完全正当性の証明

<A>P<B>を証明するためには,

while規則を以下のもので置換えるだけで良い

(他の規則はなぜ変更しない?)

$$\frac{<bound=n \wedge A \wedge t>P<bound<n \wedge A>}{<A>\textbf{while } t \textbf{ do } P \textbf{ od}<A \wedge \neg t>}$$

ただし,

bound: 非負整数を表す, P中のプログラム変数に関する数式

ループの繰り返し回数の限度を表す

n: 非負整数(正整数)を表す論理変数(P中には現れない)

$$\frac{<bound=n \wedge A \wedge t>P<bound<n \wedge A>}{<A>\textbf{while } t \textbf{ do } P \textbf{ od}<A \wedge \neg t>}$$

意味(停止性に関して)：

Pの実行前のboundの値がnであったとする

Pの1回の実行でboundの値が少なくとも1以上減る.

いずれはboundの値が0になるので停止する.

演習

x, y, zを自然数とする.

このとき以下を証明せよ.

<true>

begin y:=1;z=0; **while** z≠x **do begin** z:=z+1;y=y*z **end end**

<y=x!>

boundとして何をとればいいか

演習

<gcd(a, b)=gcd(x, y)>
while b≠0 do **begin** a:=a mod b; c:=a; a:=b; b:=c **end**
<gcd(a, b)=gcd(x, y)∧b=0>

を証明せよ.