1.Докажите, что программа:

y:=0; z:=1;

while y=x do y:=y+1; z=z*y od вычисляет x! и присваивает результат переменной z.

Учебник. Докажем,

что нижеприведенная программа вычисляет x! и присваивает результат

переменной z: y:=0; z:=1;

while y=x do y: =y+1; z:=z*y od

Для данной программы требуемым предикатом является:

$\sigma(z) = \sigma(x)!$.

Можно выделить последовательность вида:

σ_0^σ_1^σ_2…^ σ_k. где σ_0 = Out(O(y: =0; z:=1)σ),

σ_{i+1}=Out(O(y: =y+1; z: =z*y)σ_1).

Докажем по индукции, что σ{z} для всех промежуточных

состояний $\sigma_0,\sigma_1,\sigma_2\ldots,\sigma_k$, т.е. $\sigma_1\{z\} = \sigma_1\{y\}!$ для i=0,1,2,...k. Тогда имеем

базисный шаг:

σ_0 = Out(0(y: =0; z: = 1)σ) = Out(σ[0/y]^O(z: = 1)(σ[0/y])) = Out(σ[0/y]^σ[0/y][1/z]) = σ[0/y][1/z].

Поскольку 1=0!, получаем $\sigma_0\{z\} = \sigma_0\{y\}!$

Для индуктивного шага действуем с предположением, что $\sigma_1\{z\}$ =

$\sigma_1\{y\}!$. Тогда:

σ_{i+1}= Out(0(y: =y+1; z:=z*y)σ_1) = Out(0(z:=z*y)(σ_1[Eval(y+1)σ_1/y])) =
σ_1[Eval(y+1)σ_1/y][Evαl(z*y)(σ_1[Evαl(y+1)σ_1/y])/z] = σ_1[Eval(y+1)σ_1/y][Eval(y!*(y+1))σ_1/z]
=σ_1[Evαl(y+1)σ_1/y][Evαl(y+1)!σ_1/z]

Отсюда получаем, что σ_{i+1}\{z\}=Eval(y+1)!σ_1и σ_{i+1}\{y\}=Eval(y+1)σ_1

Из последнего равенства получаем σ_{i+1}\{y\}!= Eval(y+1)!σ_1, откуда следует, что $\sigma_{i+1}\{z\}=\sigma_{i+1}\{y\}!$.
Таким образом, для любого i≥0, имеем $\sigma_1\{z\} = \sigma_1\{y\}!$.

Поскольку это равенство справедливо, также и для заключительного состояния σ_k и учитывая, что σ_k \{y\}= σ_k \{x\}, получаем $\sigma_k(z) = \sigma_k(x)!$, что завершает доказательство.

2.Докажите, что программа:

a:= 0; b:= x; while b>=y do b:= b-y; a:= a+1 od

удовлетворяет условию (x>=0 & y>=0) программа {a*y+b=x & 0 <= b < y}

По аксиоме (A1) имеем:

{0*y+x=x & x>=0} a:=0 {a*y+x=x & x>=0}

{a*y+x=x & x>=0} b:=x {a*y+b=x & b>=0}

Применим правило (R2):

{0*y+x=x & x>=0} a:=0; b:=x {a*y+b=x & b=>0}

Так как справедливо утверждение x>=0 & y=>0 → 0*y+x=x & x>=0, применим правило (R5) и получим:

{ x>=0 & y=>0} a:=0; b:=x {a*y+b=x & b=>0}

По аксиоме (A1) имеем:

{(a+1)*y+b-y=x & b-y>=0} b:=b-y {(a+1)*y+b=x & b>=0}

{(a+1)*y+b=x & b>=0} a:=a+1 {a*y+b=x & b>=0}

Применим правило (R2):

{(a+1)*y+b-y=x & b-y>=0} b:=b-y; a:=a+1 {a*y+b=x & b>=0}

Так как справедливо утверждение a*y+b=x & b>=0 & b>=y → (a+1)*y+b-y=x & b-y>=0, применим правило (R5) и получим:

{a*y+b=x & b>=0 & b>=y}b:=b-y; a:=a+1 {a*y+b=x & b>=0}

Применим правило (R4):

{a*y+b=x & b>=0} while b>=y do b:=b-y; a:=a+1 od {a*y+b=x & b>=0 & b<y}

Далее применяя правило (R2) получим искомое утверждение.

