additional" element is k. The "nonempty sorted list" now is $\langle x, \langle k, \tilde{L}\rangle\rangle$.

By definition, since $\langle k, \tilde{L}\rangle$ is a nonempty sorted list, $k \leqslant y$. Since $\langle x, \langle k, \tilde{L}\rangle\rangle$ is a nonempty sorted list, $x \leqslant k$. Therefore, every element z in $\langle k, \tilde{L}\rangle$ satisfies $z \geqslant x$.

Therefore, in a nonempty sorted list $\langle x, L\rangle$, every element z in L satisfies $z \geqslant x$.

Exercise 2.4

(i) Base case: φ is a variable. No need for connectives from the set $\{\downarrow\}$. Let $A(\varphi,$ be the property that there exists $a\{\downarrow\}$-only proposition logically equivalent to φ. Inductive case: 1. φ is a negation. $\varphi = \neg p$. Assume the $HA(p)$. By H. there exists a $\{\downarrow\}$-only proposition $q \Leftrightarrow \cdot P$.

Here $\neg p \Leftrightarrow \neg q \Leftrightarrow q \downarrow q$. therefore. $A(\neg p)$ follows

I1. φ is a conjunction. disjunction. or implication. $\varphi = P_1 \wedge P_2, \varphi = P_1 \vee P_2, \quad \varphi \cdot P_1 \rightarrow P_1$. Assume. $\mid HA\,(p_1)$. $A\,(p_2)$, there exists $\{\downarrow\}$-only proposition $q_1 \Leftrightarrow p_1, q_2 \Leftrightarrow p_2$ Here. $p_1 \wedge p_2 \Leftrightarrow q_1 \wedge q_2 \Leftrightarrow \quad (q_1 \downarrow q_1) \downarrow (q_2 \downarrow q_2)$.

$$\begin{aligned} p_1 \vee p_2 \Leftrightarrow q_1 \vee q_2 \quad &\Leftrightarrow \quad (q_1 \downarrow q_2) \downarrow (q_1 \downarrow q_2) \\ p_1 \rightarrow p_2 \Leftrightarrow q_1 \rightarrow q_2 \Leftrightarrow &\quad ((q_1 \downarrow q_1) \downarrow q_2) \downarrow ((q_1 \downarrow q_1) \downarrow q_2)\,. \end{aligned}$$

Therefore. $A\,(P_1 \wedge P_2)\,.\quad A\,(P_1 \vee P_2)\,.\quad A\,(P_1 \rightarrow P_2)$ follows.

Hence. the statement is true.

(ii) Here. let $A(\varphi\ )$ denote the property that there exists a $\{|\}-$ only proposition logically equivalent to φ. and we need to prove $A(\varphi)$ holds for any well-formed formula φ.

Base case: φ is a variable. $\varphi = x$. No need for connectives from the set $\{|\}$. $A(\varphi)$ is vacuously true.

Inductive case: $I.\varphi$ is a negation. $\varphi = \neg p$. Assume the $IHA(P)$ there exists a $\{|\}$ - only proposition $q \Leftrightarrow p$.

Here. $\neg p \Leftrightarrow \neg q \Leftrightarrow q \mid q$. therefore $A(\neg p)$ follows 11. φ is a corjunction. disjunction. or implication. $\varphi = p_1 \wedge p_2 \quad \varphi = p_1 v p_2, \varphi = p_1 \rightarrow p_2$.

Assume $IHA\,(p_1)$. A(p, there exists a $\{|\}-$ only proposition $q_1 \Leftrightarrow p_1, q_2 \Leftrightarrow p_2$.

$$\begin{aligned} p_1 \vee p_2 \Leftrightarrow q_1 \vee q_2 \Leftrightarrow (q_1 | \, q_1) \mid (q_2 \mid q_2)\,. \\ p_1 \rightarrow p_1 \Leftrightarrow q_1 \rightarrow q_2 \Leftrightarrow q_1 \mid (q_2 \mid q_2)\,. \end{aligned}$$

Therefore. $\quad A\,(p_1 \wedge p_2)\,.\quad A\,(p_1 \vee p_2)\,.\quad A\,(p_1 \rightarrow p_2)$ follows.

Hence, the statement is true.

Exercise 2.5

(i) mergesort:

Base case: $n = 1$, there is only one element in $A[D] \Rightarrow A[]$ is sorted.

