R06 Exercises

Ramana Kumar (rk436)

November 23, 2010

EXERCISES 2

Exercise 2.1

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

A	B	¬B	¬A	¬B ⇒ ¬A
T	T	F	F	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

A	B	A ⇒ B
T	T	T
T	F	F
F	T	T
F	F	T

The truth values in the left two and rightmost columns are the same in both tables. It follows that $\neg \mathtt{B} \Rightarrow \neg \mathtt{A}$ and $\mathtt{A} \Rightarrow \mathtt{B}$ 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	¬B ⇒ ¬A	A ⇒ B	(¬B ⇒ ¬A) ⇔ (A ⇒ 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 $(\neg \mathtt{B} \Rightarrow \neg \mathtt{A}) \Leftrightarrow (\mathtt{A} \Rightarrow \mathtt{B})$ 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.

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

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

Exercise 2.3

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

$$\begin{aligned}
1 = |\mathtt{a}| = |tr(\mathtt{a})| \leq 3|\mathtt{a}| - 1 = 3(1) - 1 = 2 \\
1 = |\mathtt{T}| = |tr(\mathtt{T})| \leq 3|\mathtt{T}| - 1 = 3(1) - 1 = 2 \\
1 = |\mathtt{F}| = |tr(\mathtt{F})| \leq 3|\mathtt{F}| - 1 = 3(1) - 1 = 2
\end{aligned}$$

Inductive cases

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

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

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

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

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

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

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 $\{\{a'\}, \{a', b'\}\}$. Matching sets of equal sizes, 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 $\{b\}$ (keep in mind $a \neq b$): 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, the first case holds, so $\{b\} = \{a, b\} \cap \{b\} = \{a, b'\} \cap \{b\} = \{b'\}$, and thus $b = b'$.

Exercise 3.3

(i) By definition, whenever $p\,\mathsf{id}_P\,q$, then in fact $p = q$. We prove the two bisimulation conditions for $p\,\mathsf{id}_P\,q$ 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 $p'[= q']\,\mathsf{id}_P\,q'$.
- Symmetrically, given any q' with $q \longrightarrow q'$, we immediately have a p', namely q', such that $p \longrightarrow p'$ and $p'\,\mathsf{id}_P\,q'$.

(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 for $m\, S\, q$, 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 for $p\, R\, m$, 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 $p\, \mathsf{id}_P\, p$, 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, $\mathrm{lcm}(n, m)$ is the least natural number divisible by n and m. Therefore $n \vee m = \mathrm{lcm}(n, m)$ 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, negative, or zero. Thus $\mathbb{R} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\} \cup \mathrm{Irr}$, where Irr is the set of irrational numbers. By Theorem 3.37, $\mathbb{R}$ is uncountable. By Lemma 3.32, if $\mathbb{Q}^+$, $\mathbb{Q}^-$, $\{0\}$, and Irr were all countable, then so would be $\mathbb{R}$, therefore at least one of them is uncountable. Clearly $\{0\}$ is countable. 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 $f : \mathbb{Q}^- \to \mathbb{Q}^+$ 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 exists a y such that $x = g(f(y))$ and $y \in C$. By definition of C, there exists an n such that $y \in C_n$. Therefore $g(f(y)) \in (g \circ f) C_n$, and, equivalently, $x \in C_{n+1}$. It follows that $x \in C$. We also know $x \notin C_1$ because $x = g(f(b)) \in g\, B$, but C_1 does not include any element of $g\, B$. Therefore $x \in C \setminus C_1$ as required.

$C \setminus C_1 \subseteq (g \circ f)\, C$
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 if $g(b) \in C$ then $b \in f\, C$. Suppose $g(b) \in C$. Since C_1 does not include $g\, B$, 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 $b \in f\, C$.

