Program Verification 2012–2013
Project 3: Bytecode Verification Engine

Danny Bergsma Jaap van der Plas

April 3, 2013

1 Introduction

2 Weakest precondition rules

These are our weakest-precondition rules ☺:

$$\texttt{SETLOCAL}\ k\ x =_{sem} \{loc_k := x\}$$
$$wp\ (\texttt{SETLOCAL}\ k\ x)\ Q\ =_{def}\ Q[x/loc_k]$$

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

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

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

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

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

$$\texttt{POP} =_{sem} \{T := T - 1\}$$
$$wp\ (\texttt{POP})\ Q\ =_{def}\ Q[T-1/T] \wedge T \geq 0$$

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

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

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

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

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

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

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

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

$$\texttt{EQUIV} =_{sem} \{stack_{T-1} := stack_{T-1} \leftrightarrow stack_T\ ;\ T := T - 1\}$$
$$wp\ (\texttt{EQUIV})\ Q\ =_{def}\ (Q[(T-1)/T])[(stack_{T-1} \leftrightarrow stack_T)/stack_{T-1}] \wedge T \geq 1$$

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

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

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

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