Inductive case: Assume that for n element, $A[1. \ldots, n]$ can be sorted through mergesort, where $n = 1, 2, 3, \ldots, k-1$ Then for k elements. L contains $\frac{k}{2}$ elements. $\because 1 \leqslant \frac{k}{2} \leqslant k-1 \therefore L$ can be sorted.

R contains $\frac{k}{2}$ elements. $\because 1 \leq \frac{k}{2} \leq k-1 \therefore R$ can be sorted.

Then by using merge $(L, R), A[1..k]$ an be sorted in increasing order.

(ii) merge:

Base case:

(1) $n = 0$ then X is empty, only return Y, which is sorted

(2) $m = 0$ then Y is empty. only return X, which is sorted.

Inductive case: Assume that for n-i elements in X and for m-elements in Y. X∪Y an be sort through merge namely merge $(X[1 \ldots n-1], Y)$ and merge X. $Y[1 \ldots -1])$ hold.

Then for n elements in X and m elements in Y, namely $X[1.n]$ and $Y[1..m]$

We compare $X[1]$ and $Y[1]$: $(1) X[1] < Y[1]$, return $X[1]$ followed by merge $(X[2..n], Y)$

As $X[2 \ldots n]$ contains $n-1$ elements, merge $(X[2.n]$. Y) holds $\Rightarrow x[1 \ldots n] \cup Y[1 \ldots n]$ can be sorted

(2) $X[1] \geqslant Y[1]$, return $Y[1]$ followed by merge ($X.Y[2 \ldots m-1]$)

As $Y[2 \ldots m-1]$ contains $m-1$ elements, merge $(X$. Y[2...m-1])holds $\Rightarrow X[1 \ldots n] \cup Y[1 \ldots n]$ can be sorted

Exercise 2.6

(i) Reflexive:

For any a $\in \mathbb{Z}, a-a=0$. Since $2 \mid 0, a \sim a$. Therefore, $\sim$ is reflexive.

Symmetric:

If $m \sim n$, then $2 \mid (n-m)$. Let $n-m=2k$, where $k \in \mathbb{Z}$. Then $m-n=-2k=2\cdot(-k)$, which implies that $2 \mid (m-n)$. Thus, $n \sim m$, which shows that $m \sim n \Rightarrow n \sim m$.

The reverse direction, i.e. $n \sim m \Rightarrow m \sim n$, is also valid with the same process given above.

Therefore, $m \sim n \Leftrightarrow n \sim m$, and $\sim$ is symmetric. Transitive:

Suppose that $m \sim n \wedge n \sim s$. Then, $2 \mid (n-m)$ and $2 \mid (s-n)$. We assume that $n-m=2k_1$, $s-n=2k_2$. Then, $s-m=(s-n)+(n-m)=2k_2+2k_1=2\left(k_1+k_2\right)$. This shows that $2 \mid (s-m)$, which implies that $m \sim s$.

Therefore, $\sim$ is transitive.

(ii) $\mathbb{Z}_2=\mathbb{Z}/\sim=\{[0],[1]\}$.

(iii) We arbitrarily take 2 representatives m_1, m_2 from the first equivalence class [m], and 2 representatives n_1, n_2 from the second equivalence class $[n]$.

- $[m_1]+[n_1]=[m_1+n_1]=\{t \in \mathbb{Z} \mid (m_1+n_1) \sim t\}$.

For $t \in \left[m_1+n_1\right], 2 \mid (t-m_1-n_1)$. Let $t-m_1-n_1=2k(k \in \mathbb{Z})$, then $t=2k+m_1+n_1$.

Since $m_1, m_2 \in \left[m_1\right], m_1 \sim m_2$. Let $m_2-m_1=2k_m\left(k_m \in \mathbb{Z}\right)$. Similarly, let $n_2-n_1=2k_n\left(k_n \in \mathbb{Z}\right)$.

Thus,

$$
\begin{aligned}
t-m_2-n_2 &= 2k+m_1+n_1-m_2-n_2 \\
&= 2k-(m_2-m_1)-(n_2-n_1) \\
&= 2k-2k_m-2k_n \\
&= 2\left(k-k_m-k_n\right)
\end{aligned}
$$

Because $k-k_m-k_n \in \mathbb{Z}, 2 \mid (t-m_2-n_2)$, which means that $m_2+n_2 \sim t$.

