Termination

Es. 5.1.2, pg. 205 exercisebook

Prove the termination of:

```
lcm:  begin z:=1;
            while z mod x != 0 or z mod y != 0 do
                  z:= z+1;
            od
      end
```

$X = N \times N \times N$, since $x = \langle x, y, z\rangle$

1. As a well-founded set we can choose $\langle N, >\rangle$
2. As a function $f: N^3 \rightarrow N$ we choose $x*y - z$
3. As loop invariant we choose $z \leq x*y$ (notice that for sure $x*y-z \in Z$, being x,y,z natural numbers. Moreover, the loop invariant holding implies that $x*y-z \in N$).

Prove that $z \leq x*y$ is a loop invariant

We modify the original invariant used for partial correctness, adding a term:

Original loop invariant: $I = \{\forall w\ (1 \leq w < z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0))\}$

Modified loop invariant (we add the conjunct $z \leq x*y$):

$J = \{\forall w\ (1 \leq w < z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0)) \wedge z \leq x*y\}$

Let's show it is indeed a loop invariant

We immediately apply IR4 to handle the while loop; therefore we want to prove:

$\{J \wedge (z \bmod x \mathrel{!=} 0 \text{ or } z \bmod y \mathrel{!=} 0)\}$

```
z:= z+1;
```

$\{J\}$

Through backsubstitution we get

$I^* = \{\forall w\ (1 \leq w < z+1 \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0)) \wedge z+1 \leq x*y\} == \{\forall w\ (1 \leq w \leq z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0)) \wedge z < x*y\}$

Now, notice that:

$\{J \wedge (z \bmod x \mathrel{!=} 0 \text{ or } z \bmod y \mathrel{!=} 0)\} ==$

$\{\forall w\ (1 \leq w < z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0)) \wedge z \leq x*y \wedge (z \bmod x \mathrel{!=} 0 \text{ or } z \bmod y \mathrel{!=} 0)\} ==$

$\{\forall w\ (1 \leq w \leq z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0)) \wedge z \leq x*y\}$

Now, we realize that the first conjunct: $\forall w\ (1 \leq w \leq z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0))$ implies, as a special case, that: $z \bmod x \mathrel{!=} 0$ or $z \bmod y \mathrel{!=} 0$. Therefore, it cannot be $z = x*y$ (otherwise it'd be $z \bmod x = z \bmod y = 0$). So we can finally get to:

$\{\forall w\ (1 \leq w \leq z \rightarrow (w \bmod x \mathrel{!=} 0 \text{ or } w \bmod y \mathrel{!=} 0)) \wedge z < x*y\} = I^*$

Prove that $f(x', y', z') > f(x'', y'', z'')$

$f(x, y, z) = x*y - z$. Therefore, since at each iteration x and y stay the same, while z increases, we conclude $f(x', y', z') > f(x'', y'', z'')$.

More explicitly, if $f(x', y', z') = x'y' - z'$ and $f(x'',y'',z'') = x''y'' - z''$, then we have to show that $x'y' - z' > x''y'' - z''$. Since: $x'' = x'$, $y'' = y'$, $z'' = z' + 1$, we have to show that: $x'y' - z' > x'y' - (z' + 1)$, that is simply $0 > -1$, which is obviously true.

Es. 5.1.3, pg. 206 exercisebook

Prove termination of (program that checks if x is prime):

```
begin
  i:= 2;
  pr:= 1;
  while i < x do
    if x mod i = 0;
      pr := 0;
    i := i+1
  od
end
```

X = N × N × N, since x = ⟨x, i, pr⟩

1. As a well-founded set we can choose ⟨N, >⟩
2. As a function f: $N^3 \rightarrow N$ we choose x-i (notice that pr does not contribute to termination).
3. As loop invariant we choose $i \leq x$. Of course $i \leq x \rightarrow x-i \in N$

Prove that $i \leq x$ is a loop invariant

The partial invariant we used to check partial correctness was:

I = `i <= x and (pr = 0 => exists y(1 < y < i and x mod y = 0)) and (pr = 1 => forall y(1 < y < i => x mod y != 0)`

Therefore, $i \leq x$ was already part of the invariant, so we don't have to prove its validity again.

Prove that f(x', y', z') > f(x'', y'', z'')

f(x, y, z) = x – i.

Therefore, since at each iteration x stays the same while i increases, we conclude:

f(x', y', z') > f(x'', y'', z'').

More formally, we have to show that x' – i' > x'' – i''. Since x is unchanged, x'' = x'; i is instead increased, so i'' = i' + 1. So the goal is to prove x' – i' > x' – (i' + 1), that is simply 0 > -1, which is obviously true.