Exercise 05

Wang, Haotian 421723

Li, Kehao, 461037

Wang, Yinghao 460777

Tao, Tingxu 453995

Exercise 1 (Calculating the Weakest Precondition) **25P**

For each of the GCL programs P, compute $wp[\![P]\!](f)$ for postcondition $f \in \mathbb{P}$.

(a) [5P]

$$P: \quad x := x_0;\ y := y_0;\ z := x;\ x := y;\ y := z$$
$$f: \quad (x = y_0) \wedge (y = x_0)$$

$wp[\![P]\!](f) = true.$

(b) [5P]

$$P: \quad \texttt{if } (x < y)\ \{\ z := y - x;\ \}\ \texttt{else}\ \{\ z := x - y;\ \}$$
$$f: \quad z = |x - y|$$

$wp[\![P]\!](f) = true$

(c) [10P]

$$P: \quad \texttt{while } (x \neq 5 \wedge x \neq 0)\ \{\ x := x - 1\ \}$$
$$f: \quad x = 5$$

$wp[\![P]\!](f) = (x \geq 5) \wedge (x \in \mathbb{Z})$

(c) [10P]

$$P: \quad \texttt{while } (x \neq 5 \wedge x \neq 0)\ \{\ x := x - 1\ \}$$
$$f: \quad x = 5$$

(d) [5P] Compute $wlp[\![P]\!](f)$ for the program P and postcondition f of part (c). What are the preconditions such that P diverges?

$wlp[\![P]\!](f) = (x \geq 5) \vee (x < 0) \vee (x \notin \mathbb{Z})$

Preconditions such that P diverges: $(x < 0) \vee (x \notin \mathbb{Z})$.

are the preconditions such that P diverges.

Exercise 2 (Matching Properties) $\boxed{25P}$

Match each of the following statements to one of the statements below, where P and Q are GCL programs and $f, g \in \mathbb{P}$ are postconditions.

(a) $wlp[\![P]\!](f) = \text{true}$

(b) $\neg wp[\![P]\!](\text{true}) = \text{false}$ $\quad wp[\![P]\!](\text{true}) = \text{true}$.

(c) $wlp[\![P]\!](\text{false})$

(d) $wp[\![P]\!](\text{true}) \implies wp[\![Q]\!](\text{true})$

(e) $wp[\![P]\!](g)$, where $wp[\![Q]\!](f) = g$

(f) $wlp[\![P]\!](f \wedge g) = wlp[\![P]\!](f) \wedge wlp[\![P]\!](g)$

1. The precondition such that the program diverges.
2. This statement is false.
3. The precondition of program $P; Q$ with postcondition f.
4. For any initial state, the program either diverges or the final state satisfies the predicate f.
5. The program always terminates.
6. If program P terminates for an initial state then also program Q terminates for this state.

(a). – 4.

(b). – 5

(c). – 1

(d). – 6

(e). – 3

(f) – 2

Exercise 3 **(Non-deterministic Choice)** $\boxed{\textbf{25P}}$

Recall from lecture 7, slide 7 that Dijkstra's original guarded command language contained a *non-deterministic* choice statement $C_1 \Box C_2$, which we omitted so far. Intuitively, this statement executes either program C_1 or program C_2, but there is *no* probability distribution underlying this choice. Two common models to deal with non-determinism are known as *demonic non-determinism* and *angelic non-determinism*, i.e. we either choose the "worst" (demonic) or "best" (angelic) option. In terms of weakest (liberal) preconditions, this translates to taking a conjunction (demonic) or a disjunction (angelic) of the predicates. We call the corresponding transformers *dwp*, *awp*, *dwlp*, and *awlp*, respectively.

More formally, for $F \in \mathbb{P}$, we define

$$\begin{aligned}
dwp[\![C_1 \Box C_2]\!](F) &= dwp[\![C_1]\!](F) \wedge dwp[\![C_2]\!](F) && \text{(demonic wp)}\\
dwlp[\![C_1 \Box C_2]\!](F) &= dwlp[\![C_1]\!](F) \wedge dwlp[\![C_2]\!](F) && \text{(demonic wlp)}\\
awp[\![C_1 \Box C_2]\!](F) &= awp[\![C_1]\!](F) \vee awp[\![C_2]\!](F) && \text{(angelic wp)}\\
awlp[\![C_1 \Box C_2]\!](F) &= awlp[\![C_1]\!](F) \vee awlp[\![C_2]\!](F) && \text{(angelic wlp)}
\end{aligned}$$

For all other GCL statements, both *dwp* and *awp* coincide with *wp*. Analogously, *dwlp* and *awlp* coincide with *wlp*.

Prove that for all GCL programs C (including non-deterministic choice) and $F \in \mathbb{P}$,

$$dwp[\![C]\!](F) \quad = \quad \neg awlp[\![C]\!](\neg F) \quad (*)$$

For all programs C_1 and C_2, it holds that:

$$dwp[\![C_1 \Box C_2]\!](F) = dwp[\![C_1]\!](F) \wedge dwp[\![C_2]\!](F)$$

$$\begin{aligned}
\neg awlp[\![C_1 \Box C_2]\!](\neg F) &= \neg\left(awlp[\![C_1]\!](\neg F) \vee awlp[\![C_2]\!](\neg F)\right)\\
&= \neg awlp[\![C_1]\!](\neg F) \wedge \neg awlp[\![C_2]\!](\neg F).
\end{aligned}$$

If we can prove that $(*)$ holds for all deterministic programs C, then it should also hold for non-deterministic program C by induction.

For a deterministic program C, $dwp[\![C]\!](F) = wp[\![C]\!](F)$, $awlp[\![C]\!](\neg F) = wlp[\![C]\!](\neg F)$.

so we need to prove $\quad wp[\![C]\!](F) = \neg wlp[\![C]\!](\neg F) \quad (**)$

On the one hand, $\neg wlp[\![C]\!](\neg F) = \neg\left(wp[\![C]\!](\neg F) \vee \neg wp[\![P]\!](true)\right)$

On the other hand, for each initial state s, the program C either does not terminates, or terminates in state t, and either $t \models F$, or $t \models \neg F$,

so $(**)$ always holds.

Therefore, $(*)$ holds for all programs C.