COMP3151/9154
Week 2 – Notes on Floyd's Method

Ron van der Meyden

June 11, 2023

These notes expand on the example application of Floyd's method discussed in lectures in more precise detail.

1 Hoare Logic

Floyd's method is used to prove "Hoare Logic" assertions of the form $\{\alpha\}\ P\ \{\beta\}$, meaning that program P, when started in any state satisfying formula α will, whenever it terminates, do so in a state satisfying β. (Note that this is a safety property. It is not part of the assertion that P will always terminate!)

To apply Floyd's method, we need to deal with variants of formulas $Q(\ell)$ labelling a location ℓ of the transition diagram of P after the application of an update function f. This is denoted $Q(\ell) \circ f$ in the lecture slides.

Effectively, Floyd's method breaks down the proof down into a set of simpler Hoare Logic statements, each corresponding to a single possible step of the program. Suppose we have a transition $\ell_i \xrightarrow{g;S} \ell_j$ and $Q(\ell_i) = \alpha$ and $Q(\ell_j) = \beta$, where α, β and g are formulas, and S is a single step program, or *action* (typically an assignment statement $x = e$, or simply the action *skip* that does not change any of the program's variables). Then the formula $(Q(\ell_i) \wedge g) \implies Q(\ell_j) \circ f$ in the lecture slides corresponds to a Hoare logic statement $\{\alpha\}\ g; S\ \{\beta\}$.

The formula g is called the *guard* of the step. Intuitively, the program $g; S$ is able to proceed only if the guard g is true. If not, the step is not able to execute, but this does not amount to termination, so there is nothing to prove in this case. The statement $\{\alpha\}\ g; S\ \{\beta\}$ only cares about the initial states where $\alpha \wedge g$ is true. In these cases, we run S, and we require that β is true when S terminates.

To reason precisely about such statements, we need a little terminology from predicate logic. The notation $\beta[e/x]$ is used to represent the result of substituting expression e for the *free* occurrences of variable x in a formula β. "Free" here means not in the scope a quantification of that variable. For example,

$$(x = 3 \wedge \forall x(0 \leq x))[e/x] \quad = \quad (e = 3 \wedge \forall x(0 \leq x))$$

Note that we don't substitute for the third occurrence of x because it is in the scope of the quantification $\forall x$.

We can now characterize the validity of some simple Hoare logic statements as follows:

- For *skip* statements, $\{\alpha\}\ g; skip\ \{\beta\}$ is equivalent to the validity of the following formula
$$(\alpha \wedge g) \Rightarrow \beta$$
- For assigment statements $x = e$, where e is some expression, $\{\alpha\}\ g; x = e\ \{\beta\}$ is equivalent to the validity of the following formula:
$$(\alpha \wedge g) \Rightarrow (\beta[e/x])$$

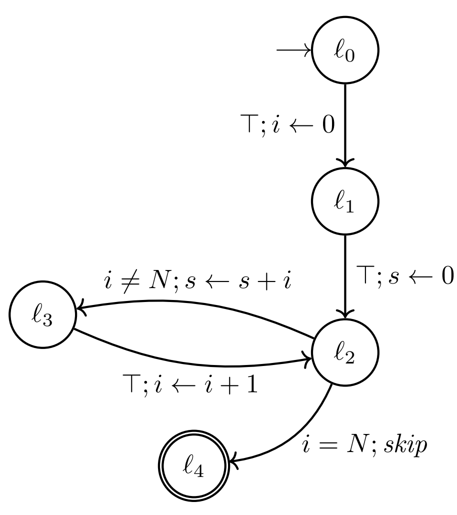
We use these characterizations below to calculate the formulas we need to apply Floyd's method to a simple program.

