- Verification condition generation for IMP
- Proof of soundness
- Applications: Proof carrying code, automatic patch exploit generation

1 Verification condition generation for IMP

We saw that weakest preconditions don't really work for **while**, in the sense that they produce formulas that are too hard to prove correct, and further, the **while** precondition construction doesn't scale to realistic languages.

One way to get around this weakness is to ask the programmer to supply loop invariants. Every loop looks like **while** b **do** $\{D\}$ c, where D is the loop invariant. We can then generate a *verification condition* that soundly enforces correctness of the program, in the sense that proving the verification condition ensures the program is correct. The verification condition will not in general be (even relatively) complete—if the loop invariants are wrong, the verification condition might be false even though the program is correct.

We now define a verification condition generator $vc[\![c]\!]B$, which takes a command c and a postcondition c as arguments. This verification condition generator is different, and little more complicated, than the one in Winskel, Chapter 7. It has the advantage that it only requires invariants to be given in loops, whereas Winskel's also requires assertions to be given between commands in sequence.

The function $vc[\![c]\!]B = (P, U)$ where P and U are assertions. The assertion P corresponds to the weakest precondition that must hold of the state before the command c executes; the assertion U is a formula that must be true universally. The idea is that if we want to show that a program c is correct (i.e., $\models \{A\}'\{c\}B$), we prove $(A \Rightarrow P) \wedge U$. Therefore, the function $vc[\![c]\!]B$ is sound if:

Soundness: For all c, B, σ, if $(P,U) = vc[\![c]\!]B$, and $\sigma \models^I P$, and $\models U$, and $\langle c, \sigma\rangle \Downarrow \sigma'$, then $\sigma' \models B$.

We proceed to define $vc[\![c]\!]B$ by induction on the structure of commands, and along the way we prove soundness by induction on the big-step derivation of $\langle c, \sigma\rangle \Downarrow \sigma'$.

Case $c =$ **skip:** $vc[\![\textbf{skip}]\!]B = (B, \top)$

We assume all the antecedents to implication in the soundness condition. Since $P = B$, then $\sigma \models^I B$. And $\sigma = \sigma'$, so $\sigma' \models^I B$.

Case $c = x := a$**:** $vc[\![x := a]\!]B = (B\{a/x\}, \top)$

Assuming $\sigma \models B\{a/x\}$, then by the substitution lemma we used for Hoare logic,

$$\sigma' = \sigma[x \mapsto \mathcal{A}[\![a]\!]I\sigma] \models^I B$$

Case $c = c_1; c_2$:

$$vc[\![c_1; c_2]\!]B = (P_1, U_1 \wedge U_2)$$
$$\text{where}(P_2, U_2) = vc[\![c_2]\!]B, (P_1, U_1) = vc[\![c_1]\!]P_2$$

We assume $\langle c_1; c_2, \sigma\rangle \Downarrow \sigma''$, so we know that $\langle c_1, \sigma\rangle \Downarrow \sigma''$ and $\langle c_2, \sigma''\rangle \Downarrow \sigma'$ for some σ''. We also have $\sigma \models^I P_1$ and $\models U_1$, so we can apply the induction hypothesis to the subderivation $\langle c_1, \sigma\rangle \Downarrow \sigma''$ to conclude that $\sigma'' \models P_2$. Using $\models U_2$, we apply the induction hypothesis to the subderivation $\langle c_2, \sigma''\rangle \Downarrow \sigma'$ to conclude $\sigma' \models^I B$.

Case $c =$ **if** b **then** c_1 **else** c_2:

$$vc[\![c]\!]B = ((b \wedge P_1) \vee (\neg b \wedge P_2), U_1 \wedge U_2)$$
$$\text{where } (P_1, U_1) = vc[\![c_1]\!]B, (P_2, U_2) = vc[\![c_2]\!]B$$

Assume WLOG that $\sigma \models^I \mathit{true}$. Then we know that $\langle c_1, \sigma\rangle \Downarrow \sigma'$. We assume $\sigma \models^I (b \wedge P_1) \vee (\neg b \wedge P_2)$, which can only be true if $\sigma \models^I P_1$. With that and $\models U_1$, we can use the induction hypothesis on $\langle c_1, \sigma\rangle \Downarrow \sigma'$ to conclude $\sigma' \models^I B$. The case of **false** is symmetric.

Case $c =$ **while** b **do**$\{D\}$ c':

$$vc[\![c]\!]B = (D, (D \wedge b \Rightarrow P') \wedge (D \wedge \neg b \Rightarrow B) \wedge U')$$
$$\text{where } (P', U') = vc[\![c]\!]B$$

Proceed by cases on the value of b. In each case we can assume that $\sigma \models^I D$ and $\models (D \wedge b \Rightarrow P') \wedge (D \wedge \neg b \Rightarrow B) \wedge U')$.

Case $\sigma \models^I \neg b$: Then $\sigma' = \sigma$, so $\sigma' \models^I D \wedge \neg b$. Because $D \wedge \neg b \Rightarrow B$, we know $\sigma' \models B$.

Case $\sigma \models^I b$: From the evaluation rule we know there exists σ'' such that $\langle c', \sigma\rangle \Downarrow \sigma''$ and $\langle$**while** b **do**$\{D\}$ $c', \sigma''\rangle \Downarrow \sigma'$. Since $\sigma \models^I D^b$, $\sigma \models P'$. By the IH on $\langle c', \sigma\rangle \Downarrow \sigma''$, we know that $\sigma'' \models D$. Since $\sigma'' \models D$ and $(D \wedge b \Rightarrow P') \wedge (D \wedge \neg b \Rightarrow B) \wedge U'$, we can use the IH on the subderivation $\langle$**while** b **do**$\{D\}$ $c', \sigma''\rangle \Downarrow \sigma'$ to conclude $\sigma' \models^I B$.