Introduction to Software Verification

Orna Grumberg

Lectures Material
winter 2017-18

Lecture 3

Floyd Proof Rule for Partial Correctness

To prove $\{q_1\}P\{q_2\}$:

1. Choose a set of cut points such that:
   i. start and halt are cut points
   ii. every cycle in the graph of P contains at least one cut point

2. For every cut point l find an inductive assertion $I_l(\bar{x})$, such that $I_{l_0}(\bar{x}) = q_1(\bar{x})$, $I_{l_*}(\bar{x}) = q_2(\bar{x})$

Floyd Proof Rule for Partial Correctness (cont.)

3. For every basic path $\alpha = (l, l')$ prove:
   $\forall \bar{x}[I_l(\bar{x}) \wedge R_\alpha(\bar{x}) \rightarrow I_{l'}(T_\alpha(\bar{x}))]$

If we successfully applied the proof rule for some invariants we will write

$\vdash_F \{q_1\}P\{q_2\}$

Floyd Proof Rule for Partial Correctness

Soundness of Floyd proof system (F):

If $\vdash_F \{ q_1 \} P \{ q_2 \}$

then $\models \{ q_1 \} P \{ q_2 \}$

Floyd Proof Rule for Partial Correctness

Lemma:

If $\vdash_F \{q_1\}P\{q_2\}$ then for every computation π of P from l_0 with state σ such that $\sigma \vDash q_1(\bar{x})$ if the computation reaches cut point l' with state σ' then $\sigma' \vDash I_{l'}(\bar{x})$

Proof:

By induction on the number of cut points traversed in π

Floyd Proof Rule for Partial Correctness

Completeness of the proof system F:

If $\models \{ q_1 \} P \{ q_2 \}$

then $\vdash_F \{ q_1 \} P \{ q_2 \}$

We will not prove this.

Floyd Proof Rule for Partial Correctness (cont.)

If we change the requirement

3. For every basic path $\alpha = (l, l')$ prove:
   $\forall \bar{x}[I_l(\bar{x}) \wedge R_\alpha(\bar{x}) \rightarrow I_{l'}(T_\alpha(\bar{x}))]$

To

$\forall \bar{x}[I_l(\bar{x}) \rightarrow I_{l'}(T_\alpha(\bar{x}))]$

Will the new rule be sound? Complete?

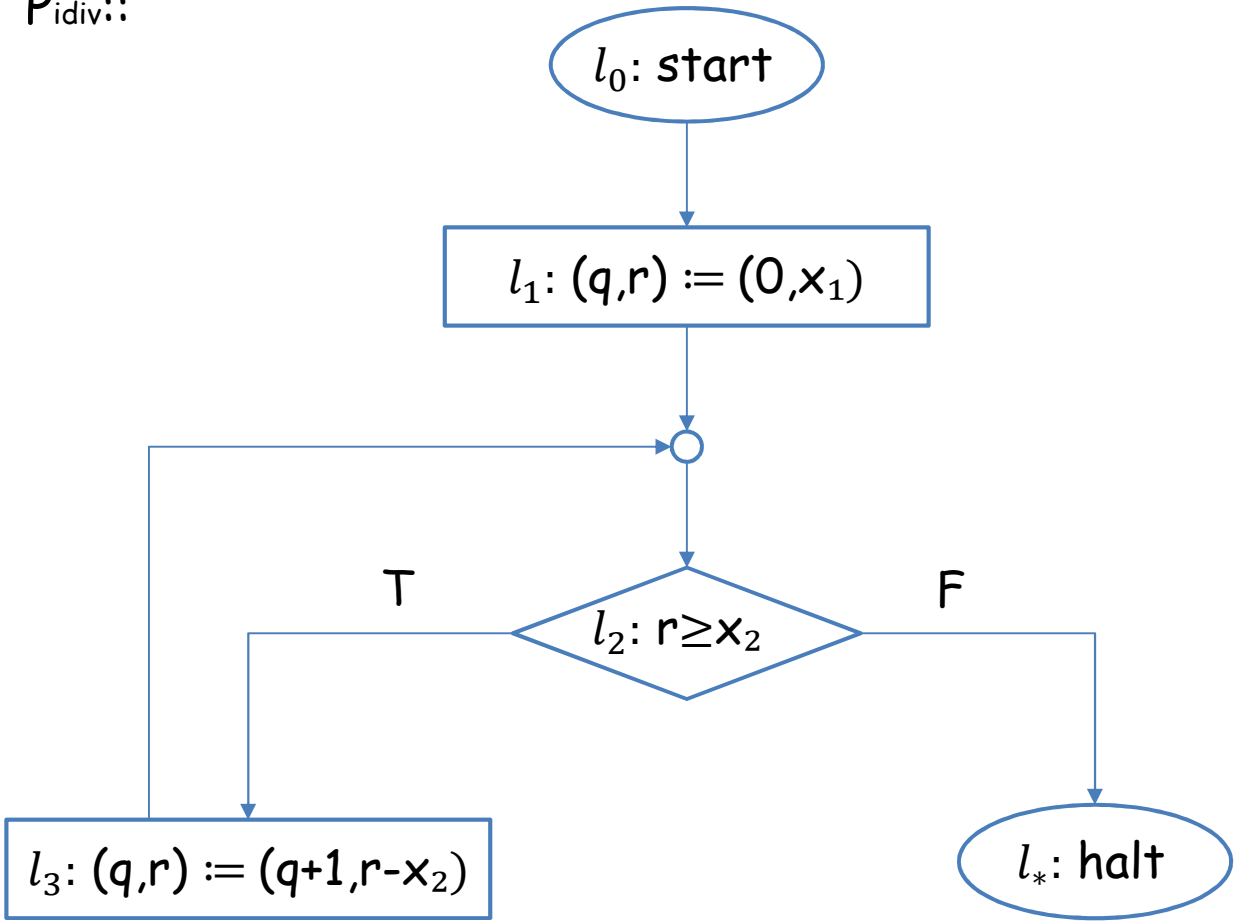
F* Proof Rule for Proving Termination (full correctness)

