Review Q & A - Apr. 8

Final Exam

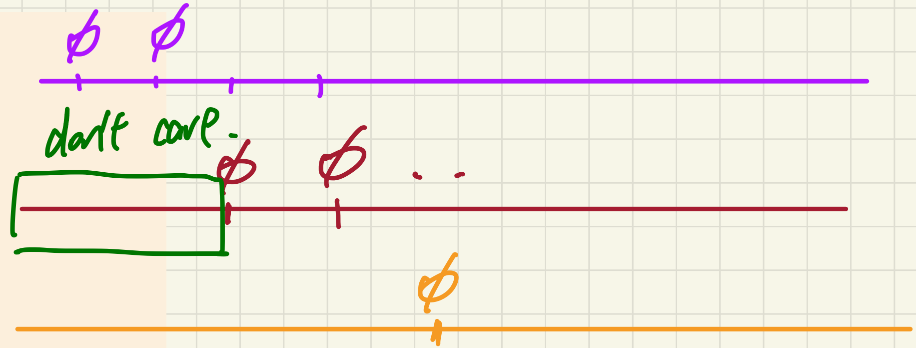
strongest

1. G phi
2. FG phi
3. F phi
4. G phi => FG phi

weakest

true

true.



$$\pi \models F\,\underbrace{\boxed{(\phi_1 \,\mathcal{U}\, \phi_2)}}_{\phi_3}$$

apply def. of $\mathcal{U}$ operator

↳ result should be nested quantifications.

$$\exists i \cdot i \geq 1 \wedge \pi^i \models \phi_3$$

To be released after review session.

$$\exists k \cdot k \geq 1 \wedge \left(\exists i \cdot i \geq k \wedge \left(\begin{array}{l} \pi^i \models \phi_2 \\ \wedge \\ \forall j \cdot k \leq j \leq i-1 \Rightarrow \pi^j \models \phi_1 \end{array} \right) \right)$$

```
if (B1) {
    if (B2) { ______ }
    else    { ______ }
}
else {
    if (B3) { ______ }
    else    { ______ }
}
```

→

```
if (B1 ∧ B2) { ______ }
else if (B1 ∧ ¬B2) { ______ }
else if (¬B1 ∧ B3) { ______ }
else if (¬B1 ∧ ¬B3) { ______ }
```

precedence

tightest $\neg$

$\wedge$

$\vee$

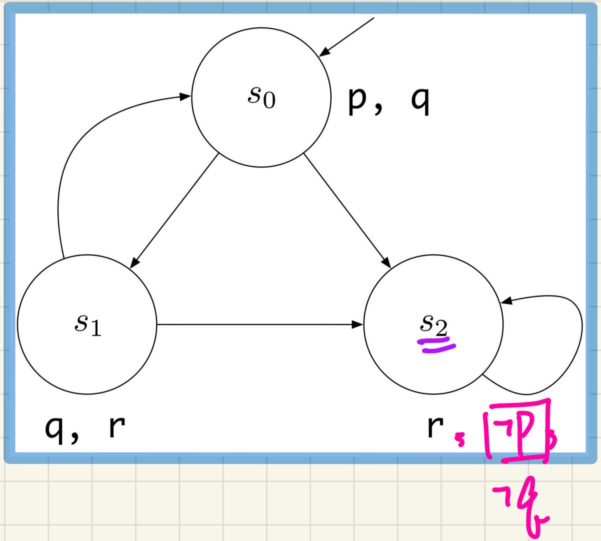
$\Rightarrow$

$\equiv$

Lab 4

Pay attention to the invariant property being checked.

Model Satisfaction: Exercises (7.1)



$s \models \phi \Leftrightarrow$ **all π starting at s, $\pi \models \phi$**

$\cancel{s_0}$ $s_2 \models \boxed{p \ U \ r}$

True

(1) r^{I}

$\boxed{s_2} \to s_2 \to s_2 \to \cdots$

go back to some earlier exercise on U. op.

why p is sat. from state I to I-1

(2) $\neg(G\, p)$

$\cancel{s_0}$ $s_2 \models p \ W \ r$

True

$\cancel{s_0}$ $s_2 \models r \ R \ p$

False

Witness:

$r \to r \to r \to \ldots$

(1) when r is sat., p is never sat.

Exercise: What if we change the LHS to s_2?

I smoke

$\boxed{\phi_1} \;\, \mathcal{U} \;\, \phi_2$

vs.

