

Program Verification 2012–2013

Project 3: Bytecode Verification Engine

Danny Bergsma Jaap van der Plas

April 2, 2013

1 Introduction

2 Weakest precondition rules

These are our weakest-precondition rules ☺:

$$\begin{array}{l} \text{SETLOCAL } k \ x =_{sem} \{loc_k := x\} \\ wp(\text{SETLOCAL } k \ x) \ Q =_{def} \ Q[x/loc_k] \end{array}$$

$$\begin{array}{l} \text{LOADLOCAL } k =_{sem} \{T := T + 1 ; stack_T := loc_k\} \\ wp(\text{LOADLOCAL } k) \ Q =_{def} \ (Q[loc_k/stack_T])[(T + 1)/T] \end{array}$$

$$\begin{array}{l} \text{STORELOCAL } k =_{sem} \{loc_k := stack_T ; T := T - 1\} \\ wp(\text{STORELOCAL } k) \ Q =_{def} \ (Q[(T - 1)/T])[stack_T/loc_k] \wedge T \geq 0 \end{array}$$

$$\begin{array}{l} \text{LOADPARAM } k =_{sem} \{T := T + 1 ; stack_T := param_k\} \\ wp(\text{LOADPARAM } k) \ Q =_{def} \ (Q[param_k/stack_T])[(T + 1)/T] \end{array}$$

$$\begin{array}{l} \text{STOREPARAM } k =_{sem} \{param_k := stack_T ; T := T - 1\} \\ wp(\text{STOREPARAM } k) \ Q =_{def} \ (Q[(T - 1)/T])[stack_T/param_k] \wedge T \geq 0 \end{array}$$

$$\begin{array}{l} \text{PUSHLITERAL } l =_{sem} \{T := T + 1 ; stack_T := l\} \\ wp(\text{PUSHLITERAL } l) \ Q =_{def} \ (Q[l/stack_T])[(T + 1)/T] \end{array}$$

$$\begin{aligned} \text{POP} &=_{\text{sem}} \{T := T - 1\} \\ wp(\text{POP}) Q &=_{\text{def}} Q[T - 1/T] \wedge T \geq 0 \end{aligned}$$

$$\begin{aligned} \text{ADD} &=_{\text{sem}} \{stack_{(T-1)} := stack_{T-1} + stack_T ; T := T - 1\} \\ wp(\text{ADD}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} + stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{MIN} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} - stack_T ; T := T - 1\} \\ wp(\text{MIN}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} - stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{MUL} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} * stack_T ; T := T - 1\} \\ wp(\text{MUL}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} * stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{EQ} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} \equiv stack_T ; T := T - 1\} \\ wp(\text{EQ}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} \equiv stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{LT} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} < stack_T ; T := T - 1\} \\ wp(\text{LT}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} < stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{LTE} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} \leq stack_T ; T := T - 1\} \\ wp(\text{LTE}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} \leq stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{GT} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} > stack_T ; T := T - 1\} \\ wp(\text{GT}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} > stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{GTE} &=_{\text{sem}} \{stack_{T-1} := stack_{T-1} \geq stack_T ; T := T - 1\} \\ wp(\text{GTE}) Q &=_{\text{def}} (Q[(T-1)/T])[(stack_{T-1} \geq stack_T) / stack_{T-1}] \wedge T \geq 1 \end{aligned}$$

$$\begin{aligned} \text{return} &=_{\text{sem}} \{return := stack_T ; T := T - 1\} \\ wp(\text{return}) Q &=_{\text{def}} (Q[T - 1/T])[stack_T / return] \wedge T \geq 0 \end{aligned}$$

$$wp(s_1 ; s_2 ; \dots ; s_n) Q =_{\text{def}} wp s_1 (wp s_2 (\dots (wp s_n Q)))$$

$$wp(\text{iftrue } s_1 \text{ else } s_2) Q =_{\text{def}} ((wp s_1 Q)[T - 1/T] \wedge stack_T) \vee ((wp s_2 Q)[T - 1/T] \wedge \neg stack_T) \wedge T \geq 0$$

$$wp(\text{prog } P \ (n) \ s) Q =_{\text{def}} (wp s (Q \wedge T \equiv -1)[a_0/param_0][a_1/param_1] \dots [a_{n-1}/param_{n-1}])[-1/T]$$