We would like to prove <p>S<q>

Example:

Flowchart: Example

P_{idiv}::



Well Founded Sets

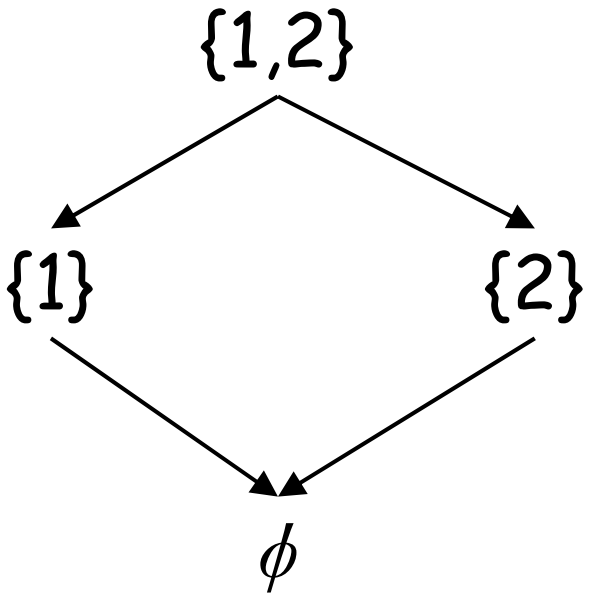
A set W with a (possibly partial) order $<$ $(W,<)$ is a well founded set if there is no infinitely decreasing sequences in W.

That is, there is no sequence $w_i \in W$ such that:

$w_0 > w_1 > w_2 > \ldots$

Well Founded Sets - Examples

The partially ordered set $(2^A, \subset)$ for $A=\{1,2\}$



Well Founded Sets - Examples

- Naturals with the usual order $<$ $(N,<)$ is a well founded set
- Integers with the usual order $<$ is **not** well founded
- Positive rational numbers with the usual order $<$ is **not** well founded
- $(2^A,\subset)$ for any **finite** A is well founded
- $(2^A,\subset)$ for an **infinite** A is **not** well founded
- $N\times N$ with the lexicographical order is a well founded set

F* Proof System for Proving Termination (full correctness)

To prove $\langle q_1 \rangle$ P $\langle$true$\rangle$:

1. Choose $(W,<)$ to be $(N,<)$ with the usual order
2. Choose a cut set as in F
3. For every cut point l find a parameterized inductive assertion $\boldsymbol{I_l(\bar{x}, w)}$ where $w \in W$

4. Prove (in First order logic):

- (INIT) $\forall \bar{x}\left[q_1(\bar{x}) \rightarrow \exists w\left(I_{l_0}(\bar{x}, w)\right)\right]$
- (DEC) For every basic path $\alpha = (l, l')$ prove:

$$\forall w \forall \bar{x}\left[\begin{array}{c} I_l(\bar{x}, w) \wedge R_\alpha(\bar{x}) \rightarrow \\ \exists w'\left(\, w' < w \;\wedge\; I_{l'}(T_\alpha(\bar{x}), w')\right) \end{array}\right]$$

If we successfully applied the proof rule for some invariants we will denote

$$\vdash_{F^*} < q_1 > P < true >$$

F* Proof System for Proving Termination (full correctness)

To prove $\langle q_1 \rangle P \langle q_2 \rangle$ we need to prove in addition in First order logic:

$$\forall w \forall \bar{x} \left[I_{l_*}(\bar{x}, w) \rightarrow q_2(\bar{x}) \right]$$

F* Proof System for Proving Termination (full correctness)

Soundness of the proof system F* :

If $\vdash_{F^*} \langle q_1 \rangle P \langle q_2 \rangle$

then $\models \langle q_1 \rangle P \langle q_2 \rangle$

F* Proof System for Proving Termination (full correctness)

Lemma:

If $\vdash_{F^*}$ <q_1>P<true>then for every computation π of P from l_0 with state σ such that $\sigma \vDash q_1(\bar{x})$ if the computation reaches cut point l' with state σ' then there is $v \in W$ such that $\sigma' \vDash I_{l'}(\bar{x}, v)$

In addition, if the computation pass through cutpoints $l_0, l_1, \ldots$ with states $\sigma_0, \sigma_1, \ldots$ then there exists a sequence $v_0 > v_1 > \ldots$ such that for every I, $\sigma_i \vDash I_{l_i}(\bar{x}, v_i)$

F* Proof System for Proving Termination (full correctness)

Completeness of the proof system F* :

If $\models \langle q_1 \rangle P \langle q_2 \rangle$

then $\vdash_{F^*} \langle q_1 \rangle P \langle q_2 \rangle$