Taking the contrapositive of the above result, we get $b \notin f\, C \Rightarrow g(b) \notin C$. We now show h is surjective. Let $b \in B$. We proceed by cases on $b \in f\, C$. If $b \in f\, C$ then there exists an $a \in C$ such that $b = f(a)$. Therefore $h(a) = f(a) = b$. Alternatively, if $b \notin f\, C$ 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 $h(z) = (f(z), g(z))$. Observe that $\pi_1(h(z)) = \pi_1(f(z), g(z)) = f(z)$ 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 $h' : Z \to X \times Y$ 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 $f : \mathcal{P}(X) \to X$ 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 $k : \mathcal{P}(X) \to (X \to Y)$ 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 $f : (X \to Y) \to X$ is an injection, and Y has at least two distinct elements. Then $k : \mathcal{P}(X) \to (X \to Y)$ as defined above is an injection. Therefore $f \circ k : \mathcal{P}(X) \to X$, 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

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

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, by definition of φ, 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 postfixed 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 postfixed 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 postfixed 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 postfixed point of φ. But M is the union of all postfixed points of φ, so $\{n\} \subseteq M$, which means $n \in M$. Thus $O \subseteq M$, and hence $M = O$.

(iv) We will show

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

($\Leftarrow$) Assume $\forall n.\ n \in U \wedge n$ is even $\Rightarrow 3n/2 \in U$. 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 $n \in U$. Thus $\varphi(U) \subseteq U$.

($\Rightarrow$) Assume $\varphi(U) \subseteq U$. 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

An infinite descending chain $\cdots \prec n_i \prec \cdots \prec n_1 \prec n_0$ is an infinite ascending chain $n_0 < n_1 < \cdots < n_i < \ldots$. The definition of $\prec$ also gives $n_1 \leq 101, n_2 \leq 101, \ldots, n_i \leq 101, \ldots$. Consider n_{102}. Whenever one natural number is strictly above another, their difference is at least 1. Clearly $n_{102} - n_0$ is the sum of all differences between the 102 pairs of adjacent numbers from n_0 to n_{102}, therefore $n_{102} - n_0 \geq 1 \times 102 \geq 102$. But we know $n_{102} \leq 101$, which is a contradiction. Therefore no such infinite chain exists. It follows that $\prec$ is well-founded.

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

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

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

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

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

We proceed by cases on $x > 100$. If $x > 100$ we immediately have $P(x, x-10)$, since only one rule applies when $x > 100$ so the result must be $x-10$. If, instead, $x \leq 100$, our instantiated inductive hypotheses are $P(x+11, y)$ and $P(y, z)$, and we must prove $P(x, z)$, that is $x \Downarrow z' \Rightarrow z = z'$. 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 y in any pair $(x, y) \in \Downarrow$ 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

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

on each $x \in \mathbb{N}_0$.

Now let $P(x)$ be the property

$$P(x) \Leftrightarrow f(x) = \begin{cases} x - 10 & x > 100 \\ 91 & x \leq 100 \end{cases}$$

We prove $\forall x \in \mathbb{N}_0.\ P(x)$ by well-founded induction on $\prec$. It suffices to show

$$\forall m.\ (\forall n \prec m.\ P(n)) \Rightarrow P(m)$$

Let $m \in \mathbb{N}_0$ and assume $\forall n \prec m.\ P(n)$. Suppose $m > 100$. Then $f(m) = m - 10$ by our characterisation of f, and hence $P(m)$ holds. Suppose instead that $m \leq 100$. Now to prove $P(m)$ is to prove $f(m) = 91$. Let $n_1 = m + 11$ and $n_2 = f(n_1)$. By our characterisation of f, we have $f(m) = f(n_2)$. We split into cases again:

- $m > 100$
  From our characterisation of f we have $f(m) = m - 10$, thus $P(m)$ holds.

- $90 \leq m \leq 100$
  From our characterisation of f we have $f(91) = f(f(91+11)) = f(f(102)) = f(102-10) = f(92) = f(f(92+11)) = f(f(103)) = f(103-10) = f(93) = f(f(93+11)) = f(f(104)) = f(104-10) = f(94) = f(f(94+11)) = f(f(105)) = f(105-10) = f(95) = f(f(95+11)) = f(f(106)) = f(106-10) = f(96) = f(f(96+11)) = f(f(107)) = f(107-10) = f(97) = f(f(97+11)) = f(f(108)) = f(108-10) = f(98) = f(f(98+11)) = f(f(109)) = f(109-10) = f(99) = f(f(99+11)) = f(f(110)) = f(110-10) = f(100) = f(f(100+11)) = f(f(111)) = f(111-10) = f(101) = 101-10 = 91$. Additionally, $f(90) = f(f(90+11)) = f(f(101)) = f(91) = 91$. Thus for all m in the required range, we have $f(m) = 91$ and $P(m)$ holds.

