Bali Virtual Machine (BVM)

Operational semantics for instructions:

exec_mo (Getfield idx) CFS cn hp stk pc =
(let $oref$ = hd stk;
  (cl,fs) = get_Obj (hp !! (get_Addr $oref$));
  $cpool$ = get_cpool (CFS !! cn);
  (fc,fn,fd) = extract_Fieldref $cpool$ idx;
  xp' = if $oref$=Null then Some NullPoint
    else None
in
(xp', hp, (fs !! (fc,fn))#(tl stk), pc+1))

Program execution:

Execution terminates, if the frame stack is empty or an excpetion has been thrown:

exec (CFS, None, hp, []) = None
exec (CFS, None, hp, fr#frs) = Some ...
exec (CFS, Some xpt, hp, frs) = None

$$CFS \vdash \sigma \longrightarrow^* \sigma' \stackrel{\text{def}}{=}$$
$$(\sigma,\sigma') \in \{(s,t).\ \text{exec}\ (CFS,s) = \text{Some}\ t\}^*$$

Bytecode Verifier (BV)

Program type information

Collects type information for all instructions:

Φ :: $(stack\_type \times vars\_type)$ $list$

Well-typed instruction

wt_mo (Getfield idx) CFS cn Φ max pc =
(let (ST,LT) = Φ ! pc;
    $cpool$ = get_cpool (CFS !! cn);
    (fc,fn,fd) = extract_Fieldref $cpool$ idx
 in
 $\exists rs\ ST'$.
   $pc+1 < max \wedge$
   get_fields (CFS !! fc) (fc,fn) = Some $fd \wedge$
   ST = (RTS rs) # $ST' \wedge$
   convertible CFS rs (CT fc) $\wedge$
   Φ $(pc+1) \sqsupseteq$ ((fd2tys CFS fd) # ST', LT))

Well-typed method code

$\forall pc<$length ins.
   wt $(ins$! $pc)$ CFS cn Φ (length ins) pc

Soundness of the BV

Runtime value conforms to static type:

conf_val $CFS\ hp$ (Intg i) $tys = (tys =$ PTS Int$)$
conf_val $CFS\ hp$ (Addr a) $tys =$
$\exists obj\ rt\ rs.$
$tys =$ RTS $rs \wedge$
$hp\ a =$ Some $obj \wedge$
fd2tys CFS (get_obj_type obj) $=$ RTS $[rt] \wedge$
convertible $CFS\ [rt]\ rs$
conf_val $CFS\ hp$ Null $tys = (\exists rs.\ tys =$ RTS $rs)$

Main theorem:

If well-formed class files have been checked by BV before execution then runtime values will be type conform in all states:

wf_cfs $CFS \wedge$ wt_cfs $CFS\ \Phi\ \wedge$
conf_state $CFS\ \sigma\ \Phi \wedge CFS \vdash\ \sigma \longrightarrow^{*} \sigma'$
$\Longrightarrow$ conf_state $CFS\ \sigma'\ \Phi$