

R06 Exercises

Ramana Kumar (rk436)

November 2, 2010

EXERCISES 2

Exercise 2.1

(i) Consider truth tables for $\neg B \Rightarrow \neg A$ and for $A \Rightarrow B$.

A	B	$\neg B$	$\neg A$	$\neg B \Rightarrow \neg A$	A	B	$A \Rightarrow B$
T	T	F	F	T	T	T	T
T	F	T	F	F	T	F	F
F	T	F	T	T	F	T	T
F	F	T	T	T	F	F	T

The truth values in the left two and rightmost columns are the same in both tables. It follows that $\neg B \Rightarrow \neg A$ and $A \Rightarrow B$ are logically equivalent.

The truth table rule for \Leftrightarrow assigns T when the inputs are the same and F otherwise. Thus we have the following truth table.

A	B	$\neg B \Rightarrow \neg A$	$A \Rightarrow B$	$(\neg B \Rightarrow \neg A) \Leftrightarrow (A \Rightarrow B)$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

The rightmost column has T in every row, so $(\neg B \Rightarrow \neg A) \Leftrightarrow (A \Rightarrow B)$ is a tautology. Indeed, it is clear that connecting any logically equivalent propositions by \Leftrightarrow will result in a tautology.

(ii) We prove the equality as follows.

$$\begin{aligned}
\llbracket \neg B \Rightarrow \neg A \rrbracket_{\mathcal{M}} &= \llbracket \neg \neg B \vee \neg A \rrbracket_{\mathcal{M}} && \text{definition of } \Rightarrow \\
&= \llbracket \neg \neg B \rrbracket_{\mathcal{M}} \cup \llbracket \neg A \rrbracket_{\mathcal{M}} && \text{interpretation of } \vee \\
&= \llbracket \neg A \rrbracket_{\mathcal{M}} \cup \llbracket \neg \neg B \rrbracket_{\mathcal{M}} && \text{commutativity of } \cup \\
&= \llbracket \neg A \rrbracket_{\mathcal{M}} \cup \llbracket \neg B \rrbracket_{\mathcal{M}}^c && \text{interpretation of } \neg \\
&= \llbracket \neg A \rrbracket_{\mathcal{M}} \cup (\llbracket B \rrbracket_{\mathcal{M}}^c)^c && \text{interpretation of } \neg \\
&= \llbracket \neg A \rrbracket_{\mathcal{M}} \cup \llbracket B \rrbracket_{\mathcal{M}} && \text{complement identity} \\
&= \llbracket \neg A \vee B \rrbracket_{\mathcal{M}} && \text{interpretation of } \vee \\
&= \llbracket A \Rightarrow B \rrbracket_{\mathcal{M}} && \text{definition of } \Rightarrow
\end{aligned}$$

The equality above, considered as subset inclusion in both directions, can be rephrased as $\neg B \Rightarrow \neg A$ entails $A \Rightarrow B$ in \mathcal{M} , and $A \Rightarrow B$ entails $\neg B \Rightarrow \neg A$ in \mathcal{M} . Since \mathcal{M} is arbitrary, we deduce both $\neg B \Rightarrow \neg A \models A \Rightarrow B$ and $A \Rightarrow B \models \neg B \Rightarrow \neg A$, which together mean $(\neg B \Rightarrow \neg A) = (A \Rightarrow B)$. By Corollary 2.12 we conclude $\models [(\neg B \Rightarrow \neg A) \Leftrightarrow (A \Rightarrow B)]$.

Exercise 2.3

Base cases In each case, the result follows from $1 \leq 2$:

$$1 = |\mathbf{a}| = |\text{tr}(\mathbf{a})| \leq 3|\mathbf{a}| - 1 = 3(1) - 1 = 2$$

$$1 = |\mathbf{T}| = |\text{tr}(\mathbf{T})| \leq 3|\mathbf{T}| - 1 = 3(1) - 1 = 2$$

$$1 = |\mathbf{F}| = |\text{tr}(\mathbf{F})| \leq 3|\mathbf{F}| - 1 = 3(1) - 1 = 2$$

Inductive cases

- When $\mathbf{A} = \mathbf{B} \wedge \mathbf{C}$, our inductive hypotheses are $|\text{tr}(\mathbf{B})| \leq 3|\mathbf{B}| - 1$ and $|\text{tr}(\mathbf{C})| \leq 3|\mathbf{C}| - 1$. We reason as follows.

