Contents

CONTEXT A-functions

CONSTANTS

factorial

n

s

AXIOMS

axm1: $n \in \mathbb{N}$

axm2: $factorial \in \mathbb{N} \leftrightarrow \mathbb{N}$

axm3: $0 \mapsto 1 \in factorial$

axm4:
$\forall a \cdot \forall b \cdot a \in \mathbb{N} \land b \in \mathbb{N} \land a \mapsto b \in factorial$
$\Rightarrow a + 1 \mapsto (a + 1) * b \in factorial$

axm5:
$\forall f \cdot f \in \mathbb{N} \leftrightarrow \mathbb{N}$
$\land\ 0 \mapsto 1 \in f$
$\land\ (\forall a, b \cdot a \in \mathbb{N} \land b \in \mathbb{N} \land a \mapsto b \in f$
$\Rightarrow a + 1 \mapsto (a + 1) * b \in f)$
$\Rightarrow factorial \subseteq f$

axm6: $s \in \mathbb{N} \to \mathbb{N} \land (\forall i \cdot i \in \mathbb{N} \Rightarrow s(i) = i + 1)$

axm7: $\forall A \cdot A \subseteq \mathbb{N} \land 0 \in A \land s[A] \subseteq A \Rightarrow \mathbb{N} \subseteq A$

axm8: ⟨theorem⟩ $\forall i \cdot i \in \mathbb{N} \land i \in dom(factorial) \Rightarrow (factorial^{-1}; factorial)[\{i\}] = \{i\}$

axm9: ⟨theorem⟩ $factorial^{-1}; factorial \subseteq id(\mathbb{N} \times \mathbb{N})$

axm10: ⟨theorem⟩ $dom(factorial) = \mathbb{N}$

axm11: ⟨theorem⟩ $factorial \in \mathbb{N} \to \mathbb{N}$

axm12: ⟨theorem⟩ $factorial(0) = 1$

axm13: ⟨theorem⟩ $\forall u \cdot u \in \mathbb{N} \land u \neq 0 \Rightarrow factorial(u) = u * factorial(u - 1)$

END

MACHINE B-prepost
SEES A-functions
VARIABLES
r
INVARIANTS
inv1: $r \in \mathbb{Z}$
EVENTS
Initialisation
begin
act1: $r :\in \mathbb{Z}$
end
Event final ⟨ordinary⟩ $\widehat{=}$
begin
act1: $r := factorial(n)$
end
Event iteration ⟨anticipated⟩ $\widehat{=}$
begin
act1: $r :\mid (r' \in \mathbb{Z})$
end
END

MACHINE C-computing
REFINES B-prepost
SEES A-functions
VARIABLES

r

fac

cfac

INVARIANTS

inv1:
$fac \in \mathbb{N} \pfun \mathbb{N}$

inv7: $cfac \in \mathbb{N}$

inv2: $dom(fac) \subseteq 0 \upto n$

inv3: $dom(fac) \neq \varnothing$

inv4: $\forall i \cdot i \in dom(fac) \Rightarrow fac(i) = factorial(i)$

inv6: $dom(fac) = 0 \upto cfac$

VARIANT

$0 \upto n \setminus dom(fac)$

EVENTS

Initialisation

begin

act1: $r :\in \mathbb{Z}$

act2: $fac := \{0 \mapsto 1\}$

act3: $cfac := 0$

end

Event final ⟨ordinary⟩ $\widehat{=}$
refines final

when

grd1: $n \in dom(fac)$

then

act1: $r := fac(n)$

end

Event step2 ⟨convergent⟩ $\widehat{=}$
refines iteration

when

grd13: $n \notin dom(fac)$

then

act11: $fac(cfac + 1) := (cfac + 1) * fac(cfac)$

act1: $cfac := cfac + 1$

end

END

MACHINE D-prealgo
REFINES C-computing
SEES A-functions
VARIABLES

r
vfac
cfac
fac

INVARIANTS

inv1: $vfac \in \mathbb{N}$
inv5: $vfac = fac(cfac)$

VARIANT

$0 \,..\, n \setminus 0 \,..\, cfac$

EVENTS
Initialisation

begin

act1: $r :\in \mathbb{N}$
act2: $fac := \{0 \mapsto 1\}$
act3: $cfac := 0$
act4: $vfac := 1$

end

Event final ⟨ordinary⟩ $\widehat{=}$
refines final

when

grd2: $cfac = n$

then

act1: $r := vfac$

end

Event step3 ⟨convergent⟩ $\widehat{=}$
refines step2

when

grd3: $cfac \neq n$

then

act1: $vfac := (cfac + 1) * vfac$
act2: $cfac := cfac + 1$
act3: $fac(cfac + 1) := (cfac + 1) * fac(cfac)$

end

END

MACHINE E-algo
REFINES D-prealgo
SEES A-functions
VARIABLES

r

vfac

cfac

INVARIANTS

thm1: ⟨theorem⟩ $vfac = factorial(cfac)$

inv1: $r \in \mathbb{N}$

computation_inv1:
$fac \in \mathbb{N} \pfun \mathbb{N}$

inv2: $dom(fac) \subseteq 0 \upto n$

inv3: $dom(fac) \neq \varnothing$

inv4: $\forall i \cdot i \in dom(fac) \Rightarrow fac(i) = factorial(i)$

inv5: $cfac \in dom(fac)$

inv6: $dom(fac) = 0 \upto cfac$

algorithm_inv1: $vfac \in \mathbb{N}$

algorithm_inv2: $cfac \in \mathbb{N}$

algorithm_inv3: $cfac \leq n$

algorithm_inv4: $cfac \geq 0$

algorithm_inv6: $cfac \in dom(fac)$

algorithm_inv5: $vfac = fac(cfac)$

inv7: $cfac + 1 \notin dom(fac)$

inv8: $dom(fac) = 0 \upto cfac$

VARIANT

$n - cfac$

EVENTS

Initialisation

begin

act1: $r :\in \mathbb{N}$

act3: $cfac := 0$

act4: $vfac := 1$

end

Event final ⟨ordinary⟩ $\widehat{=}$

refines final

when

grd2: $cfac = n$

then

act1: $r := vfac$

end

Event step4 ⟨convergent⟩ $\widehat{=}$

refines step3

when

grd1: $cfac \neq n$

then

act1: $vfac := (cfac + 1) * vfac$

act2: $cfac := cfac + 1$

end

END

MACHINE E-algo1
REFINES E-algo
SEES A-functions
VARIABLES
r
vfac
cfac
EVENTS
Initialisation
begin
act1: $r :\in \mathbb{N}$
act3: $cfac := 0$
act4: $vfac := 1$
end
Event final ⟨ordinary⟩ $\widehat{=}$
refines final
when
grd2: $cfac = n$
then
act1: $r := vfac$
end
Event step4 ⟨ordinary⟩ $\widehat{=}$
refines step4
when
grd1: $cfac \neq n$
then
act1: $vfac := (cfac + 1) * vfac$
act2: $cfac := cfac + 1$
end
END