Exercises

Chapter 8

Sean Li [1]

Problem

(Q 8.1) Let

$$\Gamma \equiv \mathbb{Z} : *_s, \mathbb{N}^+ : *_s$$
$$\triangleright p\,(m, n, u) := \texttt{sorry} : \exists x, y : \mathbb{Z}.(m\,x + n\,y = 1)$$
$$\triangleright \text{coprime}(m, n) := \texttt{sorry} : *_p$$
$$\triangleright q\,(m, n) := \texttt{sorry} : \text{coprime}(m, n) \to \text{coprime}(n, s)$$
$$\equiv n : \mathbb{N}^+, m : \mathbb{N}^+, u : \text{coprime}(m, n)$$

Prove $\exists x, y : \mathbb{Z}.(n\,x + m\,y = 1)$ in Γ.

Solution.

Proof.

1. $q\,(m, n) : \text{coprime}(m, n) \to \text{coprime}(n, m)$

2. $q\,(m, n)\,u : \text{coprime}(n, m)$

3. $p\,(n, m, (q\,(m, n)\,u)) : \exists x, y : \mathbb{Z}.(n\,x + m\,y = 1)$

∎

(Q 8.2) Consider the following formal proof in analysis.

Proof.

1. $V : *_s$

2. $\quad u : V \subseteq \mathbb{R}$

3. $\quad\quad$ bounded-from-above$(V, u) := \exists y : R . \forall x : \mathbb{R}, (x \in V \Rightarrow x \leq y) : *_p$

4. $\quad\quad s : \mathbb{R}$

5. $\quad\quad\quad$ upper-bound$(V, u, s) := \forall x \in \mathbb{R}.(x \in V \Rightarrow x \leq s) : *_p$

$\quad\quad\quad$ least-upper-bound$(V, u, s) :=$ upper-bound$(V, u, s) \wedge$

6. $\quad\quad\quad\quad \forall x : \mathbb{R}.(x < s \Rightarrow \neg$ upper-bound$(V, u, x)) : *_p$

7. $\quad\quad v : V \neq \emptyset$

8. $\quad\quad\quad w :$ bounded-from-above(V, u)

9. $\quad\quad\quad\quad p_4 \ (V, u, w \ v) :=$ sorry $: \exists^1 \ s : \mathbb{R}.$ least-upper-bound(V, u, s)

10. $S := \left\{ x : \mathbb{R} \mid \exists n : \mathbb{R}.\left(n \in \mathbb{N} \wedge x = \frac{n}{n+1} \right) \right\}$

11. $p_6 :=$ sorry $: S \subseteq \mathbb{R}$

12. $p_7 :=$ sorry $:$ bounded-from-above(S, p_6)

13. $p_8 :=$ sorry $:$ least-upper-bound$(S, p_7, 1)$

∎

Translate the proof into a more usual format. Note $\exists^1$ denotes unique existence, that is,

$$\exists^1 \ n : \alpha. \ P \ (n) := \exists n : \alpha.(P \ (n) \wedge \neg(\exists k : \alpha.(P \ (n) \wedge k \neq n)))$$

Which lines are formalized definitions? Which of them are formalized mathematical statements?

Which constants have been introduced before the text and which are introduced within?

Underline all instantiations of parameter lists and explain accurately what has been instantiated for what, and why that is correct.

Solution. What we want to prove is that 1 is the least upper bound of the set $\left\{ x : \mathbb{R} \mid \exists n \in \mathbb{R}, \left(n \in \mathbb{N} \wedge x = \frac{n}{n+1} \right) \right\}$. (For shorter notation we use $S \equiv \left\{ \frac{n}{n+1} : n \in \mathbb{N} \right\}$)

Proof. We first give formal definitions of a set being "bounded above".

Definition A set $^{(1)}$ $V \subseteq \mathbb{R}$ $^{(2)}$ being **bounded from above** $^{(3)}$ means that there exists $y \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, x being an element of V implies that $x \leq y$.