It shows that $t \in [m_2+n_2]$, which implies that $[m_1+n_1] \subset [m_2+n_2]$.

The proof of $[m_2+n_2] \subset [m_1+n_1]$ is done with the same process shown above.

Therefore, $[m_1+n_1]=[m_2+n_2]$. This implies that the definition of addition on $\mathbb{Z}$ is independent of the representatives m and n.

- For any $t \in [m_1] \cdot [n_1]=\left[m_1 \cdot n_1\right], 2 \mid (t-m_1n_1)$. Let $t-m_1n_1=2k(k \in \mathbb{Z})$, then $t=2k+m_1n_1$.

Then, $t-m_2n_2=2k+m_1n_1-m_2n_2$.

As is assumed in the previous section, $m_2-m_1=2k_m, n_2-n_1=2k_n\left(k_m, k_n \in \mathbb{Z}\right)$.

Thus,

$$
\begin{aligned}
t-m_2n_2 &= 2k+m_1n_1-\left(m_1+2k_m\right)\left(n_1+2k_n\right) \\
&= 2k+m_1n_1-\left(m_1n_1+2k_mn_1+2k_nm_1+4k_mk_n\right) \\
&= 2k-2k_mn_1-2k_nm_1-4k_mk_n \\
&= 2\left(k-k_mn_1-k_nm_1-2k_mk_n\right)
\end{aligned}
$$

Since $k - k_m n_1 - k_n m_1 - 2k_m k_n \in \mathbb{Z}, 2 \mid (t - m_2 n_2)$. This shows that $t \in [m_2 \cdot n_2]$, which implies that $[m_1 \cdot n_1] \subset [m_2 \cdot n_2]$.

The proof of $[m_2 \cdot n_2] \subset [m_1 \cdot n_1]$ is done with the same process shown above.

Therefore, $[m_1 \cdot n_1] = [m_2 \cdot n_2]$. This implies that the definition of multiplication on $\mathbb{Z}$ is independent of the representatives m and n.

(iv) For the following section, we keep in mind that

$\mathbb{Z}_2 = \{[0], [1]\}$.

(a) $[0] + [0] = [0] \in \mathbb{Z}_2$
$[0] + [1] = [1] \in \mathbb{Z}_2$
$[1] + [1] = [2] = [0] \in \mathbb{Z}_2$
Thus, $(\mathbb{Z}_2, +, \cdot)$ is closure under addition.

(b) $[0] \cdot [0] = [0] \in \mathbb{Z}_2$
$[0] \cdot [1] = [0] \in \mathbb{Z}_2$
$[1] \cdot [1] = [1] \in \mathbb{Z}_2$
Thus, $(\mathbb{Z}_2, +, \cdot)$ is closure under multiplication.

(c) Let the representatives of m and n be m_r and n_r respectively. Then, $m + n = [m_r + n_r] = [n_r + m_r] = n + m$. Therefore, $m + n = n + m$, and commutativity of the addition "+" is valid for $(\mathbb{Z}_2, +, \cdot)$.

(d) Let the representatives of m and n be m_r and n_r respectively. Then, $m \cdot n = [m_r \cdot n_r] = [n_r \cdot m_r] = n \cdot m$. Therefore, $m \cdot n = n \cdot m$, and commutativity of the multiplication "·" is valid for $(\mathbb{Z}_2, +, \cdot)$.

(e) For this section, we refer to table 1. Clearly, $(m + n) + k = n + (m + k)$.

m	n	k	$(m+n)+k$	$n+(m+k)$	$(m \cdot n) \cdot k$	$n \cdot (m \cdot k)$	$k \cdot (m+n)$	$k \cdot m + k \cdot n$
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[0]	[0]	[1]	[1]	[1]	[0]	[0]	[0]	[0]
[0]	[1]	[0]	[1]	[1]	[0]	[0]	[0]	[0]
[0]	[1]	[1]	[0]	[0]	[0]	[0]	[1]	[1]
[1]	[0]	[0]	[1]	[1]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[0]	[0]	[0]	[0]	[1]	[1]
[1]	[1]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[1]	[1]	[1]	[1]	[1]	[0]	[0]

(f) For this section, we refer to table 1. Clearly, $(m \cdot n) \cdot k = n \cdot (m \cdot k)$.

(g) For this section, we refer to table 1 . Clearly, $k \cdot (m + n) = k \cdot m + k \cdot n$.