2 The example

We have the program

$$P = \begin{cases} i \leftarrow 0; \\ s \leftarrow 0; \\ \textbf{while } i \neq N \textbf{ do} \\ \quad s \leftarrow s + i; \\ \quad i \leftarrow i + 1 \\ \textbf{od} \end{cases}$$

which corresponds to the transition diagram



We will show that $\{\top\}\ P\ \{s = \sum_{j=0}^{N-1} j\}$. We label this diagram as follows:

- $Q(\ell_0)$ is $\top$
- $Q(\ell_1)$ is $i = 0$
- $Q(\ell_2)$ is $s = \sum_{j=0}^{i-1} j$
- $Q(\ell_3)$ is $s = \sum_{j=0}^{i} j$
- $Q(\ell_4)$ is $s = \sum_{j=0}^{N-1} j$

(Note that the question of *how* a particular program should be labelled in order to prove its correctness is not always easy to answer. The intuition is that $Q(\ell)$ should be a formula that is *always* true when the computation is at location ℓ, but finding such formulas is an art.)

For each of the edges of the transition diagram, as well as the initial and final states, we now have a formula to prove valid.

- For the initial state, we need to show $\top \Rightarrow \top$, which is obviously valid.
- Transition $\ell_0 \xrightarrow{\top; i \leftarrow 0} \ell_1$ corresponds to $\{\top\}\ \top; i \leftarrow 0\ \{i = 0\}$ which is $\top \Rightarrow (i = 0)[0/i]$, that is, $\top \Rightarrow (0 = 0)$. This is obviously valid!
- Transition $\ell_1 \xrightarrow{\top; s \leftarrow 0} \ell_2$ corresponds to $\{i = 0\}\ \top; s \leftarrow 0\ \{s = \sum_{j=0}^{i-1} j\}$ which is $i = 0 \Rightarrow (s = \sum_{j=0}^{i-1} j)[0/s]$, that is, $i = 0 \Rightarrow (0 = \sum_{j=0}^{i-1} j)$. Noting that if $i = 0$, the sum in question is the empty sum $\sum_{j=0}^{-1} j$, which we conventionally treat as equal to 0, this is valid.
- Transition $\ell_2 \xrightarrow{i \neq N; s \leftarrow s+i} \ell_3$ corresponds to the Hoare Logic statement $\{s = \sum_{j=0}^{i-1} j\}\ i \neq N; s \leftarrow s + i\ \{s = \sum_{j=0}^{i} j\}$ which is

$$((s = \sum_{j=0}^{i-1} j) \wedge i \neq N)) \Rightarrow (s = \sum_{j=0}^{i} j)[s + i/s]$$

  which is

$$((s = \sum_{j=0}^{i-1} j) \wedge i \neq N)) \Rightarrow (s + i = \sum_{j=0}^{i} j)$$

  This is also valid, since if $s = \sum_{j=0}^{i-1} j$ then $s + i = (\sum_{j=0}^{i-1} j) + i = \sum_{j=0}^{i} j$.
- $\ell_3 \xrightarrow{i \leftarrow i+1} \ell_2$ corresponds to the Hoare Logic statement $\{s = \sum_{j=0}^{i} j\}\ \top; i \leftarrow i + 1\ \{s = \sum_{j=0}^{i-1} j\}$ which is

$$(s = \sum_{j=0}^{i} j) \Rightarrow (s = \sum_{j=0}^{i-1} j)[i + 1/i]$$

which is

$$(s = \sum_{j=0}^{i} j) \Rightarrow (s = \sum_{j=0}^{i+1-1} j)$$

This is also valid, since $i + 1 - 1 = i$, so the left and right hand sides of this implication are the same.

- $\ell_2 \xrightarrow{i=N;skip} \ell_4$ corresponds to the Hoare Logic statement $\{s = \sum_{j=0}^{i-1} j\}\ i = N; skip\ \{s = \sum_{j=0}^{N-1} j\}$ which is

  $$((s = \sum_{j=0}^{i-1} j) \wedge i = N) \Rightarrow s = \sum_{j=0}^{N-1} j$$

  This also is obviously valid.

- For the final state, we need to prove that its label implies the right hand formula of the Hoare logic statement that we are trying to prove for P. This is trivial, since they are the same.

We have now checked all of the proof obligations for Floyd's method, and can conclude that $\{\top\}\ P\ \{s = \sum_{j=0}^{N-1} j\}$.