$$\begin{aligned}
|\text{tr}(\mathbf{B} \wedge \mathbf{C})| &= |\text{tr}(\mathbf{B}) \wedge \text{tr}(\mathbf{C})| && \text{definition of } \text{tr} \\
&= |\text{tr}(\mathbf{B})| + |\text{tr}(\mathbf{C})| + 1 && \text{definition of } |\cdot| \\
&\leq 3|\mathbf{B}| - 1 + 3|\mathbf{C}| - 1 + 1 && \text{inductive hypotheses} \\
&= 3(|\mathbf{B}| + |\mathbf{C}|) - 1 \\
&\leq 3(|\mathbf{B}| + |\mathbf{C}| + 1) - 1 \\
&= 3|\mathbf{B} \wedge \mathbf{C}| - 1 && \text{definition of } |\cdot|
\end{aligned}$$

- When $\mathbf{A} = \neg \mathbf{B}$, our inductive hypothesis is $|\text{tr}(\mathbf{B})| \leq 3|\mathbf{B}| - 1$. We reason as follows.

$$\begin{aligned}
|\text{tr}(\neg \mathbf{B})| &= |\neg \text{tr}(\mathbf{B})| && \text{definition of } \text{tr} \\
&= |\text{tr}(\mathbf{B})| + 1 && \text{definition of } |\cdot| \\
&\leq 3|\mathbf{B}| - 1 + 1 && \text{inductive hypothesis} \\
&\leq 3(|\mathbf{B}| + 1) - 1 \\
&= 3|\neg \mathbf{B}| - 1 && \text{definition of } |\cdot|
\end{aligned}$$

- Finally, when $A = B \vee C$, our inductive hypotheses are $|tr(B)| \leq 3|B| - 1$ and $|tr(C)| \leq 3|C| - 1$, and we reason as follows.

$$\begin{aligned}
|tr(B \vee C)| &= |\neg(\neg tr(B) \wedge \neg tr(C))| && \text{definition of } tr \\
&= |\neg tr(B) \wedge \neg tr(C)| + 1 && \text{definition of } |\cdot| \\
&= |\neg tr(B)| + |\neg tr(C)| + 1 + 1 && \text{definition of } |\cdot| \\
&= |tr(B)| + 1 + |tr(C)| + 1 + 1 + 1 && \text{definition of } |\cdot| \\
&\leq 3|B| - 1 + 1 + 3|C| - 1 + 1 + 1 + 1 && \text{inductive hypotheses} \\
&= 3|B| + 3|C| + 2 \\
&= 3(|B| + |C| + 1) - 1 \\
&= 3|B \vee C| - 1 && \text{definition of } |\cdot|
\end{aligned}$$

EXERCISES 3

Exercise 3.1

- (\Leftarrow) Assuming $a = a'$ and $b = b'$, the equality $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$ follows immediately.
(\Rightarrow) Assume $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$.

- If $a = b$, we have $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\} = \{\{a'\}, \{a', b'\}\}$. Therefore $\{\{a'\}, \{a', b'\}\} \subseteq \{\{a\}\}$, which means, in particular, $\{a', b'\} \in \{\{a\}\}$. Since there is only one element on the right, we must have $\{a', b'\} = \{a\}$, which implies $\{a', b'\} \subseteq \{a\}$. Again since there is only one element on the right, we must have both $a' = a$ and $b' = a$ (and, by assumption, $a = b$, so $b' = b$).
- If $a \neq b$, then $\{\{a\}, \{a, b\}\}$ contains exactly two sets, one, $\{a\}$, of size 1, and one, $\{a, b\}$, of size 2. We must have $a' \neq b'$, since otherwise $\{\{a'\}, \{a', b'\}\}$ would contain only one set. Therefore $\{a', b'\}$ has size 2 and is the only set of size 2 in $\{\{a'\}, \{a', b'\}\}$. It follows that $\{a', b'\} = \{a, b\}$, and $\{a'\} = \{a\}$. From the latter equality we can deduce $a' = a$, and therefore $\{a, b'\} = \{a, b\}$. Now consider intersection with $\{b\}$: on the right we have $\{a, b\} \cap \{b\} = \{b\}$, and on the left we must have either $\{a, b'\} \cap \{b\} = \{b'\}$ or $\{a, b'\} \cap \{b\} = \emptyset$. Since $\{b\}$ is clearly not empty, we must have $\{b\} = \{a, b\} \cap \{b\} = \{a, b'\} \cap \{b\} = \{b'\}$, and thus $b = b'$.