For $s \in \mathbb{R}$ $^{(4)}$ to **be the upper bound of V** $^{(5)}$, it means that any real x being an element of V implies that $x \leq s$.

For $s \in \mathbb{R}$ to be the **least upper bound of V** $^{(6)}$, it means that s is a upper bound of V and any real number $x \in \mathbb{R}$ such that $x \leq s$ is not a upper bound of V.

Corollary 1.   Any non-empty set $V \subseteq \mathbb{R}$ bounded from above has one and only one least upper bound.

Consider the set $S := \left\{ \frac{n}{n+1} : n \in \mathbb{N} \right\}$ $^{(10)}$. Because division is closed under $\mathbb{R}$ when $n + 1 \neq 0$, $S \subseteq \mathbb{R}$ $^{(11)}$. By ...*proof omitted*..., S is bounded from above $^{(12)}$, and by ...*proof omitted*... and the fact that S is bounded from above, 1 is the least upper bound for S $^{(13)}$.   ∎

Lines (3), (5), (6), and (10) are definitions; those introduce new notions and constants, and (9), (11), (12), and (13) all statements; those construct the proof for the goal and serve as intermediate steps in the main proof.

The sets V and S, proof $u : V \subseteq \mathbb{R}$, the element $s \in \mathbb{R}$ are all defined in the proof. The sets $\mathbb{R}$ and $\mathbb{N}$, the proposition constructor $\subseteq$, the set constructor notation, real operations, and the set $\emptyset$ are all defined out of the proof.

We use blue for constants defined within the proof, and red for proofs outside.

1. $V : *_s$

2. | $u : V \subseteq \mathbb{R}$

3. | | bounded-from-above$(V, u) := \exists y : R . \forall x : \mathbb{R}, (x \in V \Rightarrow x \leq y) : *_p$

4. | | $s : \mathbb{R}$

5. | | | upper-bound$(V, u, s) := \forall x \in \mathbb{R}.(x \in V \Rightarrow x \leq s) : *_p$

     | | | least-upper-bound$(V, u, s) :=$ upper-bound$\underline{(V, u, s)^1} \wedge$

6. | | | $\quad \forall x : \mathbb{R}.\left(x < s \Rightarrow \neg \text{ upper-bound } \underline{(V, u, x)^2} \right) : *_p$

7. | | $v : V \neq \emptyset$

8. | | | $w :$ bounded-from-above$\underline{(V, u)^3}$

9. | | | | $p_4 \, (V, u, w\,v) := \texttt{sorry} : \exists^1 \, s : \mathbb{R}. \text{ least-upper-bound}\underline{(V, u, s)^4}$

10. $S := \{ x : \mathbb{R} \mid \exists n : \mathbb{R}.(n \in \mathbb{N} \wedge x = n \,/\,(n+1)) \}$

11. $p_6 := \texttt{sorry} : S \subseteq \mathbb{R}$

12. $p_7 := \texttt{sorry} : \text{bounded-from-above}\underline{(S, p_6)}^5$

13. $p_8 := \texttt{sorry} : \text{least-upper-bound}\underline{(S, p_7, 1)}^6$

In instantiation 1 on line 5, (V, u, s) states the proposition that s is an upper bound of V in order to proof that s is the least upper bound of V.

In instantiation 2 on line 6, (V, u, x) states that the proposition of x being an upper bound of V, which later on eventual leads to contradiction. This proves that no such x required exists.

In instantiation 3 on line 8, (V, u) construct a proposition of V being bounded from above.

In instantiation 4 on line 9, (V, u, s) constructed a proposition of s being the least upper bound, which was introduced as the one and only one such element of $\mathbb{R}$ that satisfies this.

In instantiation 5 on line 12, (S, p_6) constructed a proposition that S was bounded from above, and is proven by p_7.

In instantiation 6 on line 13, $(S, p_7, 1)$ constructed a proposition that S has 1 as the least upper bound, and is proven by p_8.

All of this is is correct because the types match: by the PAT paradigm it means that each evidence provided suffices to construct each next step of the proof.