Scribe: Helgi Ingolfsson and Yoni Ben-Simhon Lecturer: Andrew Myers

1 Problems with PCA

Last lecture we dealt with Partial Correctness Assertions of the type $\{A\}\ c\ \{B\}$.
This gave us a set of rules to produce statements about a program. But this proof system is not syntax directed. We have 2 main problems:

1. With the sequence rule $\dfrac{\{A\}\ c_1\ \{C\} \quad \{C\}\ c_2\ \{B\}}{\{A\}\ c_1; c_2\ \{B\}}$ it is unclear how to choose the set $\{C\}$.
2. The consequence rule $\dfrac{\models A \Rightarrow A' \quad \{A'\}\ c\ \{B'\} \quad \models B' \Rightarrow B}{\{A\}\ c\ \{B\}}$ doesn't indicate how to choose the sets A' and B'. It is also unclear when to use the consequence rule at all. Not to mention that we need some theorem prover to proove statments such as $\models A \Rightarrow A'$.

So this can't be use to make an automatic theorem prover. A solution to these problems exists and is presented below.

2 Weakest Precondition

Given a command c and a postcondition $\{B\}$ we ask what is the weakest precondition $\{A\}$ to satisfy the PCA? The weakest precondition is the largest set of states satisfying the PCA.

$(A \Rightarrow wp(c, B)) \ \Rightarrow\ \{A\}\ c\ \{B\}\ \ (\Leftrightarrow \forall \sigma \models A.\ \mathcal{C}[\![c]\!]\sigma \models B)$

$[\![wp_I(c, B)]\!] = \{\sigma | \mathcal{C}[\![c]\!]\sigma \models_I B\}$ where I is an interpretation environment.
So $\{\sigma | \sigma \models_I A\} \subseteq \{\sigma | \mathcal{C}[\![c]\!]\sigma \models_I B\}$ is equivalent to $A \Rightarrow wp(c, B)$

We want to have an automatic theorem prover. We will see that we will have to slightly cheat when dealing with while using weakest precondition.

Weakest Precondition rules

- $wp_I(skip, B) = \{\sigma |\ \mathcal{C}[\![skip]\!]\sigma \models_I B\} = \{\sigma | \sigma \models_I B\} = [\![B]\!]$, i.e. precondition = postcondition.
- $wp_I(x := a, B) = \{\sigma |\ \sigma[x \mapsto \mathcal{A}[\![a]\!]\sigma] \models_I B\} = B\{a/x\}$, this is our substitution lemma.
- $wp_I(c_1; c_2, B) = \{\sigma |\ \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma) \models_I B\} = wp_I(c_1, wp_I(c_2, B))$, so we can push back the weakest precondition in command sequences.
- $wp_I(if\ b\ then\ c_1\ else\ c_2, B) = (b\ \wedge\ wp_I(c_1, B)) \vee (\neg b\ \wedge\ wp_I(c_2, B))$
- $wp_I(while\ b\ do\ c, B) =?$. We need Gödel numbers to proove this. It is possible to add them to our assertion language but it is not practical.

One such non-practical way to deal with while is:
$\forall k. \forall \sigma_0, \ldots, \sigma_k. [\sigma = \sigma_0 \wedge \forall i \in (0..k). \sigma_i \models_I b \wedge \mathcal{C}[\![c]\!]\sigma_i = \sigma_{i+1}]\ \Rightarrow\ \sigma_k \models_I B$

3 Verification Conditions

To be able to better handle while loops we introduce verification conditions. Here we push some of the work to the programmers making them supply the loop invariants. We can make use of these loop invariants in our proofs if those are supplied.
while b do $\{D\}$ *c*, where $\{D\}$ is the loop invariant, is the format in which the loop invariant is supplied..

Verification Conditions rules

- $vc(\{A\}\ skip\ \{B\}) = \{A \Rightarrow B\}$, since *skip* doesn't change anything
- $vc(\{A\}\ x := a\ \{B\}) = \{A \Rightarrow B\{a/x\}\}$
- $vc(\{A\}\ c_1;\{D\}\ c_2\ \{B\}) = vc(\{A\}\ c_1\ \{D\}) \wedge vc(\{D\}\ c_2\ \{B\})$, though $\{D\}$ isn't really necessary.
- $vc(\{A\}\ if\ b\ then\ c_1\ else\ c_2\ \{B\}) = vc(\{A \wedge b\}\ c_1\ \{B\}) \wedge vc(\{A \wedge \neg b\}\ c_2\ \{B\})$
- $vc(\{A\}\ \ while\ b\ do\ \{D\}\ c\ \ \{B\}) = \{A \Rightarrow D,\ D \wedge \neg b \Rightarrow B\} \vee vc(\{D \wedge b\}\ c\ \{D\})$

4 Proof carrying code

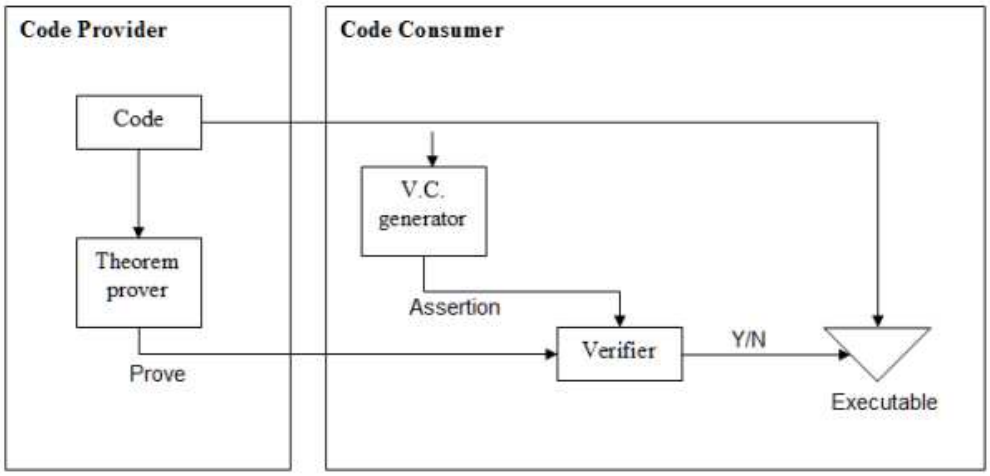

Figure 1: One possible application of verification conditions is proof carrying code

5 Total Correctness

Total correctness is similar to partial correctness, only that we have to show that while loops terminate. That is $([A]c[B] \Rightarrow \{A\}c\{B\} \wedge c \Downarrow$.
Here we will need a decrementing function d, such that the loop terminates when d reaches 0.

- $$\frac{[A \wedge b \wedge d = i]c[A \wedge d < i] \quad \models d \leq 0 \Rightarrow \neg b}{[A]\ while\ b\ do\ c\ [A \wedge \neg b]}$$