Exercise 3.3

- (i) By definition, whenever $p \text{id}_P q$, then in fact $p = q$. We prove the two bisimulation conditions for $p \text{id}_P q$ as follows.
- Given any p' with $p \longrightarrow p'$, we immediately have a q' , namely p' , such that both $q[=p] \longrightarrow [p' =]q'$ and $p'[=q'] \text{id}_P q'$.
 - Symmetrically, given any q' with $q \longrightarrow q'$, we immediately have a p' , namely q' , such that $p \longrightarrow p'$ and $p' \text{id}_P q'$.
- (ii) Assume R is a bisimulation on P . Suppose $p R^{-1} q$. By definition of the converse relation, this means $q R p$. Since R is a bisimulation, we infer
- $\forall p' \in P. q \longrightarrow p' \Rightarrow \exists q' \in P. p \longrightarrow q' \wedge p' R q'$, and

- $\forall q' \in P. p \longrightarrow q' \Rightarrow \exists p' \in P. q \longrightarrow p' \wedge p' R q'$.

We prove the two bisimulation conditions for $p R^{-1} q$ as follows.

- Given any p' with $p \longrightarrow p'$, we deduce from the second condition for $q R p$ that there exists a q' such that $q \longrightarrow q'$ and $q' R p'$. Observing that $q' R p'$ implies $p' R^{-1} q'$, we satisfy the first condition for $p R^{-1} q$.
- Given any q' with $q \longrightarrow q'$, we deduce from the first condition for $q R p$ that there exists a p' such that $p \longrightarrow p'$ and $q' R p'$. Observing that $q' R p'$ implies $p' R^{-1} q'$, we satisfy the second condition for $p R^{-1} q$.

(iii) Assume R and S are bisimulations on P . Suppose $p(S \circ R)q$. By definition of composition, this means there exists an m such that $p R m$ and $m S q$. Since R and S are bisimulations, we infer

- $\forall p' \in P. p \longrightarrow p' \Rightarrow \exists q' \in P. m \longrightarrow q' \wedge p' R q'$,
- $\forall q' \in P. m \longrightarrow q' \Rightarrow \exists p' \in P. p \longrightarrow p' \wedge p' R q'$,
- $\forall p' \in P. m \longrightarrow p' \Rightarrow \exists q' \in P. q \longrightarrow q' \wedge p' S q'$, and
- $\forall q' \in P. q \longrightarrow q' \Rightarrow \exists p' \in P. m \longrightarrow p' \wedge p' S q'$.

We prove the bisimulation conditions for $p(S \circ R)q$ as follows.

- Given any p' with $p \longrightarrow p'$, we deduce from the first condition for $p R m$ that there exists a q' such that $m \longrightarrow q'$ and $p' R q'$. From $m \longrightarrow q'$ and the first condition on $m S q$, we deduce that there exists a q'' such that $q \longrightarrow q''$ and $q' S q''$. Now we have $q \longrightarrow q''$ and $p'(S \circ R)q''$, so we have satisfied the first condition for $p(S \circ R)q$.
- Given any q' with $q \longrightarrow q'$, we deduce from the second condition for $m S q$ that there exists a p' such that $m \longrightarrow p'$ and $p' S q'$. From $m \longrightarrow p'$ and the second condition on $p R m$, we deduce that there exists a p'' such that $p \longrightarrow p''$ and $p'' R p'$. Now we have $p \longrightarrow p''$ and $p''(S \circ R)q'$, so we have satisfied the second condition for $p(S \circ R)q$.

We prove \sim is an equivalence relation in three parts.

Reflexivity

For all $p \in P$ we have $p \text{id}_P p$, and from (i) we know id_P is a bisimulation, therefore $p \sim p$.

Symmetry

Suppose $p \sim q$. Then there exists a bisimulation R such that $p R q$. Since R is a bisimulation, we deduce R^{-1} is a bisimulation from (ii). From $p R q$ we deduce $q R^{-1} p$, and therefore $q \sim p$.