- $m < 90$
  Here $n_1 \leq 100$, therefore $m < n_1 \leq 101$ hence $n_1 \prec m$ and we get $P(n_1)$ as an inductive hypothesis. From $P(n_1)$ we get $f(n_1) = 91$, and therefore $n_2 = f(91)$. In the previous case we saw $f(91) = 91$, therefore $f(m) = f(n_2) = f(91) = 91$. Thus $P(m)$ holds.

This exhausts the cases, and we conclude $P(m)$ for all natural numbers m.

EXERCISES 8

Exercise 8.1

Let $\varphi : \mathcal{P}(U) \to \mathcal{P}(U)$ be monotonic.

We first show that there exists an ordinal γ such that $\varphi^\gamma(\emptyset) = \varphi^{\gamma+1}(\emptyset)$. The proof is by contradiction; in particular, we use the assumption that there is no such γ to construct a surjection from a set onto the class of ordinals. Suppose there is no such γ. In other words, for all $\gamma \in \mathbf{On}$ we have $\varphi^\gamma(\emptyset) \neq \varphi^{\gamma+1}(\emptyset)$. Since the approximations are increasing, we know $\varphi^\gamma(\emptyset) \subseteq \varphi^{\gamma+1}(\emptyset)$. Therefore we must have $\varphi^{\gamma+1}(\emptyset) \not\subseteq \varphi^\gamma(\emptyset)$. In other words, for each γ there exists an element $x \in U$ such that $x \in \varphi^{\gamma+1}(\emptyset)$ but $x \notin \varphi^\gamma(\emptyset)$. Define a function $f : \mathbf{On} \to U$ to select these elements, so that for all $\gamma \in \mathbf{On}$ we have $f(\gamma) \in \varphi^{\gamma+1}(\emptyset)$ and $f(\gamma) \notin \varphi^\gamma(\emptyset)$.

Now we show f is injective. Suppose $x = f(\alpha) = f(\beta)$, so $x \in \varphi^{\alpha+1}(\emptyset)$ and $x \in \varphi^{\beta+1}(\emptyset)$, and $x \notin \varphi^\alpha(\emptyset)$ and $x \notin \varphi^\beta(\emptyset)$. If $\alpha \in \beta$ then $\varphi^\alpha(\emptyset) \subseteq \varphi^\beta(\emptyset)$ since the approximations form an increasing chain. But then $x \in \varphi^\beta(\emptyset)$ since $x \in \varphi^\alpha(\emptyset)$. This is a contradiction, so we cannot have $\alpha \in \beta$. Symmetrically, we cannot have $\beta \in \alpha$. By Lemma 7.3 (trichotomy) it follows that $\alpha = \beta$, and therefore f is injective.

Every injective function induces a surjection from its direct image onto its domain. In the case of f, we have a function $g : f[\mathbf{On}] \to \mathbf{On}$ satisfying $f(g(x)) = x$ for all $x \in f[\mathbf{On}]$. The function g is a surjection from a subset of U onto the ordinals; in other words, it indexes the ordinals by a set. This contradicts the fact that the ordinals form a proper class. Therefore there can be no f, and we must have some ordinal γ such that $\varphi^{\gamma+1}(\emptyset) = \varphi^\gamma(\emptyset)$. Observe that this γ is a prefixed point: $\varphi(\varphi^\gamma(\emptyset)) = \varphi^{\gamma+1}(\emptyset) = \varphi^\gamma(\emptyset)$. [1]