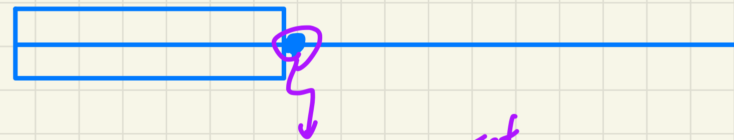
$\phi_2 \;\, \mathcal{R} \;\, \boxed{\phi_1}$

I smoke

I was zz

$\mathcal{U}$

I was zz



at this point where ϕ_2 is true should ϕ_1 be true at the same time?

↳ yes → $\mathcal{R}$

no → $\mathcal{U}$

$\{B \wedge I\}\ S_{body}\ \{I\} \rightarrow wp(S_{body}, I)$

Solution to Part (d)

We first calculate the wp for the loop body to maintain the LI:

$$
\begin{aligned}
& wp(\texttt{if(input[i] > result) \{ result := input[i] \}; i := i + 1;}, \boxed{\forall j \bullet j \in 1 \mathinner{..} i-1 \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]}) \\
= & \ \{wp \texttt{ rule for sequential composition }\} \\
& wp(\texttt{if(input[i] > result) \{ result := input[i] \}}, \boxed{wp(\texttt{i := i + 1}, \boxed{\forall j \bullet j \in 1 \mathinner{..} i-1 \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]})}) \\
= & \ \{wp \texttt{ rule for assignment}\} \\
& wp(\texttt{if(input[i] > result) \{ result := input[i] \}}, \boxed{\forall j \bullet j \in 1 \mathinner{..} \mathbf{i} \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]}) \\
= & \ \{wp \texttt{ rule for conditional}\} \\
& input[i] > result \Rightarrow wp(\texttt{result := input[i]}, \boxed{\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]}) \\
& \wedge \\
& input[i] \le result \Rightarrow wp(\texttt{result := result}, \boxed{\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]}) \\
= & \ \{wp \texttt{ rule for assignment, twice}\} \\
& input[i] > result \Rightarrow (\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge \mathbf{input[i]} \ge input[j]) \\
& \wedge \\
& input[i] \le result \Rightarrow (\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge \mathbf{result} \ge input[j])
\end{aligned}
$$

We then prove that the precondition (i.e., Stay Condition $\wedge$ LI) is no weaker than the above calculated wp:

- To prove the left conjunct:

B   LI

$$
\begin{aligned}
& \boxed{i \le Len(input)} \wedge \boxed{(\ \forall j \bullet j \in 1 \mathinner{..} \mathbf{i - 1} \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]\ )} \Rightarrow \\
& input[i] > result \Rightarrow \boxed{\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge input[i] \ge input[j]} \\
\equiv & \ \{\ \underline{\texttt{Shunting}}\texttt{:}\quad p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q) \Rightarrow r \quad \} \\
& i \le Len(input) \wedge (\ \forall j \bullet j \in 1 \mathinner{..} \mathbf{i - 1} \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]\ ) \wedge input[i] > result \Rightarrow \\
& \boxed{\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge input[i] \ge input[j]}
\end{aligned}
$$

Proof via Assuming the Antecedent:

$$
\begin{aligned}
& \boxed{\forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge input[i] \ge input[j]} \\
\equiv & \ \{\texttt{split range: } \forall j \bullet j \in 1 \mathinner{..} i \Rightarrow P(j) \equiv (\forall j \bullet j \in 1 \mathinner{..} i-1 \Rightarrow P(j)) \wedge P(i)\} \\
& (\forall j \bullet j \in 1 \mathinner{..} \mathbf{i - 1} \Rightarrow 1 \le j \wedge j \le Len(input) \wedge \boxed{input[i] \ge input[j]}) \wedge (1 \le \mathbf{i} \wedge \mathbf{i} \le Len(input) \wedge input[i] \ge input[\mathbf{i}]) \\
\equiv & \ \{\texttt{antecedent: } input[i] > \mathbf{result}\texttt{; and RHS of precond: } \forall j \bullet j \in 1 \mathinner{..} i-1 \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]\} \\
& true \wedge (1 \le i \wedge i \le Len(input) \wedge input[i] \ge input[i]) \\
\equiv & \ \{\texttt{LHS of precond: } i \le Len(input) \texttt{ and } input[i] \ge input[i] \equiv true\} \\
& true
\end{aligned}
$$

$input[i] > result$

$\wedge\ result \geq input[j]$

$\Rightarrow input[i] \geq input[j]$

- (*Exercise*) To prove the right conjunct:

$$
\begin{aligned}
& i \le Len(input) \wedge (\ \forall j \bullet j \in 1 \mathinner{..} \mathbf{i - 1} \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]\ ) \\
& \Rightarrow input[i] \le result \Rightarrow \forall j \bullet j \in 1 \mathinner{..} i \Rightarrow 1 \le j \wedge j \le Len(input) \wedge result \ge input[j]
\end{aligned}
$$