Rafael Fernández Ortiz

Assignments 1

Exercise 1 - Variations on Integer Division Using Subtraction

During the lectures we proved that the formulas we posited as invariants for the Event B translation of the division through subtraction code were indeed invariants. We will now assume that we change some of the problem conditions. Your task is to determine whether the invariant preservation proofs would have failed and, if so, why and where, in each of the following situations:

```
EVENT INIT
    a, r = 0, b
end
```

```
EVENT Progress
    when
        r>=c
    then
        r, a := r - c, a + 1
    end
```

```
EVENT Finish
    when
        r<c
    then
        skip
    end
```

with a set of axioms and invariants:

$$\mathcal{A}: \quad b \in \mathbb{N}, c \in \mathbb{N}, c > 0$$

$$\begin{aligned} I_1 &\equiv \quad a \in \mathbb{N} \\ I_2 &\equiv \quad r \in \mathbb{N} \\ I_3 &\equiv \quad b = a \times c + r \end{aligned}$$

If we add the invariant $I_4 \equiv r > 0$

If we add the invariant $I_4 \equiv r > 0$, we obtain that b cannot be equal to 0. Therefore, $b \notin \mathbb{N}$. That make a conflict with the EVENT INIT and the axiom $b \in \mathbb{N}$:

By reductio ad absurdum, we can assume that we can add invariant I_4.

$$\texttt{INIT/I}_4\texttt{/INV} = \mathcal{A}_{1\ldots3}(c) \vdash I_4(E_{\texttt{INIT}}(v, c), c)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash r > 0}\ \text{HYP}}{b \in \mathbb{N}, c \in \mathbb{N} \vdash r > 0}\ \text{MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, a = 0 \vdash b > 0}\ \text{MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r = b, a = 0 \vdash b > 0}\ \text{MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r = b, a = 0 \vdash b \neq 0}\ \text{ORD}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r = b, a = 0 \vdash b \notin \mathbb{N}}\ \text{SET TH}$$

Contradiction.

If we modify invariant I_3 by $I_3 \equiv b = a \times c - r$

If we modify invariant I_3 by $\equiv b = a \times c - r$, we obtain that EVENT INIT will only be satisfied when $b = -b$, i.e. $b = 0$:

$$\texttt{INIT/I}_3\texttt{/INV} = \mathcal{A}_{1\ldots3}(c) \vdash I_3(E_{\texttt{INIT}}(v,c),c)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash b = 0}\text{ HYP}}{b \in \mathbb{N}, c \in \mathbb{N} \vdash b = 0}\text{ MON}}{b \in \mathbb{N}, c \in \mathbb{N} \vdash b = -b}\text{ ARITH}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0 \vdash b = -b}\text{ MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0 \vdash b = 0 \times c - b}\text{ ARITH}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r = b, a = 0 \vdash b = a \times c - r}\text{ EQ}$$

Moreover, EVENT Progress cannot be guaranteed to be preserved:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{c > 0 \vdash c \neq 0 \qquad c > 0, c \neq 0 \vdash c = 0}{c > 0 \vdash c = 0}\text{ CUT}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash c = 0}\text{ MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash 0 = 2 \times c}\text{ ARTH}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash 0 = c + c}\text{ ARTH}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash a \times c - r = a \times c - r + c + c}\text{ ARTH}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash a \times c - r = a \times c + c - r + c}\text{ EQ}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c, b = a \times c - r \vdash a \times c - r = a \times c + c - r + c}\text{ MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c, b = a \times c - r \vdash b = a \times c + c - r + c}\text{ EQ}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c, b = a \times c - r \vdash b = (a+1) \times c - (r - c)}\text{ ARTH}$$

We have a proof tree where we assume $c \neq 0 \vdash c = 0$.

If we do not include $c > 0$ among the axioms

The invariant makes the condition $r - c$ decreasing. If we do not include the invariant $c > 0$, we cannot assume that the program terminates.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{c > 0 \vdash c > 0}\text{ HYP}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash c > 0}\text{ MON}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash 0 > -c}\text{ ARTH}}{b \in \mathbb{N}, c \in \mathbb{N}, c > 0, r \geq c \vdash r > r - c}\text{ ARTH}$$

Therefore, we can move from EVENT Progress to EVENT Finish.

Exercise 2 - An Odd Way to Calculate n^2

Someone asks us to calculate the square of a number $n \in N$ as follows:

$$n^2 = \overbrace{1 + 3 + \cdots + (2n-1)}^{n}$$

The following Event B model implements the expression above and leaves the result in r.

```
EVENT INIT
    i := n
    r := 0
    a := 1
end
```

```
EVENT Progress
    when
        i > 0
    then
        r := r + a
        a := a + 2
        i := i - 1
    end
```

```
EVENT Finish
    when
        i = 0
    then
        skip
    end
```

Identify the constants and variables

1. Constants are values that hasn't change: n
2. Variable are values that change in the events: r, a, i

Determine axioms and suitable invariants

$$\mathcal{A}: \quad n \in \mathbb{N}$$

$$\begin{aligned} I_1 &\equiv \quad r \in \mathbb{N} \\ I_2 &\equiv \quad a \in \mathbb{N} \\ I_3 &\equiv \quad i \in \mathbb{N} \\ I_4 &\equiv \quad r = (n-i)^2 \\ I_5 &\equiv \quad a = 1 + 2 \times (n-i) \end{aligned}$$

