PCC Exercise 1

- On page 2 is an example program in machine code.
- Pages 3-5 define a Verification Condition Generator.
- Page 6 shows the outline of the computation of the verification condition of the example program and asks you to compute one of its conjuncts.
- Informally, what is the meaning of the resulting formula? What must be proved and why?

Definition of Verification Condition Generator

- Let \( \Pi \) be the list of instructions output by the certifying compiler. Let \( \Pi(i) \) be the instruction at position \( i \) in \( \Pi \).
- Note: \( VC_{i+3} \) is needed to compute \( VC_i \).

\[
VC_i = \begin{cases} 
[t(r_1, t_2, t_3)]VC_{i+3} & \text{if } \Pi_i \text{ is ADD} \quad r_1 := r_1 + t_2 \\
[t(r_1, t_2, t_3)]VC_{i+3} & \text{if } \Pi_i \text{ is ADDC} \quad r_1 := r_1 + \text{c} \\
[m(r_1, \text{c})]VC_{i+3} \wedge \text{readable}(r_1, \text{c}) & \text{if } \Pi_i \text{ is LD} \quad r_1 := m(r_1, \text{c}) \\
[sup(r_1, \text{c}, r_1, \text{m})] VC_{i+3} \wedge \text{writeable}(r_1, \text{c}) & \text{if } \Pi_i \text{ is ST} \quad m(r_1, \text{c}) := r_1 
\end{cases}
\]

Definition of VCG (continued)

\[
VC_0 = \begin{cases} 
(r_1 = r_2) \Rightarrow VC_{i+3} & \text{if } \Pi_i \text{ is ADD} \quad r_1 := r_1 + t_2 \\
(r_1 > r_2) \Rightarrow VC_{i+3} & \text{if } \Pi_i \text{ is ADDC} \quad r_1 := r_1 + \text{c} \\
(r_1 = r_2) \Rightarrow VC_{i+3} & \text{if } \Pi_i \text{ is BEQ (t_1 = t_2)} \quad \text{c} \\
(r_1 > r_2) \Rightarrow VC_{i+3} & \text{if } \Pi_i \text{ is BGT (t_1 > t_2)} \quad \text{c} \\
\text{post} & \text{if } \Pi_i \text{ is RET} \\
p & \text{if } \Pi_i \text{ is INV} \quad \text{p} 
\end{cases}
\]

- post is the postcondition.
- Every jump point must be proceeded by an INV statement.

Verification Condition

- Let \( \text{inv} \) be the set of line numbers containing INV machine instructions. Also, \( 0 \in \text{inv} \).
- \( \text{inv}_i \) is the precondition.
- \( \text{inv}_i \) denotes the formula at line \( i \).
- \( \text{sp} \) is the function computing the safety predicate (verification condition) from the code.

\[
\text{sp}(\text{inv}_{\text{post}}) = \forall k \forall r_1 \exists \Psi_{\text{inv}} \Rightarrow VC_{i+3}
\]

VCGen Applied to Example Program

0: \( r_0 \bowtie \text{inlist} \land r_3 = 0 \)

... 

9: \( \text{INV} \quad r_1 : \text{in} \)

\((\text{inv}_0 \Rightarrow VC_3) \land (\text{inv}_2 \Rightarrow VC_4) \land (\text{inv}_9 \Rightarrow VC_9) \)

- Exercise: Compute \( (\text{inv}_2 \Rightarrow VC_9) \)