Program Logics Hand-in 6

Zijun Yu 202203581

November 2023

Exercise 1

We need to show three things:

1. The operation is commutative

2. The operation is associative

3. The closure property

The first one is obvious. For second one, we need to show

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

The result of both sides is either an element in $\mathbb{N} \times \mathbb{N}$ or $\bot$. If the left side is $\bot$, it means that the second part of the pairs of the three operands are not all equal, which indicates that the right side is also $\bot$. If the left side is not $\bot$, it means that the second part of the pairs of the three operands are all equal, and the result of the left side is the sum of the first part of the three operands, which is also the result of the right side.

For the second one, we need to show
$$a \cdot b \in \mathcal{V} \Rightarrow a \in \mathcal{V}$$

Since $a \cdot b \in \mathcal{V}$, a must be some (x, n) and b be some (y, m) where $n = m$ and $x + y \leq n$. Then it is obvious that $x \leq n$, i.e. $a \in \mathcal{V}$.

Exercise 2

Because $t \equiv o \mod cap$ and $t \geq o$, t must be of the form $o + k \cdot cap$ where $k \in \mathbb{N}$. But we also know that $o \leq t < o + \text{cap}$. Substituting the expression for t, we get $o \leq o + k \times \text{cap} < o + \text{cap}$, which indicates that $k = 0$, hence we have $t = o$.

Exercise 3

Expanding the authoritative resource algebra, we need to prove:

$$((o, seq(o, i)), (o, \{o\})) \rightsquigarrow ((o + 1, seq(o + 1, i - 1)), (o + 1, \emptyset))$$

We denote the left side as m and the right side as n, by the definition of $\rightsquigarrow$, we need to prove that

$$\forall x = (\alpha, \beta).m \cdot x \in \mathcal{V} \Rightarrow n \cdot x \in \mathcal{V}$$

In order to make $m \cdot x$ valid, x must be of the form $(\bot, (\varepsilon, A))$ where A is a set of $seq(o + 1, j)$ for $0 \leq j \leq i - 1$. Let's see why this is the case.

- To see why the first part of x must be $\bot$, notice that if it is not $\bot$, the first part of $m \cdot x$ will be $\top$, making $m \cdot x$ impossible to be valid.

- We then know $m \cdot x$ must be $((o, seq(o, i)), (?_1, ?_2))$. Since $m \cdot x$ is valid, we have $?_1 \preccurlyeq o$ and $?_2 \subseteq seq(o, i)$, making o the only choice for $?_1$ and subsets of $seq(o, i)$ the only choices for $?_2$. Then, per definition of $\cdot$ on $\mathrm{EX}(\mathbb{N})_?$ and $\mathbb{P}_{fin}(\mathbb{N})$, we know α must be ε and β must be a subset of $seq(o + 1, i - 1)$.

Given $x = (\bot, (\varepsilon, A))$, we then have

$$n \cdot x = ((o + 1, seq(o + 1, i - 1)), (o + 1, A))$$

This is obviously valid as $o + 1 \preccurlyeq o + 1$ and $A \preccurlyeq seq(o + 1, i - 1)$.