Transitivity

Suppose $p \sim m$ and $m \sim q$. Then there are bisimulations R and S such that $p R m$ and $m S q$. From (iii) we infer that $S \circ R$ is a bisimulation. Now since $p(S \circ R)q$, we conclude $p \sim q$.

Finally, we show sim is a bisimulation. Suppose $p \sim q$. Then there exists a bisimulation R such that $p R q$. Therefore

- $\forall p' \in P. p \longrightarrow p' \Rightarrow \exists q' \in P. q \longrightarrow q' \wedge p' R q'$, and
- $\forall q' \in P. q \longrightarrow q' \Rightarrow \exists p' \in P. p \longrightarrow p' \wedge p' R q'$.

But by the definition of \sim , and the fact that R is a bisimulation, it follows that

- $\forall p' \in P. p \longrightarrow p' \Rightarrow \exists q' \in P. q \longrightarrow q' \wedge p' \sim q'$, and
- $\forall q' \in P. q \longrightarrow q' \Rightarrow \exists p' \in P. p \longrightarrow p' \wedge p' \sim q'$.

Therefore \sim is a bisimulation.

Exercise 3.4

Reflexivity

We have $n \leq n$ for all $n \in \mathbb{N}$, since every natural number divides itself.

Transitivity

Suppose n_1 divides n_2 and n_2 divides n_3 . That is, there exist factors d_1 and d_2 such that $n_2 = d_1 n_1$, and $n_3 = d_2 n_2$. Then $n_3 = d_2(d_1 n_1) = (d_2 d_1) n_1$, so n_1 divides n_3 as required.

Antisymmetry

Suppose n divides m and m divides n . That is, $n = d_1 m$ and $m = d_2 n$ for some natural numbers d_1 and d_2 . Then $n = d_1 d_2 n$, which means $d_1 d_2 = 1$. In \mathbb{N} it follows that $d_1 = d_2 = 1$, therefore $n = m$ as required.

Lubs and Glbs

Let $n, m \in \mathbb{N}$. Observe that, by definition, $\gcd(n, m)$ divides both n and m , and is the greatest natural number that does so. Similarly, $\text{lcm}(n, m)$ is the least natural number divisible by n and m . Therefore $n \vee m = \text{lcm}(n, m)$ and $n \wedge m = \gcd(n, m)$.

In this partial order, the least upper bound is commonly known as the lowest common multiple, and the greatest lower bound as the greatest common divisor.

In \mathbb{Z}

The “divides” relation gives a preorder over the integers, but antisymmetry fails to hold. In particular, an integer a and its negation $-a$ both divide one another, but are not equal.

EXERCISES 4

Exercise 4.4

We take for granted that every real number is either rational or irrational, and that every rational number is either positive or negative. Thus $\mathbb{R} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \text{Irr}$, where Irr is the set of irrational numbers. By Theorem 3.37, \mathbb{R} is uncountable. By Lemma 3.32, if \mathbb{Q}^+ , \mathbb{Q}^- , and Irr were all countable, then so would be \mathbb{R} , therefore at least one of them is uncountable. Corollary 3.30 says \mathbb{Q}^+ is countable. Lemma 3.28 implies \mathbb{Q}^- is countable as long as there is an injection from \mathbb{Q}^- to \mathbb{Q}^+ . The function $f : \mathbb{Q}^- \rightarrow \mathbb{Q}^+$ given by $f(q) = -q$ is clearly an injection: if $f(q_1) = f(q_2)$ then $-q_1 = -q_2$, hence $q_1 = q_2$. Therefore \mathbb{Q}^- is also countable, forcing the conclusion that Irr is uncountable.

Exercise 4.6

- (i) Let $a \in C$ and $a' \notin C$. By definition, $h(a) = f(a)$ and $h(a') = g^{-1}(a')$. Now suppose $h(a) = h(a')$, so $f(a) = g^{-1}(a')$, and thus $g(f(a)) = g(g^{-1}(a')) = a'$. Since $a \in C$, there exists an n such that $a \in C_n$. It follows that $g(f(a)) \in C_{n+1}$, and thus $g(f(a)) \in C$.

This is a contradiction, since we also know $g(f(a)) = a' \notin C$. Therefore we must have $h(a) \neq h(a')$.