(h) $0 = [0]$, since $[0] + [0] = [0]$ and $[1] + [0] = [1]$.

(i) $1 = [1]$, since $[0] \cdot [1] = [0]$ and $[1] \cdot [1] = [1]$.

(j) For $[0], [0] + [0] = [0] = 0$. For $[1], [1] + [1] = [0] = 0$.

(k) For $[0]$, since $[0] = 0$, we ignore this case. For $[1], [1] \cdot [1] = [1] = 1$.

(l) $0 = [0] \neq [1] = 1$.

Exercise 2.7

	reflexive	symmetric	transitive
$x+y=0$	$\perp$	$\top$	$\perp$
$2 \mid (x-y)$	$\top$	$\top$	$\top$
$xy=0$	$\perp$	$\top$	$\perp$
$x=1$ or $y=1$	$\perp$	$\top$	$\perp$
$x=\pm y$	$\top$	$\top$	$\top$
$x=2y$	$\perp$	$\perp$	$\perp$
$xy \geq 0$	$\top$	$\top$	$\perp$
$x=1$	$\perp$	$\perp$	$\top$

Exercise 2.8

(i)

$$\begin{aligned}
f(A\cup B) &= \{f(x) \mid x \in A\cup B\} \\
&= f(x \mid x \in A) \cup f(x \mid x \in B) \\
&= f(A) \cup f(B) \\
\therefore f(A\cup B) &= f(A) \cup f(B)
\end{aligned}$$

(ii)

$$\begin{aligned}
&f(A\cap B) \subset f(A), f(A\cap B) \subset f(B) \\
&\qquad\qquad\qquad\qquad \Leftrightarrow f(A\cap B) \subset f(A)\cap f(B)
\end{aligned}$$

Now, if f is an injective function, let $y \in f(A)\cap f(B)$. Then, there exists x_1 in A that satisfies $f(x_1) = y$ and x_2 in B that satisfies $f(x_2) = y$. By injectivity, $x_1 = x_2$.

$$\begin{aligned}
x_1 = x_2 \in A\cap B &\Leftrightarrow y = f(x_1) = f(x_2) \in f(A\cap B) \\
&\Leftrightarrow f(A)\cap f(B) \subset f(A\cap B)
\end{aligned}$$

Since the two sets are subset of each other, $f(A\cap B) = f(A)\cap f(B)$. Therefore, we can conclude that $f(A\cap B) \subset f(A)\cap f(B)$, where equality holds if f is injective.

(iii) There exists $y \in f(A) - f(B)$ and x such that $y = f(x)$

$$y \in f(A) - f(B) \Leftrightarrow y \in f(A) \wedge x \notin f(B)$$

Then, there exists $a \in A$ that $y = f(a)$.

Also, $a \notin B$ because $x = f(a) \in f(B)$ violates the initial condition that $y \notin f(B)$. So, $a \in A - B$ and $x = f(a) \in f(A-B)$

$$\therefore f(A) - f(B) \subset f(A-B)$$

If f is injective, let $y \in f(A-B)$. There exists $x \in A-B$ such that $y = f(x)$. By injectivity, $f(x) \in f(A)$ but $f(x) \notin f(B)$.

$$\begin{aligned}
&\therefore f(A-B) \subset f(A) - f(B) \\
&\Rightarrow f(A-B) = f(A) - f(B)
\end{aligned}$$

Therefore, we can conclude that $f(A) - f(B) \in f(A-B)$, where equality holds if f is injective.

(iv) f^{-1} exists only when f is bijective. Then, $f : X \to Y$ implies $f^{-1} : Y \to X$. From the conclusion of (i) that $f(A \cup B) = f(A) \cup f(B)$ when f is injective, we can also conclude that $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(v) f^{-1} exists only when f is bijective. Then, $f : X \to Y$ implies $f^{-1} : Y \to X$. From the conclusion of (ii) that $f(A \cap B) = f(A) \cap f(B)$ when f is injective, we can also conclude that $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

(vi) f^{-1} exists only when f is bijective. Then, $f : X \to Y$ implies $f^{-1} : Y \to X$. From the conclusion of (iii) that $f(A) - f(B) = f(A - B)$ when f is injective, we can also conclude that $f^{-1}(A - B) = f^{-1}(A) - f^{-1}(B)$.