We now show that $\varphi^\alpha(\emptyset)$ is included in all prefixed points of φ. That is,

$$\forall \alpha \in \mathbf{On}.\ \forall X \subseteq \mathcal{P}(U).\ \varphi(X) \subseteq X \implies \varphi^\alpha(\emptyset) \subseteq X$$

[1] An alternative proof: Consider $\varphi^\alpha(\emptyset)$ as a function of α, so that $\varphi^\alpha(\emptyset) : \mathbf{On} \to \mathcal{P}(U)$. We first show that this function is injective. Suppose $\varphi^{\alpha_1}(\emptyset) = \varphi^{\alpha_2}(\emptyset)$. If $\alpha_1 \in \alpha_2$ then $\varphi^{\alpha_1}(\emptyset) = \varphi^{\alpha_1+1}(\emptyset)$:

- $\varphi^{\alpha_1}(\emptyset) \subseteq \varphi^{\alpha_1+1}(\emptyset)$
  This follows directly from the facts that $\alpha_1 \in \alpha_1 + 1$ and that the approximations are increasing.
- $\varphi^{\alpha_1+1}(\emptyset) \subseteq \varphi^{\alpha_1}(\emptyset)$

We proceed by transfinite induction.

$$\begin{aligned}
&\forall \beta \in \alpha.\ \varphi^\beta(\emptyset) \subseteq X && \text{inductive hypothesis}\\
&\implies \forall \beta \in \alpha.\ \varphi(\varphi^\beta(\emptyset)) \subseteq \varphi(X) && \varphi \text{ is monotone}\\
&\implies \forall \beta \in \alpha.\ \varphi(\varphi^\beta(\emptyset)) \subseteq X && X \text{ is a prefixed point}\\
&\implies \bigcup_{\beta\in\alpha} \varphi(\varphi^\beta(\emptyset)) \subseteq X && \text{union of subsets is a subset}\\
&\implies \varphi^\alpha(\emptyset) \subseteq X && \text{definition of } \varphi^\alpha(\emptyset)
\end{aligned}$$

It follows that $\bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset) \subseteq X$, for any prefixed point X, since every set in the union is contained in X. Thus if $\bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset)$ were itself a prefixed point of φ, it would be minimal.

In fact, we can show

$$\bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset) = \varphi^\gamma(\emptyset)$$

where $\varphi^\gamma(\emptyset)$ is the prefixed point asserted to exist above.

- $\varphi^\gamma(\emptyset) \subseteq \bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset)$
  Since each set in a union is a subset of that union, and $\gamma \in \mathbf{On}$.
- $\bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset) \subseteq \varphi^\gamma(\emptyset)$
  Since $\bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset)$ is included in all prefixed points.

Therefore $\mu X.\varphi(X)$, defined as $\bigcup_{\alpha\in\mathbf{On}} \varphi^\alpha(\emptyset)$, is a set (since $\varphi^\gamma(\emptyset) \in \mathcal{P}(U)$), and is the minimal prefixed point of φ.

Exercise 8.2

(i) We show $y \in V_\alpha \implies y \subseteq V_\alpha$ for all ordinals α by transfinite induction. We show the three cases for α—zero, successor, or limit—separately. If $\alpha = 0$, then $y \in V_\alpha = V_\emptyset = \emptyset$ is false, so anything, including $y \subseteq V_\alpha$, follows. If $\alpha = \beta + 1$ is a successor, then we reason as

---

$$\begin{aligned}
\varphi^{\alpha_1+1}(\emptyset) &= \varphi(\varphi^{\alpha_1}(\emptyset))\\
&\subseteq \bigcup_{\beta\in\alpha_2} \varphi(\varphi^\beta(\emptyset)) && \text{since } \alpha_1 \in \alpha_2\\
&= \varphi^{\alpha_2}(\emptyset) = \varphi^{\alpha_1}(\emptyset) && \text{by assumption}
\end{aligned}$$

This contradicts the assumption that there is no γ with $\varphi^{\gamma+1}(\emptyset) = \varphi^\gamma(\emptyset)$, therefore we cannot have $\alpha_1 \in \alpha_2$. Symmetrically, we cannot have $\alpha_2 \in \alpha_1$. Since the ordinals are totally ordered, we must have $\alpha_1 = \alpha_2$, and therefore $\varphi^\alpha(\emptyset)$, as a function of α, is injective.