We have shown $a \in C \wedge a' \notin C \Rightarrow h(a) \neq h(a')$. Taking the contrapositive, we obtain $h(a) = h(a') \Rightarrow a \notin C \vee a' \in C$. Instantiating the contrapositive again, we also get $h(a') = h(a) \Rightarrow a' \notin C \vee a \in C$. Now if we assume $h(a) = h(a')$, we get both $a' \notin C \vee a \in C$ and $a \notin C \vee a' \in C$. If $a \in C$ we infer $a' \in C$ from the second result, and if $a \notin C$ we infer $a' \notin C$ from the first result. Thus a and a' are either both in C or both not. If $a, a' \in C$, then $h(a) = f(a) = f(a') = h(a')$ and $a = a'$ follows from the injectivity of f . If $a, a' \notin C$, then $h(a) = g^{-1}(a) = g^{-1}(a') = h(a')$ and $a = a'$ follows from the injectivity of g^{-1} . Thus $h(a) = h(a') \Rightarrow a = a'$, which means h is injective.

(ii) We show $(g \circ f)C = C \setminus C_1$ by mutual inclusion.

$$(g \circ f)C \subseteq C \setminus C_1$$

Suppose $x \in (g \circ f)C$, which means there exist y and n such that $x = g(f(y)) \in C_n$. We infer $n \neq 1$, because C_1 does not include any element of $gB \ni g(f(y))$. Therefore $n = m+1$ for some $m \geq 1$, and $g(f(y)) \in (g \circ f)C_m$. This means there exists a $y' \in C_m$ such that $g(f(y)) = g(f(y'))$, but since g and f are both injective, we have $y = y'$, and thus $y \in C_m$. It follows that $g(f(y)) = x \in C_n$, and thus $x \in C \setminus C_1$.

$$C \setminus C_1 \subseteq (g \circ f)C$$

Suppose $x \in C \setminus C_1$, so there is an $n \neq 1$ such that $x \in C_n$. By definition, $x \in (g \circ f)C_{n-1}$. Hence $x \in (g \circ f)C$.

Now we can show that $g(b) \in C$ implies $b \in fC$. Suppose $g(b) \in C$. Since C_1 does not include gB , it follows that $g(b)$ is also in $C \setminus C_1$. Therefore $g(b) \in (g \circ f)C$. So we must have $g(b) = g(f(x))$ for some $x \in C$. Since g is injective, we have $b = f(x)$, and thus $b \in fC$.

Taking the contrapositive of the above result, we get $b \notin fC \Rightarrow g(b) \notin C$. Let $b \in B$. We proceed by cases on $b \in fC$. If $b \in fC$ then there exists an $a \in C$ such that $b = f(a)$. Therefore $h(a) = f(a) = b$. Now if $b \notin fC$ then, as we have shown, $g(b) \notin C$. Therefore $h(g(b)) = g^{-1}(g(b)) = b$. In either case b is in the range of h , therefore h is surjective.

EXERCISES 5

Exercise 5.1

Take h to be the function defined by $h(z) = (f(z), g(z))$. We verify $\pi_1(h(z)) = \pi_1(f(z), g(z)) = f(z)$ and $\pi_2(h(z)) = \pi_2(f(z), g(z)) = g(z)$ for all $z \in Z$, thus $\pi_1 \circ h = f$ and $\pi_2 \circ h = g$. Now suppose $h' : Z \rightarrow X \times Y$ also satisfies these two properties. Let $(a, b) = h'(z)$ for some arbitrary $z \in Z$. We know $\pi_1 \circ h' = f$, thus $\pi_1(a, b) = f(z)$. But $\pi_1(a, b) = a$, so we must have $a = f(z)$. Similarly, since $\pi_2 \circ h' = g$ we have $b = \pi_2(a, b) = g(z)$. Therefore $h'(z) = (f(z), g(z)) = h(z)$, so in fact $h' = h$. We conclude that h is unique.

