5F-2. VCGen Do-While

Here is the verification condition formula for the command do_{Inv} c while b with respect to a post-condition P.

$$VC(c, Inv) \wedge (\forall x_1, \ldots, x_n \; Inv \implies ((b \implies VC(c, Inv)) \wedge (\neg b \implies VC(c, P))))$$

Here we want the Invariant to hold after one evaluation of c and that's why instead of Inv at the beginning (like in the normal while loop VC) we have VC(c,Inv). And also, for the post condition to hold we let the command c to evaluate one more time before we exit the do-while loop that's why we have $\neg b \implies VC(c, P)$ at the end instead of $\neg b \implies P$ like in a normal while loop VC.

1 5F-3. VCGen Mistakes

Here is an example that cannot be proved by the **targaryen** rule: Let's say we have, X to be $x = 0$ ($A = X$ and $B = X \wedge \neg b$), c to be while $false$ do $x = x + 1$ and $\sigma(x) = 0$. And $\sigma'(x) = 0$ since $\langle$ while $false$ do $x = x + 1, \sigma\rangle \Downarrow \sigma$ by the large step operational semantic rules. And $\sigma \models x = 0$ and $\sigma' \models x = 0 \wedge true$. When we try to apply the targaryen rule with the consequence rule we will have the following,

$$\frac{\vdash \{x + 1 = 0\} x = x + 1 \{x = 0\} \qquad \vdash x = 0 \implies x + 1 = 0}{\{x = 0\} \text{ while } false \text{ do } x = x + 1 \{x = 0 \wedge \neg false\}}$$

Although here, the second premise doesn't work logically that's why we are stuck and the targaryen is incomplete considering this example.

And if we consider the **stark** rule, we can give the following unprovable example: Let's say our X is $x \leq 4$, and we have the following command: while $x < 4$ do $x = x * 2$. And we have $\sigma(x) = 2$. When we apply the large step operational semantics we will get to $\sigma'(x) = 4$. Therefore, we can say $\sigma \models x \leq 4$ and $\sigma' \models x \leq 4$. However, when we try to apply the stark and consequence rules together we will have the following,

$$\frac{\dfrac{\vdash x < 4 \implies 2 * x \leq 4 \quad \vdash \{2 * x \leq 4\} \; x = x * 2 \; \{x \leq 4\}}{\vdash \{x \leq 4 \wedge x < 4\} \; x = x * 2 \; \{x \leq 4\}}}{\{x \leq 4\} \text{ while } x < 4 \text{ do } x = x * 2 \; \{x \leq 4\}}$$

Since the first premise is not correct we cannot prove the above example using the stark rule.