By considering the injection $\varphi^\alpha(\emptyset)$ as a function to its direct image $\varphi^{[\mathbf{On}]}(\emptyset) \subseteq \mathcal{P}(U)$, we obtain a bijection, and therefore an inverse $f : \varphi^{[\mathbf{On}]}(\emptyset) \to \mathbf{On}$. Being an inverse function, f is surjective, thus f indexes the ordinals by a set, which contradicts the fact that the ordinals form a proper class. Therefore it must be the case that there is some ordinal γ such that $\varphi^{\gamma+1}(\emptyset) = \varphi^\gamma(\emptyset)$.

follows:

$$
\begin{aligned}
& y \in V_\alpha \\
& \iff y \in \mathcal{P}(V_\beta) \\
& \iff y \subseteq V_\beta \\
& \iff \forall x \in y.\ x \in V_\beta \\
& \implies \forall x \in y.\ x \subseteq V_\beta && \text{induction hypothesis, since } \beta \in \beta + 1 \\
& \iff \forall x \in y.\ x \in \mathcal{P}(V_\beta) \\
& \iff \forall x \in y.\ x \in V_\alpha \\
& \iff y \subseteq V_\alpha
\end{aligned}
$$

If α is a limit, then we reason as follows:

$$
\begin{aligned}
& y \in V_\alpha \\
& \iff y \in \bigcup_{\beta \in \alpha} V_\beta \\
& \iff \exists \beta \in \alpha.\ y \in V_\beta \\
& \implies \exists \beta \in \alpha.\ y \subseteq V_\beta && \text{induction hypothesis} \\
& \implies y \subseteq \bigcup_{\beta \in \alpha} V_\beta \\
& \iff y \subseteq V_\alpha
\end{aligned}
$$

(ii) We show that for all ordinals α and β that $\alpha \subseteq \beta \implies V_\alpha \subseteq V_\beta$ by transfinite induction on β. We prove each of the three cases for β separately. If $\beta = 0 = \emptyset$, then $\alpha \subseteq \beta$ means $\alpha \subseteq \emptyset$, which implies $\alpha = \emptyset$. Therefore $V_\alpha = V_\emptyset \subseteq \emptyset = V_\emptyset = V_\beta$ as required. If $\beta = \gamma + 1$ is a successor ordinal, then we proceed by cases on $\gamma \in \alpha$.

- $\gamma \in \alpha$
  In this case, we can prove $\beta \subseteq \alpha$. If $x \in \beta$ then $x = \gamma$ or $x \in \gamma$ since $\beta = \gamma + 1 = \{\gamma\} \cup \gamma$. If $x = \gamma$, then $x \in \alpha$ by assumption. If $x \in \gamma$, then $x \in \alpha$ by Lemma 7.2 (ii) ($\in$-transitivity). Thus $\beta \subseteq \alpha$. Now we have $\alpha \subseteq \beta \implies \beta = \alpha$. It follows that $\alpha \subseteq \beta \implies V_\alpha \subseteq V_\beta$ as required.
- $\gamma \notin \alpha$
  We reason as follows

$$
\begin{aligned}
& \alpha \subseteq \beta \\
& \iff \alpha \subseteq \{\gamma\} \cup \gamma \\
& \iff \alpha \subseteq \gamma && \text{since } \gamma \notin \alpha \\
& \implies V_\alpha \subseteq V_\gamma && \text{induction hypothesis, since } \gamma \in \gamma + 1 \\
& \iff V_\alpha \in \mathcal{P}(V_\gamma) \\
& \iff V_\alpha \in V_\beta \\
& \implies V_\alpha \subseteq V_\beta && \text{by (i)}
\end{aligned}
$$

If β is a limit ordinal, then $V_\beta = \bigcup_{\gamma \in \beta} V_\gamma$. We split into three cases:

- $\alpha \in \beta$
  Clearly $V_\alpha \subseteq \bigcup_{\gamma \in \beta} V_\gamma = V_\beta$ when $\alpha \in \beta$.

