Contents

CONTEXT LP0

CONSTANTS

n0

a

power2

AXIOMS

axm1: $n0 \in N$

axm2: $a \in 0 \mathinner{..} n0 \to N$

axm3: $\forall k \cdot k \in 0 \mathinner{..} n0 \Rightarrow a(k) = k * k$

axm4: $power2 \in N \to N$

axm5: $\forall n \cdot n \in 0 \mathinner{..} n0 \Rightarrow power2(n) = a(n)$

pre/post for power2

END

MACHINE LP1
SEES LP0
VARIABLES
done
r
INVARIANTS
inv1: $done \in BOOL \land r \in 0 \mathinner{..} n0 \to Z$
inv2: $done = TRUE \Rightarrow r = a$
EVENTS
Initialisation
begin
act1: $done := FALSE$
act2:
$r :\in 0 \mathinner{..} n0 \to Z$
end
Event computing1 ⟨ordinary⟩ $\widehat{=}$
when
grd1: $done = FALSE$
then
act1: $done := TRUE$
act2: $r := a$
end
END

MACHINE LP2
REFINES LP1
SEES LP0
VARIABLES

done

r

aa

i

INVARIANTS

inv1: $done \in BOOL \land i \in 0 \mathinner{..} n0 \land r \in 0 \mathinner{..} n0 \to Z$

inv2: $aa \in 0 \mathinner{..} n0 \pfun Z$

inv7: $dom(aa) = 0 \mathinner{..} i$

inv3: $\forall k \cdot k \in dom(aa) \Rightarrow aa(k) = a(k)$

inv9: $i \in 0 \mathinner{..} n0$

inv8: $aa \subseteq a$

EVENTS

Initialisation

begin

act1: $done := FALSE$

act2:

$r :\in 0 \mathinner{..} n0 \to Z$

act3: $i := 0$

act5: $aa := \{0 \mapsto 0\}$

end

Event computing2 ⟨ordinary⟩ $\widehat{=}$

refines computing1

when

grd1: $done = FALSE$

grd2: $n0 \in dom(aa)$

then

act1: $done := TRUE$

act2: $r := aa$

end

Event power2 ⟨ordinary⟩ $\widehat{=}$

when

grd1: $done = FALSE$

grd2: $n0 \notin dom(aa)$

then

act1: $i := i + 1$

act2: $aa(i + 1) := power2(i + 1)$

end

END

MACHINE LP3
REFINES LP2
SEES LP0
VARIABLES
done
r
aa
i
EVENTS
Initialisation
begin
act1: $done := FALSE$
act2:
$r :\in 0 \mathinner{..} n0 \to Z$
act3: $i := 0$
act5: $aa := \{0 \mapsto 0\}$
end
Event computing3 ⟨ordinary⟩ $\widehat{=}$
refines computing2
when
grd1: $done = FALSE$
grd2: $i = n0$
then
act1: $done := TRUE$
act2: $r := aa$
end
Event power3 ⟨ordinary⟩ $\widehat{=}$
refines power2
when
grd1: $done = FALSE$
grd2: $i < n0$
then
act1: $i := i + 1$
act2: $aa(i + 1) := power2(i + 1)$
end
END

MACHINE LP4
REFINES LP3
SEES LP0
VARIABLES
done
r
aa
i
EVENTS
Initialisation
begin
act1: $done := FALSE$
act2:
$r :\in 0 \mathinner{..} n0 \rightarrow Z$
act3: $i := 0$
act5: $aa := \{0 \mapsto 0\}$
end
Event computing4 ⟨ordinary⟩ $\widehat{=}$
refines computing3
when
grd1: $done = FALSE$
grd2: $i = n0$
then
act1: $i, r, aa, done :| (i = n0 \Rightarrow done' = TRUE \wedge r' = aa \wedge aa' = aa \wedge i' = i)$
end
Event power4 ⟨ordinary⟩ $\widehat{=}$
refines power3
when
grd1: $done = FALSE$
grd2: $i < n0$
then
act1: $i, r, aa, done :| (i < n0 \Rightarrow i' = i+1 \wedge aa' = aa \cup \{i+1 \mapsto power2(i+1)\} \wedge done' = done \wedge r' = r)$
end
END

MACHINE LP5
REFINES LP4
SEES LP0
VARIABLES
done
r
aa
i
EVENTS
Initialisation
begin
act1: $done := FALSE$
act2:
$r :\in 0 \mathinner{..} n0 \to Z$
act3: $i := 0$
act5: $aa := \{0 \mapsto 0\}$
end
Event computing5 ⟨ordinary⟩ $\widehat{=}$
refines computing4
when
grd1: $done = FALSE$
grd2: $i = n0$
then
act1:
$i, r, aa, done :| (i = n0 \Rightarrow done' = TRUE \wedge r' = aa \wedge aa' = aa \wedge i' = i)$
$\wedge (i < n0 \Rightarrow i' = i + 1 \wedge aa' = aa \cup \{i + 1 \mapsto power2(i + 1)\} \wedge done' = done \wedge r' = r)$
end
Event power5 ⟨ordinary⟩ $\widehat{=}$
refines power4
when
grd1: $done = FALSE$
grd2: $i < n0$
then
act1:
$i, r, aa, done :| (i = n0 \Rightarrow done' = TRUE \wedge r' = aa \wedge aa' = aa \wedge i' = i)$
$\wedge (i < n0 \Rightarrow i' = i + 1 \wedge aa' = aa \cup \{i + 1 \mapsto power2(i + 1)\} \wedge done' = done \wedge r' = r)$
end
END

MACHINE LP6
REFINES LP5
SEES LP0
VARIABLES
done
r
aa
i
EVENTS
Initialisation
begin
act1: $done := FALSE$
act2:
$r :\in 0 \mathinner{..} n0 \to Z$
act3: $i := 0$
act5: $aa := \{0 \mapsto 0\}$
end
Event final ⟨ordinary⟩ $\widehat{=}$
refines computing5, power5
when
grd1: $done = FALSE$
then
act1:
$i, r, aa, done :| (i = n0 \Rightarrow done' = TRUE \wedge r' = aa \wedge aa' = aa \wedge i' = i)$
$\wedge (i < n0 \Rightarrow i' = i + 1 \wedge aa' = aa \cup \{i + 1 \mapsto power2(i + 1)\} \wedge done' = done \wedge r' = r)$
end
END