Lógica Computacional - TP3 Exercício 1 - G01

Bruno Dias da Gião A96544, João Luis da Cruz Pereira A95375, David Alberto Agra A95726

November 11, 2023

1 Exercício 1 - Enunciado

Considere-se de novo o algoritmo estendido de Euclides apresentado no TP2 mas usando o tipo dos inteiros e um parâmetro $N > 0$

```
INPUT  a, b : Int
assume  a > 0 and b > 0 and a < N and b < N
r, r', s, s', t, t' = a, b, 1, 0, 0, 1
while r' != 0
  q = r div r'
  r, r', s, s', t, t' = r', r - q × r', s', s - q × s', t', t - q × t'
OUTPUT r, s, t
```

Exercício 1

Este exercício é dirigido às provas de segurança do algoritmo acima.

1. Construa um FOTS $\Sigma \equiv \langle \mathsf{X}, \mathsf{I}, \mathsf{T} \rangle$ usando este modelo nos inteiros.
2. Considere como propriedade de segurança `safety = (r > 0) and (r < N) and (r = a*s + b*t)` Prove usando k-indução que esta propriedade se verifica em qualquer traço do FOTS
3. Prove usando "Model-Checking" com interpelantes e invariantes prove também que esta propriedade é um invariante em qualquer traço de Σ.

2 Exercício 1 - Solução

[ ]: