Program Analysis HW 1

김도형

Exercise 1

We use structural induction on e. $[\![e]\!]$ stands for the value of e.

(Base case) $e = x$
The variables are divisible by n by assumption, so $n \mid x \Rightarrow n \mid [\![e]\!]$.

(Inductive case 1) $e = e_1 + e_2$
$[\![e_1]\!] = nk_1$, $[\![e_2]\!] = nk_2$ for some $k_1, k_2 \in \mathbb{Z}$ by the inductive hypothesis.
Then $[\![e]\!] = n(k_1 + k_2) \Rightarrow n \mid [\![e]\!]$.

(Inductive case 2) $e = e_1 \cdot e_2$
$[\![e_1]\!] = nk_1$, $[\![e_2]\!] = nk_2$ for some $k_1, k_2 \in \mathbb{Z}$ by the inductive hypothesis.
Then $[\![e]\!] = n(nk_1k_2) \Rightarrow n \mid [\![e]\!]$.

(Inductive case 3) $e = e_1\ ?\ e_2\ e_3$
By the inductive hypothesis, $n \mid [\![e_2]\!]$ and $n \mid [\![e_3]\!]$.
Since $[\![e]\!]$ is either $[\![e_2]\!]$ or $[\![e_3]\!]$, $n \mid [\![e]\!]$.

Exercise 2

Since $\forall P \in 2^A, \phi \subseteq P \Leftrightarrow \phi \sqsubseteq P$, ϕ is the bottom element.

Claim 1. *For a given chain S, $\sqcup S$ is the least upper bound of S by*

1. $\forall S_i \in S, S_i \sqsubseteq \sqcup S$
2. *If g is an upper bound of S, $\sqcup S \sqsubseteq g$*

Proof.

1. Since $\forall S_i \in S, S_i \subseteq \sqcup S$, it is trivial.
2. By definition, $\forall S_i \in S, S_i \sqsubseteq g \Leftrightarrow S_i \subseteq g \Rightarrow \sqcup S \subseteq g \Leftrightarrow \sqcup S \sqsubseteq g$

$\square$

Exercise 3

For each CPO A, B, we can get $\perp_A, \perp_B$, and by definition, $\forall \langle a, b\rangle \in A \times B, \langle \perp_A, \perp_B \rangle \sqsubseteq \langle a, b\rangle$, hence $\langle \perp_A, \perp_B \rangle$ is the bottom element.

Definition 1. For a given chain S, $S_A \coloneqq \{a \mid \langle a, b\rangle \in S\}$ (Same applies to S_B)

It is trivial that S_A, S_B are a chain, since A and B are CPOs. Also for the same reason, we can get the least upper bound of S_A, S_B as l_A, l_B respectively.

Claim 2. *For a given chain S, (l_A, l_B) is the least upper bound of S by*

1. $\forall S_i \in S, S_i \sqsubseteq (l_A, l_B)$
2. *If g is an upper bound of S, $(l_A, l_B) \sqsubseteq g$*

Proof.

1. $\forall S_i = (a_i, b_i) \in S, a_i \sqsubseteq_A l_A$, $b_i \sqsubseteq_B l_B$. Hence, $S_i \sqsubseteq (l_A, l_B)$
2. For $g = (g_A, g_B)$, if $l_A \not\sqsubseteq_A g_A$, then as A is a CPO, $g_A \sqsubset_A l_A$. Since g is an upper bound of S, $\forall a_i \in S_A, a_i \sqsubseteq_A g_A$, which makes g_A an upper bound of S_A, and it contradicts with the assumption that l_A is the least upper bound of S_A. Hence, $l_A \sqsubseteq_A g_A$. (Same applies to l_B, g_B).

$\square$

Exercise 4

Definition 2. For $f, g \in A \xrightarrow{\text{cont}} B$, $f \sqsubseteq g \Leftrightarrow \forall x \in A,\ f(x) \sqsubseteq_B g(x)$

Claim 3. *The five following claims hold:*

1. $\forall f \in A \xrightarrow{cont} B,\ f \sqsubseteq f$ *(Reflexivity)*
2. $\forall f, g \in A \xrightarrow{cont} B,\ f \sqsubseteq g \wedge g \sqsubseteq f \Rightarrow f = g$ *(Symmetry)*
3. $\forall f, g, h \in A \xrightarrow{cont} B,\ f \sqsubseteq g \wedge g \sqsubseteq h \Rightarrow f \sqsubseteq h$ *(Transitivity)*
4. $\forall S \subseteq A \xrightarrow{cont} B,\ S : chain \Rightarrow \sqcup S \in A \xrightarrow{cont} B$ *(Completeness)*
5. $\exists \bot \in A \xrightarrow{cont} B\ s.t\ \forall f \in A \xrightarrow{cont} B,\ \bot \sqsubseteq f$ *(Existence of a bottom element)*

Proof. The proofs are straightforward:

1. Choose $f \in A \xrightarrow{\text{cont}} B$. We need to show pointwise reflexivity for f.

$$\forall x \in A, f(x) \sqsubseteq_B f(x)\ (\because B \text{ is a CPO}) \Rightarrow f \sqsubseteq f\ (\because \text{definition of } \sqsubseteq)$$

2. Choose $f, g \in A \xrightarrow{\text{cont}} B$. We need to show pointwise symmetry for f, g.

$$\begin{aligned} f \sqsubseteq g \wedge g \sqsubseteq f &\Rightarrow \forall x \in A, f(x) \sqsubseteq_B g(x) \wedge g(x) \sqsubseteq_B f(x) && (\because \text{ definition of } \sqsubseteq) \\ &\Rightarrow \forall x \in A, f(x) = g(x) && (\because B \text{ is a CPO}) \\ &\Rightarrow f = g && (\because \text{ definition of function's equality}) \end{aligned}$$

3. Choose $f, g, h \in A \xrightarrow{\text{cont}} B$. We need to show pointwise transitivity for f, g, h.

$$\begin{aligned} f \sqsubseteq g \wedge g \sqsubseteq h &\Rightarrow \forall x \in A, f(x) \sqsubseteq_B g(x) \wedge g(x) \sqsubseteq_B h(x) && (\because \text{definition of } \sqsubseteq) \\ &\Rightarrow \forall x \in A, f(x) \sqsubseteq_B h(x) && (\because B \text{ is a CPO}) \\ &\Rightarrow f \sqsubseteq h && (\because \text{definition of } \sqsubseteq) \end{aligned}$$

4. We want to prove: If $S \subseteq A \xrightarrow{\text{cont}} B$ is a chain,
   (a) $\forall x \in A, S_x := \{f(x) | f \in S\} \subseteq B$ is a chain
   (b) $F := \lambda x. \sqcup S_x$ is a continuous function from A to B
   (c) F is the least upper bound of S

   Proof.

   (a) Choose $y_1, y_2 \in S_x$. Then $y_1 = f_1(x), y_2 = f_2(x)$ for some $f_1, f_2 \in S$. Since S is a chain, either $f_1 \sqsubseteq f_2$ or $f_2 \sqsubseteq f_1$. Then by definition of $\sqsubseteq$, either $y_1 = f_1(x) \sqsubseteq_B f_2(x) = y_2$ or vice versa. Therefore, S_x is a chain.

   (b) Then $\lambda x. \sqcup S_x$ is a well-defined function from A to B, since B is a CPO and S_x is a chain in B, therefore $\sqcup S_x$ exists in B. The continuity of F is proven by first showing that F is monotonic, then showing that F maps the *l.u.b.* of a chain in A to the *l.u.b.* of the image of that chain.
   First, F is monotonic:

$$\begin{aligned} x_1 \sqsubseteq_A x_2 &\Rightarrow \forall f \in S, f(x_1) \sqsubseteq_B f(x_2) && (\because f : \text{continuous} \Rightarrow f : \text{monotonic}) \\ &\Rightarrow \forall f \in S, f(x_1) \sqsubseteq_B \sqcup S_{x_2} && (\because f(x_1) \sqsubseteq_B f(x_2) \sqsubseteq_B \bigsqcup_{g \in S} g(x_2) = \sqcup S_{x_2}) \\ &\Rightarrow \sqcup S_{x_1} \sqsubseteq_B S_{x_2} && (\because \sqcup S_{x_2} \text{ is an upper bound of } S_{x_1}) \\ &\Rightarrow F(x_1) \sqsubseteq_B F(x_2) && (\because \text{by definition of } F) \end{aligned}$$

   Then if $A' \subseteq A$ is a chain, $F(A') \subseteq B$ is a chain, and $F(\sqcup A')$ is an upper bound of $F(A')$.

($\because F(A')$ is a chain because for two elements $y_1, y_2 \in F(A')$, $y_1 = F(x_1), y_2 = F(x_2)$ for some $x_1, x_2 \in A'$, and since A' is a chain, either $x_1 \sqsubseteq_A x_2$ or $x_2 \sqsubseteq_A x_1$. Then the monotonicity of F leads to the conclusion that either $y_1 \sqsubseteq_B y_2$ or vice versa. $F(\sqcup A')$ is the upper bound of $F(A')$, since $\sqcup A'$ is bigger than any element of A', and F preserves this ordering.)

Now, to show that $F(\sqcup A')$ is the least upper bound of $F(A')$, we must show that if y is an upper bound of $F(A')$, then y must be at least $F(\sqcup A')$.

$$\begin{aligned}
&y \text{ is an upper bound of } F(A') \\
&\quad\Rightarrow \forall x \in A', F(x) = \bigsqcup_{f \in S} f(x) \sqsubseteq_B y && (\because \text{by definition of an upper bound}) \\
&\quad\Rightarrow \forall x \in A', f \in S, f(x) \sqsubseteq_B y && (\because y \text{ is an upper bound of } \{f(x) | f \in S\}) \\
&\quad\Rightarrow \forall f \in S, \sqcup f(A') \sqsubseteq_B y && \begin{array}{r}(\because y \text{ is an upper bound of } f(A'), \text{ which is a} \\ \text{chain by continuity of } f, \text{ so } \exists \sqcup f(A') \sqsubseteq_B y)\end{array} \\
&\quad\Rightarrow \forall f \in S, f(\sqcup A') \sqsubseteq_B y && (\because \sqcup f(A') = f(\sqcup A') \text{ by continuity of } f) \\
&\quad\Rightarrow \bigsqcup_{f \in S} f(\sqcup A') \sqsubseteq_B y && (\because y \text{ is an upper bound of } S_{\sqcup A'}) \\
&\quad\Rightarrow F(\sqcup A') \sqsubseteq_B y && (\because \text{definition of } F)
\end{aligned}$$

Thus we have shown that F preserves chains and their *l.u.b.*s, so $F \in A \xrightarrow{\text{cont}} B$.

(c) We want to show that (1) $\forall f \in S, f \sqsubseteq F$ and (2) If g is an upper bound of S, then $F \sqsubseteq g$.
(1) $\forall f \in S, \forall x \in A, f(x) \sqsubseteq_B \bigsqcup_{g \in S} g(x) = \sqcup S_x = F(x) \Rightarrow \forall f \in S, f \sqsubseteq F$.
(2) For all $f \in S$,

$$\begin{aligned}
f \sqsubseteq g &\Rightarrow \forall f \in S, \forall x \in A, f(x) \sqsubseteq_B g(x) && (\because \text{definition of } \sqsubseteq) \\
&\Rightarrow \forall x \in A, \sqcup S_x \sqsubseteq_B g(x) && (\because g(x) \text{ is an upper bound of } S_x) \\
&\Rightarrow \forall x \in A, F(x) \sqsubseteq_B g(x) && (\because \text{definition of } F) \\
&\Rightarrow F \sqsubseteq g && (\because \text{definition of } \sqsubseteq)
\end{aligned}$$

$\therefore F = \sqcup S$ is in $A \xrightarrow{\text{cont}} B$.

5. Define $\perp := \lambda x.\perp_B$. Then $\perp$ is continuous, since it maps a chain to the chain $\{\perp_B\}$ ($\because$ by reflexivity of $\sqsubseteq_B$), and it maps the chain's *l.u.b.* to $\perp_B$, which is the *l.u.b.* of $\{\perp_B\}$.

   Since $\forall f \in A \xrightarrow{\text{cont}} B, x \in A, \perp(x) = \perp_B \sqsubseteq_B f(x) \Rightarrow \forall f \in A \xrightarrow{\text{cont}} B, \perp \sqsubseteq f$, we proved the existence of a bottom element in $A \xrightarrow{\text{cont}} B$.

□

Exercise 5

1. The fixpoint x_0 must satisfy $x_0 = 1$, so the only fixpoint is 1.
2. The fixpoint x_0 must satisfy $x_0 = x_0$, so the fixpoints are x ($x \in \mathbb{N}$).
3. The fixpoint x_0 must satisfy $x_0 = x_0 + 1$, so the unique fixpoint must be ∞.
4. The fixpoint f_0 must satisfy $f_0 = \lambda x.\texttt{if } x = 0 \,?\, 0 : x + f_0(x-1)$. We can prove that

   $$f_0(x) = \frac{x(x+1)}{2}$$

   by mathematical induction. This also means that the fixpoint is unique.

   Proof. For $x = 0$, $f_0(0) = 0$. Assuming that the equation holds for some $x \geq 0$,

   $$f_0(x+1) = x + 1 + f_0(x) = x + 1 + \frac{x(x+1)}{2} = \frac{(x+1)(x+2)}{2}$$

   Therefore the equation holds for all $x \in \mathbb{N}$. □

We can confirm that $f_0 = \lambda x.\dfrac{x(x+1)}{2}$ is indeed the fixpoint by calculation.

5. The fixpoint X_0 must satisfy $X_0 = \{\epsilon\} \cup \{\star x \mid x \in X_0\}$. Similar to the case above, we can prove that $\forall i \geq 0, \star^i \in X_0$, so $S \subseteq X_0 \subseteq S \Rightarrow X_0 = S$ by mathematical induction.

   Proof. For $i = 0$, $\star^0 = \epsilon \in \{\epsilon\} \subseteq \{\epsilon\} \cup \{\star x \mid x \in X_0\} = X_0$. Assuming that the equation holds for some $i \geq 0$, $\star^{i+1} \in \{\star x \mid x \in \{\star^i\}\} \subseteq \{\star x \mid x \in X_0\} \subseteq X_0$ by the inductive hypothesis, so the equation also holds for all $i \geq 0$. ☐

   We can confirm that S is indeed the fixpoint by calculation.

Exercise 6

Claim 1. *For a finite collection $\{A_i\}_{0 \leq i \leq n}$ of subsets of S,* $f\left(\bigcup_{0 \leq i \leq n} A_i\right) = \bigcup_{0 \leq i \leq n} f(A_i)$.

Proof. We prove by mathematical induction on n.

When $n = 0$, the equality is trivial by $f(A_0) = f(A_0)$.

When we assume that the claim holds for some $n (\geq 0)$,

$$f\left(\bigcup_{0 \leq i \leq n+1} A_i\right) = f\left(\bigcup_{0 \leq i \leq n} A_i \cup A_{n+1}\right) = f\left(\bigcup_{0 \leq i \leq n} A_i\right) \cup f(A_{n+1}) = \bigcup_{0 \leq i \leq n} f(A_i) \cup f(A_{n+1}) = \bigcup_{0 \leq i \leq n+1} f(A_i).$$

The second equality holds because of $f(x \cup y) = f(x) \cup f(y)$, and the third equality holds because of the inductive hypothesis. Since the claim holds also for $n+1$, the claim holds for all $n \geq 0$. ☐

Claim 2. *For a countable collection $\{A_i\}_{i \geq 0}$ of subsets of S,* $f\left(\bigcup_{i \geq 0} A_i\right) = \bigcup_{i \geq 0} f(A_i)$.

Proof. We first define $B_i := \bigcup_{0 \leq j \leq i} A_i$ for $i \geq 0$. Then $\{B_i\}_{i \geq 0}$ is a chain in 2^S, since $i \leq j \Rightarrow B_i \subseteq B_j$, so for any two elements of the chain we can compare the elements.

Since f is continuous, $f\left(\bigcup_{i \geq 0} B_i\right) = \bigcup_{i \geq 0} f(B_i)$. But $\bigcup_{i \geq 0} B_i = \bigcup_{i \geq 0} \bigcup_{0 \leq j \leq i} A_j = \bigcup_{i \geq 0} A_i$. Due to Claim 1, we have: $f(B_i) = \bigcup_{0 \leq j \leq i} f(A_j)$, so $\bigcup_{i \geq 0} f(B_i) = \bigcup_{i \geq 0} \bigcup_{0 \leq j \leq i} f(A_j) = \bigcup_{i \geq 0} f(A_i)$. Hence, $f\left(\bigcup_{i \geq 0} A_i\right) = \bigcup_{i \geq 0} f(A_i)$. ☐

Now we can prove the main claim.

Claim 3. $\mathsf{lfp}(\lambda x.A \cup f(x)) = \bigcup_{i \geq 0} f^i(A) =: \alpha$, *that is:*

1. *α is a fixpoint of $\lambda x.A \cup f(x)$*
2. *If x_0 is a fixpoint of $\lambda x.A \cup f(x)$, then $\alpha \subseteq x_0$*

Proof.

1. Plugging in α to the fixpoint equation leads to:

$$\begin{aligned}
(\lambda x.A \cup f(x))\alpha &= A \cup f(\alpha) \\
&= A \cup f\left(\bigcup_{i \geq 0} f^i(A)\right) \\
&= A \cup \bigcup_{i \geq 0} f(f^i(A)) && (\because \text{Claim 2}) \\
&= f^0(A) \cup \bigcup_{i \geq 0} f^{i+1}(A) \\
&= \bigcup_{i \geq 0} f^i(A) = \alpha
\end{aligned}$$

2. We first prove that $\forall i \geq 0, f^i(A) \subseteq x_0$ by mathematical induction.
   For $i = 0$, $f^0(A) = A \subseteq A \cup f(x_0) = x_0$.
   Assuming that the claim holds for some $i \geq 0$, $f^{i+1}(A) = f(f^i(A)) \subseteq f(x_0) \subseteq A \cup f(x_0) = x_0$.
   $f(f^i(A)) \subseteq f(x_0)$ holds, since $f^i(A) \subseteq x_0$ by the inductive hypothesis and f is continuous. Then since f is monotonic, f preserves the order between $f^i(A)$ and x_0.
   Now, since $\forall i \geq 0, f^i(A) \subseteq x_0$, we have: $\alpha = \bigcup_{i \geq 0} f^i(A) \subseteq x_0$.

□

Exercise 7

1. We already showed in Exercise 5 that the only fixpoint is $x_0 = 1$, so it is the least fixpoint.
2. $(\lambda x.x)\bot = \bot$, and $\forall x \in \mathbb{N}_\bot, \bot \subseteq x$, so $\bot$ is the least fixpoint.
3. If f_0 is a fixpoint, then $f_0 = \lambda x.\texttt{if}\ x = 0\ ?\ 0\ :\ x + f_0(x-1)$. Then $f_0(\bot) = \bot + f_0(\bot - 1) = \bot$, and $f_0(x) = \dfrac{x(x+1)}{2}$ when $x \in \mathbb{N}$ by mathematical induction exactly as in Exercise 5. Thus $f_0 = \lambda x.\texttt{if}\ x = \bot ? \bot : \dfrac{x(x+1)}{2}$ is a fixpoint, since $\forall x \in \mathbb{N}_\bot, f_0(x) = (\lambda x'.\texttt{if}\ x' = 0\ ?\ 0\ :\ x' + f_0(x'-1))\ x$ holds. Since the fixpoint is unique, f_0 must be the least fixpoint.
4. We already showed in Exercise 5 that the only fixpoint is S, so it is the least fixpoint.

Exercise 8

1. Definition of $[\![\cdot]\!] : \mathsf{Pgm} \to (2^G \to 2^G)$
   $[\![\mathsf{init}(\mathcal{R})]\!]A := \mathcal{R}$
   $[\![\mathsf{translation}(u,v)]\!]A := \{\mathsf{trans}(p,(u,v)) \mid p \in A\}$
   $[\![\mathsf{rotation}(u,v,\theta)]\!]A := \{\mathsf{rotate}(p,(u,v,\theta)) \mid p \in A\}$
   $[\![p_1;p_2]\!]A := [\![p_2]\!]([\![p_1]\!]A)$, that is, $[\![p_1;p_2]\!] := [\![p_2]\!] \circ [\![p_1]\!]$.
   $[\![\{p_1\}\ \mathsf{or}\ \{p_2\}]\!]A := [\![p_1]\!]A \cup [\![p_2]\!]A$, that is, $[\![\{p_1\}\ \mathsf{or}\ \{p_2\}]\!] := [\![p_1]\!] \cup [\![p_2]\!]$, when $\cup$ means pointwise union.
   $[\![\mathsf{iter}\{p\}]\!]A := \bigcup_{i \geq 0} [\![p]\!]^i A$, that is, $[\![\mathsf{iter}\{p\}]\!] := \bigcup_{i \geq 0} [\![p]\!]^i$.
2. Calculation of the given program

$$
\begin{aligned}
&[\![\mathsf{iter}\{\{\mathsf{translation}(1,0)\}\ \mathsf{or}\ \{\mathsf{translation}(1,1)\}\}]\!]([\![\mathsf{init}\{(0,0),(0,1)\}]\!]A) && (\because p_1;p_2)\\
&= [\![\mathsf{iter}\{\{\mathsf{translation}(1,0)\}\ \mathsf{or}\ \{\mathsf{translation}(1,1)\}\}]\!]\{(0,0),(0,1)\} && (\because \mathsf{init})\\
&= \bigcup_{i \geq 0} [\![\{\mathsf{translation}(1,0)\}\ \mathsf{or}\ \{\mathsf{translation}(1,1)\}]\!]^i\{(0,0),(0,1)\} && (\because \mathsf{iter})\\
&= \bigcup_{i \geq 0} \bigcup_{j=0}^{i} ([\![\mathsf{translation}(1,0)]\!]^j [\![\mathsf{translation}(1,1)]\!]^{i-j}\{(0,0),(0,1)\})\\
&(\because \text{translation commute over } \cup)\\
&= \bigcup_{i \geq 0} \bigcup_{j=0}^{i} ([\![\mathsf{translation}(i,i-j)]\!]\{(0,0),(0,1)\})\\
&= \bigcup_{0 \leq j \leq i} \{(i,j),(i,j+1)\}\\
&= \{(i,j) \in \mathbb{Z}^2 \mid i \geq 0, 0 \leq j \leq i+1\}
\end{aligned}
$$

   So $[\![p]\!]$ is the constant function $\lambda A.\{(i,j) \in \mathbb{Z}^2 \mid i \geq 0, 0 \leq j \leq i+1\}$.

Exercise 9

Claim 1. $\gamma(x) \dot{+} \gamma(y) = \gamma(x +^{\#} y)$

Proof. Since the abstract domain is finite, we can exhaustively check all cases for (x, y).

$(\bot, \_) : \gamma(x) \dot{+} \gamma(y) = \emptyset \dot{+} \gamma(y) = \{x' + y' \mid x' \in \emptyset, y' \in \gamma(y)\} = \emptyset = \gamma(\bot) = \gamma(\bot +^{\#} y) = \gamma(x +^{\#} y)$
$(\top, \_) : \gamma(x) \dot{+} \gamma(y) = \mathbb{Z} \dot{+} \gamma(y) = \mathbb{Z} = \gamma(\top) = \gamma(\top +^{\#} y) = \gamma(x +^{\#} y) \qquad (y \neq \bot)$
$(0, 0) : \gamma(x) \dot{+} \gamma(y) = 2\mathbb{Z} \dot{+} 2\mathbb{Z} = \{x' + y' \mid x' \in 2\mathbb{Z}, y' \in 2\mathbb{Z}\} = \{2(x'' + y'') \mid x'' \in \mathbb{Z}, y'' \in \mathbb{Z}\} = 2\mathbb{Z}$
$= \gamma(0) = \gamma(0 +^{\#} 0) = \gamma(x +^{\#} y)$
$(1, 1) : \gamma(x) \dot{+} \gamma(y) = (2\mathbb{Z} + 1) \dot{+} (2\mathbb{Z} + 1) = \{x' + y' \mid x' \in 2\mathbb{Z} + 1, y' \in 2\mathbb{Z} + 1\}$
$= \{2(x'' + y'' + 1) \mid x'' \in \mathbb{Z}, y'' \in \mathbb{Z}\} = 2\mathbb{Z} = \gamma(0) = \gamma(1 +^{\#} 1) = \gamma(x +^{\#} y)$
$(0, 1) : \gamma(x) \dot{+} \gamma(y) = 2\mathbb{Z} \dot{+} (2\mathbb{Z} + 1) = \{x' + y' \mid x' \in 2\mathbb{Z}, y' \in 2\mathbb{Z} + 1\} = \{2(x'' + y'') + 1 \mid x'' \in \mathbb{Z}, y'' \in \mathbb{Z}\}$
$= 2\mathbb{Z} + 1 = \gamma(1) = \gamma(0 +^{\#} 1) = \gamma(x +^{\#} y)$
Other cases are covered by the commutativity of $+^{\#}$. ☐

Claim 2. $\gamma(x) = \dot{-}\gamma(x)$

Proof. Since the abstract domain is finite, we can exhaustively check all cases for x.

$\bot : \gamma(\bot) = \emptyset = \{-s \mid s \in \emptyset\} = \dot{-}\emptyset = \dot{-}\gamma(\bot)$
$\top : \gamma(\top) = \mathbb{Z} = \{z \mid z \in \mathbb{Z}\} = \{-(-z) \mid z \in \mathbb{Z}\} = \{-w \mid w \in \mathbb{Z}\} = \dot{-}\mathbb{Z} = \dot{-}\gamma(\top)$
$0 : \gamma(0) = 2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\} = \{-2(-z) \mid z \in \mathbb{Z}\} = \{-2w \mid w \in \mathbb{Z}\} = \dot{-}2\mathbb{Z} = \dot{-}\gamma(0)$
$1 : \gamma(1) = 2\mathbb{Z}{+}1 = \{2z{+}1 | z \in \mathbb{Z}\} = \{-(2(-z{-}1){+}1) | z \in \mathbb{Z}\} = \{-(2w{+}1) | w \in \mathbb{Z}\} = \dot{-}(2\mathbb{Z}{+}1) = \dot{-}\gamma(1)$ ☐

Claim 3. $\gamma(x) \cup \gamma(y) = \gamma(x \cup^{\#} y)$

Proof. Since the abstract domain is finite, we can exhaustively check all cases for (x, y).

$(\bot, \_) : \gamma(\bot \cup^{\#} y) = \gamma(y) = \emptyset \cup \gamma(y) = \gamma(\bot) \cup \gamma(y)$
$(\top, \_) : \gamma(\top \cup^{\#} y) = \gamma(\top) = \mathbb{Z} = \mathbb{Z} \cup \gamma(y) = \gamma(\top) \cup \gamma(y) \qquad (y \neq \bot)$
$(x, x) : \gamma(x \cup^{\#} x) = \gamma(x) = \gamma(x) \cup \gamma(x)$
$(0, 1) : \gamma(0 \cup^{\#} 1) = \gamma(\top) = \mathbb{Z} = 2\mathbb{Z} \cup (2\mathbb{Z} + 1) = \gamma(0) \cup \gamma(1)$
Other cases are covered by the commutativity of $\cup^{\#}$. ☐

Now we can prove our main claim.

Claim 4. *For any program C, $S \subseteq \gamma(s^{\#}) \Rightarrow [\![C]\!]S \subseteq \gamma([\![C]\!]^{\#} s^{\#})$*

Proof. We use structural induction on C.

(Base case 1) $C = \mathsf{store}\ E$

To prove $S \subseteq \gamma(s^{\#}) \Rightarrow [\![E]\!]S \subseteq \gamma([\![E]\!]^{\#} s^{\#})$, we use structural induction on E.

(Base case 1) $E = n$

$[\![E]\!]S = \{n\}$, and $[\![E]\!]^{\#} s^{\#} = n \bmod 2 \Rightarrow \gamma([\![E]\!]^{\#} s^{\#}) = \{m \mid n \equiv m \pmod 2\}$.
Since $n \equiv n \pmod 2$, $[\![E]\!]S \subseteq \gamma([\![E]\!]^{\#} s^{\#})$.

(Base case 2) $E = \mathsf{load}$

$[\![E]\!]S = S$, and $[\![E]\!]^{\#} s^{\#} = s^{\#}$, so directly we can see that $[\![E]\!]S = S \subseteq \gamma(s^{\#}) = \gamma([\![E]\!]^{\#} s^{\#})$.

(Inductive case 1) $E = E_1 + E_2$

$$\begin{aligned}
[\![E]\!]S &= [\![E_1]\!]S \dot{+} [\![E_2]\!]S \\
&\subseteq \gamma([\![E_1]\!]^{\#} s^{\#}) \dot{+} \gamma([\![E_2]\!]^{\#} s^{\#}) && (\because [\![E_i]\!]S \subseteq \gamma([\![E_i]\!]^{\#} s^{\#}) \text{ by the inductive hypothesis,} \\
& && \text{and } A_i \subseteq B_i \Rightarrow A_1 \dot{+} A_2 \subseteq B_1 \dot{+} B_2) \\
&= \gamma([\![E_1]\!]^{\#} s^{\#} +^{\#} [\![E_2]\!]^{\#} s^{\#}) && (\because \text{Claim 1}) \\
&= \gamma([\![E_1 + E_2]\!]^{\#} s^{\#})
\end{aligned}$$

(Inductive case 2) $E = -E_1$

$$\begin{aligned}
[\![E]\!]S &= [\![-E_1]\!]S \\
&= \dot{-}[\![E_1]\!]S \\
&\subseteq \dot{-}\gamma([\![E_1]\!]^{\#}s^{\#}) && (\because [\![E_i]\!]S \subseteq \gamma([\![E_i]\!]^{\#}s^{\#}) \text{ by the inductive hypothesis, and } A \subseteq B \Rightarrow \dot{-}A \subseteq \dot{-}B) \\
&= \gamma([\![E_1]\!]^{\#}s^{\#}) && (\because \text{Claim 2}) \\
&= \gamma([\![-E_1]\!]^{\#}s^{\#})
\end{aligned}$$

$\therefore S \subseteq \gamma(s^{\#}) \Rightarrow [\![C]\!]S = [\![E]\!]S \subseteq \gamma([\![E]\!]^{\#}s^{\#}) = \gamma([\![C]\!]^{\#}s^{\#})$

(Base case 2) $C = \mathsf{skip}$

$[\![C]\!]S = S \subseteq \gamma(s^{\#}) = \gamma([\![C]\!]^{\#}s^{\#})$

(Inductive case 1) $C = C_1 \;\mathsf{or}\; C_2$

$$\begin{aligned}
[\![C]\!]S &= [\![C_1]\!]S \cup [\![C_2]\!]S \\
&\subseteq \gamma([\![C_1]\!]^{\#}s^{\#}) \cup \gamma([\![C_2]\!]^{\#}s^{\#}) && (\because [\![C_i]\!]S \subseteq \gamma([\![C_i]\!]^{\#}s^{\#}) \text{ by the inductive hypothesis}) \\
&= \gamma([\![C_1]\!]^{\#}s^{\#} \cup^{\#} [\![C_2]\!]^{\#}s^{\#}) && (\because \text{Claim 3}) \\
&= \gamma([\![C_1 \;\mathsf{or}\; C_2]\!]^{\#}s^{\#}) \\
&= \gamma([\![C]\!]^{\#}s^{\#})
\end{aligned}$$

(Inductive case 2) $C = C_1; C_2$

$[\![C]\!]S = [\![C_2]\!]([\![C_1]\!]S)$. Let $S_1 = [\![C_1]\!]S$, and $s_1^{\#} = [\![C_1]\!]^{\#}s^{\#}$, so that we may write $[\![C]\!]S = [\![C_2]\!]S_1$ and $[\![C]\!]^{\#}s^{\#} = [\![C_2]\!]^{\#}s_1^{\#}$.

Now,

$$\begin{aligned}
S \subseteq \gamma(s^{\#}) &\Rightarrow S_1 \subseteq \gamma(s_1^{\#}) && (\because \text{by the inductive hypothesis for } C_1) \\
&\Rightarrow [\![C_2]\!]S_1 \subseteq \gamma([\![C_2]\!]^{\#}s_1^{\#}) && (\because \text{by the inductive hypothesis for } C_2) \\
&\Rightarrow [\![C]\!]S \subseteq \gamma([\![C]\!]^{\#}s^{\#}) && (\because \text{by definition of } S_1, s_1^{\#})
\end{aligned}$$

$\square$