Correctness by Construction
First Event-B Exercise Sheet

Manuel Carro
manuel.carro@upm.es

February 23th, 2022

General

- This exercise sheet is individual.
- Please make sure you have read the course policy.
- Please turn in this exercise sheet not later than **March 2nd, 16:00**.
- I plan to review the solutions during the lecture of March 2nd.
- Please let me know of any difficulty with time enough to react / replan. Do not procrastinate.
- You can:
  - send me a PDF file (highly preferred), or
  - A **good** scan of a (handwritten) solution. Please make sure it is readable!
- **Please do not send me Word, LibreOffice, etc. files**.
  They tend to be hard to reproduce faithfully.

1 Variations on *Integer Division Using Subtraction*

During the lectures we proved that the formulas we posited as invariants for the Event B translation (Fig. 1) 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
```

Axioms

$b \in \mathbb{N}$

$c \in \mathbb{N}$

$c > 0$

Invariants

I_1: $a \in \mathbb{N}$

I_2: $r \in \mathbb{N}$

I_3: $b = a \times c + r$

Figure 1: Dividing by repeated subtraction

1. If we add the invariant $I_4 \equiv r > 0$.
2. If we modify invariant I_3 and instead of

$$I_3 \equiv a \times c + r = b$$

   we have

$$I_3 \equiv a \times c - r = b$$

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

2 An Odd Way to Calculate n^2

Someone asks us to calculate the square of a number $n \in \mathbb{N}$ 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 Finish
  when i = 0
  then
    skip
end
```

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

Your tasks are:

1. Identify the constants and variables.
2. Determine axioms and suitable invariants. Please see item 5 before answering this question: an important property we want these invariants to have is stated there.
3. Prove that the `INIT` event establishes the invariants. You do not need to prove invariant establishment for the invariants related with the type of the variables, such as $i \in \mathbb{N}$.
4. Prove that the `Progress` event preserves the invariants. You do not need to prove invariant preservation for the invariants related with the type of the variables, such as $i \in \mathbb{N}$.
5. The invariants and axioms you decided to use should make it possible to determine that the model is correct w.r.t. the initial specification, i.e., that the sequent

   $$A_{1\ldots l}, I_{1\ldots m}, G_{\texttt{Finish}} \vdash r = n^2$$

   is valid for the axioms $A_{1\ldots l}$ and the invariants $I_{1\ldots m}$. Prove it.