1 5F-1 Bookkeeping

- **0 pts** Correct

Exercise 5F-2. VCGen Do-While

In order to provide the backward verification condition formula for the command do $do_{Inv1,\ Inv2}\ c\ while\ b$, we can express the command in the following way because Inv1 should hold before c is first executed and Inv2 should hold before evaluating the loop predicate b for each iteration .

$do_{Inv1,\ Inv2}\ c\ while\ b$ = $Inv1;\ c;\ while_{\ Inv2}\ b\ do\ c$

If we analyze closer to Inv1 and Inv2, Inv1 should be always true before Inv2 is evaluated in the while loop, so if we incorporate this implication relationship between Inv1 and Inv2, we can get its backward verification condition formula into the following form.

VC($do_{Inv1,\ Inv2}\ c\ while\ b$, B)

= VC($Inv1;\ c;\ while_{\ Inv2}\ b\ do\ c$, B)

= Inv1 ∧ Inv2 ⇒ Inv1 ∧ VC($c;\ while_{\ Inv2}\ b\ do\ c$, B)

= Inv1 ∧ Inv2 ⇒ Inv1 ∧ VC(c, VC($while_{\ Inv2}\ b\ do\ c$, B))

= Inv1 ∧ Inv2 ⇒ Inv1 ∧ VC(c, Inv2 ∧ (for all x1, …, xn. Inv2 ⇒ (b ⇒ VC(c, Inv2)) ∧ ¬b ⇒ B))

where Inv2 ∧ (for all x1, …, xn. Inv2 ⇒ (b ⇒ VC(c, Inv2)) ∧ ¬b ⇒ B) comes from the slide #10 in the lecture 11.

2 5F-2 VCGen Do-While

- **0 pts** Correct

Exercise 5F-3. VCGen Mistakes

If we look at the correct while Hoare rules, it looks like below:

$$\frac{\vdash \{A \wedge b\}\ c\ \{A\}}{\vdash \{A\}\ while\ b\ do\ c\ \{A \wedge \neg b\}}$$

For this question, three alternate while Hoare rules(lannister, stark, and targaryen) are presented, and all of them are sound but incomplete. Among these three rules, we will prove that stark and targaryen rules are incomplete. If we have a closer look on stark and targaryen rules below:

Stark rule: $\frac{\vdash \{X \wedge b\}\ c\ \{X\}}{\vdash \{X\}\ while\ b\ do\ c\ \{X\}}$ Targaryen rule: $\frac{\vdash \{X\}\ c\ \{X\}}{\vdash \{X\}\ while\ b\ do\ c\ \{X \wedge \neg b\}}$

we can see that for stark rule it does not have ¬b on its postcondition and for targaryen rule it does not have b on its premise, compared to the correct version of the while Hoare rule. These differences will make stark and targaryen rules sound but incomplete, and we will provide counterexamples of stark and targaryen rules respectively in order to prove their incompleteness below.

1. Stark rule
2. A: x = 0
3. B: x = 3
4. sigma: sigma(x) = 0
5. sigma1: sigma1(x) = 3
6. c: while x != 3 do x += 1
7. <c, sigma> ⇓ sigma1: sigma1(x) = 3
8. sigma ⊨ A: sigma ⊨ A holds because sigma: sigma(x) = 0 and A: x = 0. Therefore, sigma(x) and A are same
9. sigma1 ⊨ B: sigma1 ⊨ B holds because sigma1: sigma1(x) = 3 and B: x = 3. Therefore, sigma1(x) and B are same
10. It is not possible to prove the stark rule. If the last rule used is the rule of consequence, it will look like $\frac{\vdash \{x = 0\} \Rightarrow C \quad \frac{\vdash \{C \wedge x\ != 3\}\ x\ +=\ 1\ \{C\}}{\vdash \{C\}\ while\ x\ != 3\ do\ x\ +=\ 1\ \{C\}} \quad \vdash C \Rightarrow \{x = 3\}}{\vdash \{x = 0\}\ while\ x\ != 3\ do\ x\ +=\ 1\ \{x = 3\}}$.
    On the rule of consequence above, the middle part of the premise is the stark rule, but it is impossible to have C such that it connects from {x = 0} to {x = 3}(in other words, {x = 0} ⇒ C ⇒ {x = 3}) In addition, according to the stark rule, the precondition and postcondition should be the same, but it is actually not same in stark rule(x = 0 and x = 3) if we assume that the last rule used is the stark rule. Because of the following reasons, the stark rule presented in the question is not complete.

1. Targaryen rule
2. A: x < 3
3. B: x = 3
4. sigma: sigma(x) = 0
5. sigma1: sigma1(x) = 3
6. c: while x < 3 do x += 1
7. <c, sigma> ⇓ sigma1: sigma1(x) = 3
8. sigma ⊨ A: sigma ⊨ A holds because sigma: sigma(x) = 0 and A: x < 3. Therefore, sigma(x) < 3.
9. sigma1 ⊨ B: sigma1 ⊨ B holds because sigma1: sigma1(x) = 3 and B: x = 3. Therefore, sigma1(x) = B.
10. It is not possible to prove the targaryen rule. If the last rule used is the rule of consequence, it will look like

$$\frac{\vdash \{x < 3\} \Rightarrow C \quad \dfrac{\vdash \{C\}\ x \mathrel{+}= 1\ \{C\}}{\vdash \{C\}\ while\ x < 3\ do\ x \mathrel{+}= 1\ \{C \wedge \neg(x < 3)\}} \quad \vdash C \wedge \neg(x < 3) \Rightarrow \{x = 3\}}{\vdash \{x < 3\}\ while\ x < 3\ do\ x \mathrel{+}= 1\ \{x = 3\}}.$$

On the rule of consequence above, the middle part of the premise is the targaryen rule, but there is a contradiction on ⊢ {C} x += 1 {C} because C is coming from ⊢ {x < 3} and it cannot satisfy ⊢ {x < 3} x += 1 {x < 3} when x += 1 results in x = 3 on the while loop. Because of this contradiction, it is incomplete when the last rule used is the rule of consequence. In addition, according to the targaryen rule, the postcondition should be precondition ∧ ¬(x < 3) but it leads to contradiction if we assume that the last rule used is the targaryen rule. Because of the following reasons, the targaryen rule presented in the question is not complete.

3 5F-3 VCGen Mistakes

- **0 pts** Correct