Prove that the INIT event establishes the invariants

$$\texttt{INIT/I}_4\texttt{/INV} = \mathcal{A}_{1\ldots3}(c) \vdash I_4(E_{\texttt{INIT}}(v,c),c)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 0 = 0}\ \text{EQL}}{\color{red}{n \in \mathbb{N}, a = 1} \color{black}{\vdash 0 = 0}}\ \text{MON}}{n \in \mathbb{N}, a = 1 \vdash 0 = \color{red}{0^2}}\ \text{ARTH}}{n \in \mathbb{N}, a = 1 \vdash 0 = \color{red}{(n-n)^2}}\ \text{ARTH}}{n \in \mathbb{N}, \color{red}{i = n}\color{black}{, a = 1 \vdash 0 = (n-i)^2}}\ \text{MON}}{n \in \mathbb{N}, i = n, a = 1, \color{red}{r = 0}\color{black}{\vdash r = (n-i)^2}}\ \text{EQ}$$

$$\texttt{INIT/I}_5\texttt{/INV} = \mathcal{A}_{1\ldots3}(c) \vdash I_5(E_{\texttt{INIT}}(v,c),c)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 1 = 1}\ \text{EQL}}{\color{red}{n \in \mathbb{N}, r = 0} \color{black}{\vdash 1 = 1}}\ \text{MON}}{n \in \mathbb{N}, r = 0 \vdash 1 = 1 \color{red}{+0}}\ \text{ARTH}}{n \in \mathbb{N}, r = 0 \vdash 1 = 1 + \color{red}{2 \times 0}}\ \text{ARTH}}{n \in \mathbb{N}, r = 0 \vdash 1 = 1 + 2 \times \color{red}{(n-n)}}\ \text{ARTH}}{n \in \mathbb{N}, \color{red}{i = n}\color{black}{, r = 0 \vdash 1 = 1 + 2 \times (n-i)}}\ \text{EQ}}{n \in \mathbb{N}, i = n, \color{red}{a = 1}\color{black}{, r = 0 \vdash a = 1 + 2 \times (n-i)}}\ \text{EQ}$$

Prove that the Progress event preserves the invariants

The first three ones are trivial and easy to prove. We will see I_4 and I_5.

$$\texttt{Progress/I}_4\texttt{/INV} = \mathcal{A}_{1\ldots3}(c)I_{1\ldots5}(v,c), G_{\texttt{Progress}}(v,c) \vdash I_4(E_{\texttt{Progress}}(v,c),c)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash r=(n-i)^2}\,\text{HYP}}{r=(n-i)^2\vdash (n-i)^2=(n-i)^2}\,\text{EQ}}{n\in\mathbb{N}, r=(n-i)^2\vdash (n-i)^2=(n-i)^2}\,\text{MON}}{n\in\mathbb{N}, r=(n-i)^2\vdash (n-i)^2+1=(n-i)^2+1}\,\text{ARTH}}{n\in\mathbb{N}, r=(n-i)^2, n\geq i\vdash (n-i)^2+1+2\times(n-i)=(n-i)^2+1+2\times(n-i)}\,\text{ARTH}}{n\in\mathbb{N}, r=(n-i)^2, n\geq i, a=1+2\times(n-i)\vdash (n-i)^2+a=(n-i)^2+1+2\times(n-i)}\,\text{EQ}}{n\in\mathbb{N}, r=(n-i)^2, n\geq i, a=1+2\times(n-i)\vdash r+a=(n-i)^2+1+2\times(n-i)}\,\text{EQ}}{n\in\mathbb{N}, r=(n-i)^2, n\geq i, a=1+2\times(n-i)\vdash r+a=(n-i+1)^2}\,\text{ARTH}}{n\in\mathbb{N}, r=(n-i)^2, n\geq i, a=1+2\times(n-i)\vdash r+a=(n-(i-1))^2}\,\text{ARTH}$$

$$\texttt{Progress/I}_5\texttt{/INV} = \mathcal{A}_{1\ldots3}(c), I_{1\ldots5}(v,c), G_{\texttt{Progress}}(v,c) \vdash I_5(E_{\texttt{Progress}}(v,c),c)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash a=1+2\times(n-i)}\,\text{HYP}}{a=1+2\times(n-i)\vdash 1+2\times(n-i)=1+2\times(n-i)}\,\text{EQ}}{n\in\mathbb{N}, a=1+2\times(n-i), r=(n-i)^2\vdash 1+2\times(n-i)=1+2\times(n-i)}\,\text{MON}}{n\in\mathbb{N}, a=1+2\times(n-i), r=(n-i)^2\vdash 1+2\times(n-i+1)=1+2\times(n-i+1)}\,\text{ARTH}}{n\in\mathbb{N}, a=1+2\times(n-i), r=(n-i)^2\vdash 1+2\times(n-i)+2=1+2\times(n-i+1)}\,\text{ARTH}}{n\in\mathbb{N}, a=1+2\times(n-i), r=(n-i)^2\vdash a+2=1+2\times(n-i+1)}\,\text{EQ}}{n\in\mathbb{N}, a=1+2\times(n-i), r=(n-i)^2\vdash a+2=1+2\times(n-(i-1))}\,\text{ARTH}$$

Prove that the invariants and axioms are valid by proving the Finish event

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash n^2=n^2}{n\in\mathbb{N}\vdash n^2=n^2}\,\text{MON}}{n\in\mathbb{N}\vdash (n-0)^2=n^2}\,\text{ARTH}}{n\in\mathbb{N}, i=0\vdash (n-i)^2=n^2}\,\text{EQ}}{n\in\mathbb{N}, r=(n-i)^2, i=0\vdash r=n^2}\,\text{EQ}}{n\in\mathbb{N}, i\in\mathbb{N}, a\in\mathbb{N}, a=1+2\times(n-i), r=(n-i)^2, i=0\vdash r=n^2}\,\text{MON}$$