Exercise 5.5

(i) Let $f : \mathcal{P}(X) \rightarrow X$ and let $W = \{f(Z) \in X \mid Z \subseteq X \wedge f(Z) \notin Z\}$. Clearly W is a subset of X since f returns elements of X , so we may consider $f(W)$. We proceed by cases on $f(W) \in W$. If $f(W) \in W$, then there is a Z such that $f(W) = f(Z)$, $Z \subseteq X$, and $f(Z) \notin Z$. The last condition ensures $Z \neq W$, but that means f is not injective since it sends distinct subsets W and Z to the same element. If $f(W) \notin W$, then there is no Z

such that $f(W) = f(Z)$, $Z \subseteq X$, and $f(Z) \notin Z$. But this is a contradiction, since W is one such subset. In one case, f is not injective; in the other, we reach a contradiction. Therefore, f is not injective.

(ii) Let y and z be fixed, distinct elements of Y . Define $k : \mathcal{P}(X) \rightarrow (X \rightarrow Y)$ by

$$k(s)(x) = \begin{cases} y & x \in s \\ z & x \notin s \end{cases}$$

Now suppose $k(s_1) = k(s_2)$. If $x \in s_1$ then $k(s_1)(x) = y$. Since $k(s_1) = k(s_2)$, we must also have $k(s_2)(x) = y$. By the definition of k , and because $y \neq z$, this means $x \in s_2$. Similarly, if $x \in s_2$, then $k(s_2)(x) = y = k(s_1)(x)$ so $x \in s_1$ also. Therefore $s_1 = s_2$, and thus k is injective.

(iii) Suppose $f : (X \rightarrow Y) \rightarrow X$ is an injection, and Y has at least two distinct elements. Then $k : \mathcal{P}(X) \rightarrow (X \rightarrow Y)$ as defined above is an injection. Therefore $f \circ k : \mathcal{P}(X) \rightarrow X$, being the composition of two injections, is an injection. But in (i) we showed no such injection exists. We reach a contradiction, and conclude that no such injection f exists.

EXERCISES 6

Exercise 6.1

Let R be the rules defining well-bracketed strings, and I_R the set inductively defined by them. The principle of rule induction is

$$\begin{aligned} & P([\]) \wedge \\ & (\forall x \in I_R. P(x) \Rightarrow P([x])) \wedge \\ & (\forall x, y \in I_R. P(x) \wedge P(y) \Rightarrow P(xy)) \\ & \Rightarrow \forall x \in I_R. P(x) \end{aligned}$$

Using this principle, we can show that every well-bracketed string has an equal number of left and right brackets by taking P to be the property of having an equal number of left and right brackets, and proving each of the three hypotheses above.

- Clearly $[\]$ has an equal number, 1, of each bracket type.
- Suppose x has an equal number, n , of left and right brackets. Then $[x]$ has an equal number, $n + 1$, of left and right brackets.
- Finally, suppose x has an equal number, n , and y has an equal number, m , of left and right brackets. Then xy has $n + m$ left brackets, but also $n + m$ right brackets, and thus has an equal number of each bracket type.

Therefore, every element of I_R , that is, every well-bracketed string, has an equal number of left and right brackets.

Exercise 6.6

- (i) Suppose $U \subseteq V$, and let $x \in \varphi(U)$. To show φ is monotonic is to show that $x \in \varphi(V)$. Since $x \in \varphi(U)$, there exists an $n \in U$ such that either $x = 3n/2$ and n is even, or $x = n$ and n is odd. But since $U \subseteq V$, we also have $n \in V$. Thus we either have $3n/2 \in \varphi(V)$ if n is even or $n \in \varphi(V)$ if n is odd. Therefore $x \in \varphi(V)$.
- (ii) Suppose U is a postfix point of φ . Suppose also that $n \in U$ and n is even. Since $U \subseteq \varphi(U)$, we also have $n \in \varphi(U)$. By definition of φ , there exists an $m \in U$ such that either m is even and $n = 3m/2$, or m is odd and $n = m$. But n is even, so we must have $n = 3m/2$. Thus $m = 2n/3$ is in U .
- Again supposing that U is a postfix point, we now show that U contains only odd numbers. Let $E_U = \{m \in U \mid m \text{ is even}\}$ be the subset of even numbers in U , and suppose $E_U \neq \emptyset$. Being a non-empty subset of natural numbers, E_U has a least element. Let $n \in E_U$ be the least element. Note that $n \in U$ since $E_U \subseteq U$, and n is even by definition of E_U . We deduce from the previous paragraph that $2n/3 \in U$. From the details of that paragraph, it is clear that n is divisible by 3, and thus $2n/3 = 2(n/3)$ is even. Thus $2n/3 \in E_U$. But $2n/3 < n$, which contradicts the assumption that n is the least element of E_U . Therefore the assumption that $E_U \neq \emptyset$ is untenable, and U must contain only odd numbers.
- (iii) By Theorem 5.22, we know the maximum fixed point of φ is $M = \bigcup\{S \subseteq \mathbb{N} \mid S \subseteq \varphi(S)\}$. All fixed points, including M , are postfix points. Therefore by (ii), $M \subseteq O$, where O is the set of odd natural numbers. To show $O \subseteq M$, let n be an odd number and consider the singleton $\{n\}$. By definition, $\varphi(\{n\}) = \emptyset \cup \{n\} = \{n\}$. Thus $\{n\}$ is a postfix point of φ . But M is the union of all postfix points of φ , so $\{n\} \subseteq M$, which means $n \in M$. Thus $O \subseteq M$, and hence $M = O$.
- (iv) We will show