3.Докажите, что программа удовлетворяет условиям:

{true} z:=1; y:=0; while y=x do y:=y+1; z:=z*y od (z=x!).

Учебник. P ≡ z=y! – желаемый инвариант для циклического участка.

Получаем:

{true} z:=1; y:=0; while y ≠ x do

{z=y!} y:=y+1; z:=z*y od {z=x!}

1) По аксиоме (A1) имеем:

{1=0!} z:=1 {z=0!}, {z=o!} y:=0 {z=y!}

Применим правило (R2):

{1=0!} z:=1; y:=0 {z=y!}

Так как при стандартной интерпретации на множестве целых чисел справедливо утверждение true → 1=0!, применим правило (R5) и получим:

{true} z:=1; y:=0 {z=y!}, значит программа {true} z:=1; y:=0 устанавливает инвариант P

2) По аксиоме (A1) имеем:

{z=(y+1-1)! & (y+1-1) ≠ x } y:=y+1 { z=(y-1)! & (y-1) ≠ x }

Применим правило (R5):

{z=y! & y≠ x} y:=y+1 {z*y=y! & (y-1) ≠ x}

По аксиоме (A1) имеем:

{z*y=y! & (y-1) ≠ x} z:=z*y { z=y! & (y-1) ≠ x}

Применим правило (R2):

{z=y! & y≠ x} y:=y+1; z:=z*y { z=y! & (y-1) ≠ x}

Применим правило (R4):

{z=y!} while y ≠ x do y:=y+1; z:=z*y od {z=y! & y=x}, значит программа while y ≠ x do y:=y+1; z:=z*y od сохраняет инвариант P

3)Поскольку справедливо утверждение z=y! & y=x -> z=x!, то применим правило (R5) и получим:

{z=y!} while y ≠ x do y:=y+1; z:=z*y od {z=x!}

Доказательство закончено

4. Докажите условие P & B(R) (EO) для программы:

{E0=b+y>0} b:=b-y; a:=a+1 {E0>b+y>=0}

Учебник. Так как справедливо утверждение E0=b+y>0 & y>0 & b>=y → E0={b-y} +2y>0 & y>0 & (b-y)+y>=y, то по аксиоме (A1) и по правилу (R5) получим

{E0=b+y>0 & y>0 & b>=y} b:=b-y {E0=b+2y>0 & y >0 & b+y>=y}

По правилу (R5) получим {E0=b+y>0 & y>0 & b>=y} b:=b-y {E0>b+y>=0}

По аксиоме (A1) имеем {E0>b+y>=0} a:=a+1 {E0>b+y>=0}

Далее применяя правило (R2) получим искомый результат. Отсюда следует завершимость итерационного цикла => всей программы.

5. Докажите, условие незавершимости для цикла:

$\{P\}$ while B do C od $\{P \& \neg B\}$.

Учебник. Если мы подозреваем, что такой цикл не завершается, то требуется доказать, что не только P, но и P&B является инвариантом цикла, т.е. необходимо показать, что если P&B истинно перед выполнением C, то оно будет истинно и после выполнения C. Отсюда следует незавершимость цикла.

Доказательство незавершимости позволяет также выяснить причины незавершения программы. Анализ этих причин позволяет вносить исправления в программу.

Проиллюстрируем сказанное на примере рассмотренной выше программы целочисленного деления. Вместо начальных условий x>=0 & y>0 возьмем x>=0 & y>=0. В этом случае нетрудно показать, что для y=0 утверждение b>=y будет инвариантом цикла while b>=y do b:=b-y; a:=a+1 od.

