Problem 69 with PVS

Kai Engelhardt

January 24, 2023

1 A No-Frills Encoding

```
% Problem number "69. Greatest Common Divisor Algorithm from the list
% of the "top 100" of mathematical theorems - which nowadays serves as
% some form of benchmark for theorem provers at
% <https://www.cs.ru.nl/~freek/100/> - lacked a PVS formalisation
% and proof.

gcd2: THEORY

BEGIN
x,y,z: VAR posnat

% axiomatic gcd, inspired by https://isabelle.in.tum.de/dist/library/HOL/HOL/GCD.html
gcd(x,y): posnat
gcd_dvd1: AXIOM divides(gcd(x,y),x)
gcd_dvd2: AXIOM divides(gcd(x,y),y)
gcd_greatest: AXIOM divides(z,x) IMPLIES divides(z,y) IMPLIES divides(z,gcd(x,y))

% some simple properties that ought to follow
gcd_eq:  LEMMA gcd(x,x) = x
gcd_sym: LEMMA gcd(x,y) = gcd(y,x)
gcd_stp: LEMMA x > y IMPLIES gcd(x,y) = gcd(x-y,y)
gcd_stp2: LEMMA x < y IMPLIES gcd(x,y) = gcd(x,y-x)
gcd_leq: LEMMA x >= gcd(x,y)

% algorithmic gcd, Euclid's algorithm
gcd2(x,y): RECURSIVE posnat =
  TABLE
  %--------+-------------+-------------++
  |[ x = y | x > y       | ELSE        ]|
  %--------+-------------+-------------++
  | x      | gcd2(x-y,y) | gcd2(x,y-x) ||
  %--------+-------------+-------------++
  ENDTABLE
  MEASURE x+y

gcd2_h1: LEMMA x > y IMPLIES gcd2(x-y,y) = gcd(x-y,y) IMPLIES gcd2(x,y) = gcd(x,y)
gcd2_h2: LEMMA x < y IMPLIES gcd2(x,y-x) = gcd(x,y-x) IMPLIES gcd2(x,y) = gcd(x,y)

gcd2_eq_gcd: THEOREM gcd2(x,y) = gcd(x,y)

END gcd2
```

The proofs are straightforward und uninspiring, resulting in the summary:

```
Proof summary for theory gcd2
   gcd_eq.............................proved - complete   [shostak](0.04 s)
   gcd_sym............................proved - complete   [shostak](0.01 s)
   gcd_stp_TCC1.......................proved - complete   [shostak](0.02 s)
   gcd_stp............................proved - complete   [shostak](0.08 s)
   gcd_stp2_TCC1......................proved - complete   [shostak](0.02 s)
   gcd_stp2...........................proved - complete   [shostak](0.04 s)
   gcd_leq............................proved - complete   [shostak](0.01 s)
   gcd2_TCC1..........................proved - complete   [shostak](0.01 s)
   gcd2_TCC2..........................proved - complete   [shostak](0.03 s)
   gcd2_TCC3..........................proved - complete   [shostak](0.00 s)
   gcd2_TCC4..........................proved - complete   [shostak](0.01 s)
   gcd2_h1............................proved - complete   [shostak](0.02 s)
   gcd2_h2............................proved - complete   [shostak](0.02 s)
   gcd2_eq_gcd........................proved - complete   [shostak](0.23 s)
   Theory gcd2 totals: 14 formulas, 14 attempted, 14 succeeded (0.54 s)
```