- $\exists \gamma \in \beta.\ \alpha \subseteq \gamma$
  We reason as follows:

$$\begin{aligned}
&\alpha \subseteq \gamma \\
&\implies V_\alpha \subseteq V_\gamma && \text{induction hypothesis, since } \gamma \in \beta \\
&\implies V_\alpha \subseteq \bigcup_{\gamma \in \beta} V_\gamma \\
&\iff V_\alpha \subseteq V_\beta
\end{aligned}$$

- $\alpha \notin \beta$ and $\neg \exists \gamma \in \beta.\ \alpha \subseteq \gamma$
  In this case, we can prove $\beta \subseteq \alpha$. Suppose $\gamma \in \beta$. We cannot have $\gamma = \alpha$, because otherwise we have found a $\gamma \in \beta$, namely α, such that $\alpha \subseteq \gamma$. We also cannot have $\alpha \in \gamma$, because otherwise we would have $\alpha \in \beta$ by $\in$-transitivity, and we assumed $\alpha \notin \beta$. By trichotomy, therefore, we have $\gamma \in \alpha$ as required. Thus $\beta \subseteq \alpha$, and therefore $\alpha \subseteq \beta \implies \alpha = \beta \implies V_\alpha \subseteq V_\beta$ as required.

(iii) We show $\alpha \subseteq V_\alpha$ for all ordinals α by transfinite induction on α, treating each case separately. If $\alpha = \emptyset$ then $\alpha \subseteq V_\alpha$ is immediate. If $\alpha = \beta + 1$ is a successor ordinal, then we reason as follows:

$$\begin{aligned}
&\forall x \in \beta.\ x \subseteq \beta && \text{Lemma 7.2 (ii)} \\
&\iff \forall x \in \mathbf{On}.\ x = \beta \vee x \in \beta \implies x \subseteq \beta && \text{since } \beta \subseteq \beta \\
&\iff \forall x \in \beta + 1.\ x \subseteq \beta && \text{since } \beta + 1 = \{\beta\} \cup \beta \\
&\iff \forall x \in \beta + 1.\ x \in \mathcal{P}(\beta) \\
&\iff \beta + 1 \subseteq \mathcal{P}(\beta) \\
&\iff \alpha \subseteq V_\alpha
\end{aligned}$$

If α is a limit ordinal, then we will prove the hypothesis by contradiction. Let $\beta \in \alpha$, and suppose $\beta \notin V_\alpha$. We show $\alpha = \{\beta\} \cup \beta$.

- $\{\beta\} \cup \beta \subseteq \alpha$
  If $x \in \{\beta\} \cup \beta$ then either $x = \beta$ or $x \in \beta$. If $x = \beta$ then $x \in \alpha$ by assumption. If $x \in \beta$, then $x \in \alpha$ by $\in$-transitivity.
- $\alpha \subseteq \{\beta\} \cup \beta$
  Let $x \in \alpha$. Then:

$$\begin{aligned}
&x \in \alpha \\
&\implies x \subseteq V_x && \text{induction hypothesis} \\
&\implies x \subseteq \bigcup_{\beta \in \alpha} V_\beta \\
&\iff x \subseteq V_\alpha
\end{aligned}$$

  If $x = \beta$ or $x \in \beta$, then $x \in \{\beta\} \cup \beta$. By trichotomy, the only other case is $\beta \in x$. But if $\beta \in x$ then $\beta \in V_\alpha$, since $x \subseteq V_\alpha$. This contradicts the assumption that $\beta \notin V_\alpha$. So the case $\beta \in x$ is impossible, and we always have $x \in \{\beta\} \cup \beta$ as required.

Therefore $\alpha = \beta + 1$ is a successor ordinal. But this contradicts the assumption that α is a limit ordinal. So there can be no such β. In particular, that means if $\beta \in \alpha$ then also $\beta \in V_\alpha$. In other words, $\alpha \subseteq V_\alpha$, as required.