$$\varphi(U) \subseteq U \Leftrightarrow \forall n. n \in U \wedge n \text{ is even} \Rightarrow 3n/2 \in U$$

(\Leftarrow) Suppose $n \in \varphi(U)$. Then there is an $m \in U$ such that either m is odd and $n = m$ or m is even and $n = 3m/2$. In the first case, $n \in U$ directly. In the second case, we use the assumption that if any even number m is in U then so is $3m/2$ to conclude that $n \in U$.

(\Rightarrow) Suppose $n \in U$ and n is even. Then by definition of φ , we have $3n/2 \in \varphi(U)$. Now since we assume $\varphi(U) \subseteq U$, we also have $3n/2 \in U$ as required.

We have now characterised the prefixed points of φ as those subsets of \mathbb{N} that if they contain an even number n also contain $3n/2$. The empty set is one such subset: since it contains no even numbers, the condition holds vacuously. The empty set is also clearly minimal, since it is a subset of every set, including all other prefixed points.

Theorem 5.21 shows that the least prefixed point of a monotonic function on subsets is also a fixed point. (Alternatively, it's easy to verify $\varphi(\emptyset) = \emptyset$.) Since every fixed point is a prefixed point, and the empty set is the minimum prefixed point, we conclude that the empty set is the minimum fixed point of φ .

EXERCISES 7

Exercise 7.2

Any infinite chain $\dots \prec n_i \prec \dots \prec n_1 \prec n_0$ is, by definition of \prec , also an infinite chain $\dots < n_i < \dots < n_1 < n_0 \leq 101$. But $<$ on natural numbers is well-founded, so no such infinite

chain can exist. Therefore \prec is well-founded.

Consider the following two rules, which inductively define a relation $\Downarrow \subseteq \mathbb{N}_0 \times \mathbb{N}_0$.

$$\frac{}{x \Downarrow (x - 10)} \quad (x > 100)$$

$$\frac{(x + 11) \Downarrow y \quad y \Downarrow z}{x \Downarrow z} \quad (x \leq 100)$$

We can show that \Downarrow is in fact a partial function by rule induction with the following hypothesis.

$$P(x, y) \Leftrightarrow \forall y' \in \mathbb{N}_0. x \Downarrow y' \Rightarrow y = y'$$

Assuming $x > 100$ we have $P(x, x - 10)$, since only one rule applies when $x > 100$ so the result must be $x - 10$. Assuming $x \leq 100$, our instantiated inductive hypotheses are $P(x + 11, y)$ and $P(y, z)$, and we must prove $x \Downarrow z' \Rightarrow z = z'$. Only one rule applies when $x \leq 100$, so from $x \Downarrow z'$ we infer that there exists a y' such that $(x + 11) \Downarrow y'$ and $y' \Downarrow z'$. Now from $P(x + 11, y)$ we get $y = y'$. Then from $P(y, z)$, we additionally get $z = z'$. Thus we conclude $P(x, z)$.

We have seen that the right hand side of any pair $x \Downarrow y$ in the relation is unique, so we may define a partial function by $f(x) = y$ if $x \Downarrow y$. The rules for \Downarrow ensure that f satisfies

$$f(x) = \begin{cases} x - 10 & x > 100 \\ f(f(x + 11)) & x \leq 100 \end{cases}$$

EXERCISES 8

Exercise 8.1

Exercise 8.2