Докажем это, как обычно, в два этапа: 1) установка инварианта b>=y командами, предшествующими циклу; 2) сохранение этого инварианта командами тела цикла.

1) Легко показать, что:

{x>=0 & y=0} a:=0; b:=x {b=x & x>=0 & y=0}.

Далее, поскольку справедливы утверждения:

b=x & x>=0 -> b>=0 ,

b>=0 & y=0 -> b>=y & y=0,

получаем по правилу вывода R5:

{x>=0 & y=0} a:=0; b:=x (b>=y & y=0},

т.е. b>=y истинно перед выполнением цикла.

2) Применяя аксиому A1, получаем :

{(b-y)+y>=y & y=0} b:=b-y {b+y>=y & y=0}.

Поскольку справедливо утверждение :

b+y>=y & y=0 -> b>=y,

то, по правилу вывода R5, получаем:

(b>=y & y=0) b:=b-y (b>=y}).

Далее, применяя аксиому A1, имеем:

(b>=y) a:=a+1 (b>=y).

Далее, по правилу R2, получаем :

(b>=y & y=0) b:=b-y; a:=a+1 (b>=y), откуда следует, что b>=y является инвариантом цикла, а следовательно, цикл не завершается.

Сохраняя теперь без изменения начальные условия x>=0 & y>=0 в этой программе, изменим условие выполнения цикла. Вместо условия b>=y возьмем условие b ≠0.

Покажем, что $b \neq 0$ истинно перед выполнением цикла.

Утверждение $x>0$ & $y>0$ & $(x \bmod y) \neq 0 \rightarrow x \neq 0$ & $y>0$ & $(x \bmod y) \neq 0$ справедливо, так как если $x=0$, то $(x \bmod y)=0$ также, что противоречит условию.

Далее, применяя дважды аксиому A1, а затем правила вывода

R2 и R5, получаем :

$\{x>0$ & $y>0$ & $(x \bmod y) \neq 0\}$ a:=0; b:=x $\{b \neq 0$ & $y>0$ & $(b \bmod y) \neq 0\}$, т.е. утверждение $b \neq 0$ истинно перед выполнением цикла.

Покажем теперь, что b ≠ o является инвариантом цикла в данном случае.

По аксиоме A1 имеем :

$((b-y)+y \neq 0$ & $((b-y)+y \bmod y) \neq 0$ & $y>0)$ b:=b-y $(b+y \neq 0$ & $((b+y) \bmod y) \neq 0$ & $y>0)$.

Утверждение $((b+y) \bmod y) \neq 0$ & $y>0 \rightarrow b \neq 0$ справедливо, так как в противном случае мы получаем, что $(y \bmod y) \neq 0$ для $y>0$, что противоречит определению операции деления по модулю. Также справедливо утверждение:$((b+y) \bmod y) \neq 0$ & $y>0 \rightarrow (b \bmod y) \neq 0$, так как, если $(b \bmod y)=0$, то это означает, что для некоторого целого k справедливо $b=y*k$, откуда следует, что $b+y=y*k+y=y*(k+1)=y*k'$, где k' целочисленное значение, а значит $((b+y) \bmod y)=0$, что противоречит посылке утверждения.

Применяя правило R5, получим :

$\{b \neq 0$ & $(b \bmod y) \neq 0$ & $y>0\}$ b:=b-y $\{b \neq 0$ & $(b \bmod y) \neq 0$ & $y>0\}$.

Далее, по аксиоме A1 имеем :

$\{b=0$ & $(b \bmod y) \neq 0$ & $y>0\}$ a:=a+1 $(b \neq 0$ & $(b \bmod y) \neq 0$ & $y>0)$.

Отсюда по правилу R2 получаем :

$(b=0$ & $(b \bmod y) \neq 0$ & $y>0)$ b:=b-y; a:=a+1 $(b=0$ & $(b \bmod y) \neq 0$ & $y>0\}$.

Таким образом, утверждение b×0, являющееся условием выполнения цикла, есть инвариант цикла, а следовательно, цикл не завершается.