Correctness by Construction
First Event-B Exercise Sheet

Deadline: Tuesday, February 25th 2025, 23:59

Manuel Carro
manuel.carro@upm.es

Wednesday, February 12th, 2025

General Remarks

- This exercise sheet is individual.
- Please make sure you have read the course policy.
- Please turn in the answers to this exercise sheet no later than **Tuesday, February 25th 2025, 23:59**.
- If you experience problems with the assignment, please let me know as soon as possible. It may not be possible to implement last-minute changes / adaptations.
- To turn in the homework you can:
  - Preferably send me a PDF file.
  - Alternatively, send me a **good** scan of a (handwritten) solution, in PDF format. Please make sure that it is readable and, if you scanned the page, that it is not too dark, as this makes reading solutions difficult.
- **Please do not send me Word, LibreOffice, Pages, etc. documents**.
  They may not be reproduced faithfully in all systems.
- Please make sure to include your name in the document you send!

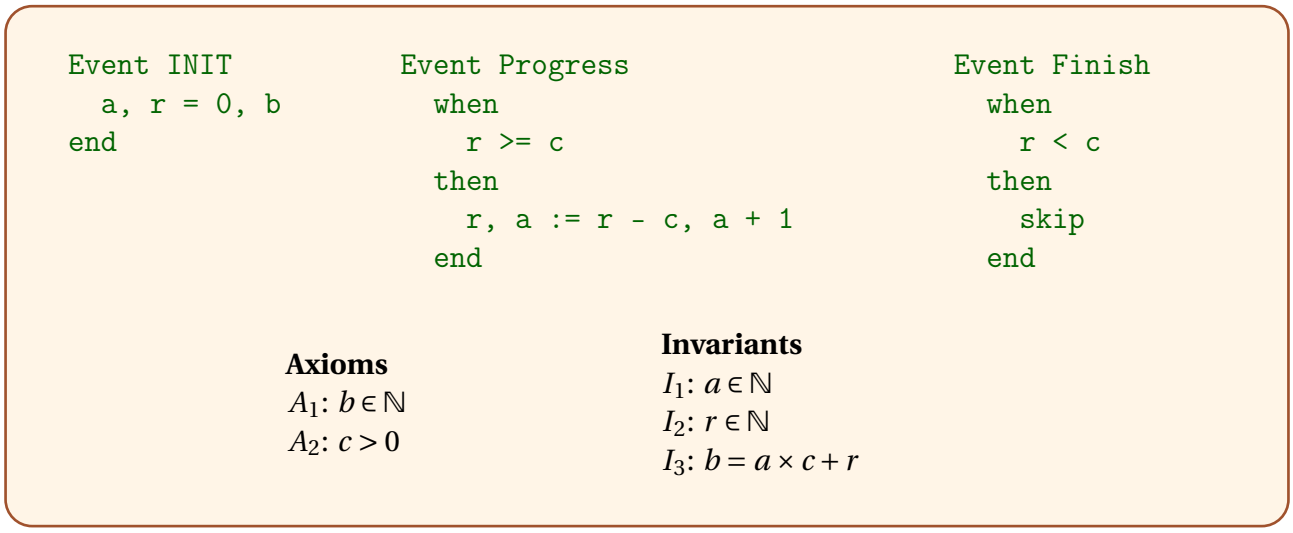

Figure 1: Dividing by repeated subtraction

1 Variations on *Integer Division Using Subtraction*

We proved that the formulas we posited as invariants for the Event B model in Fig. 1 were indeed invariants. Your task is to determine which invariant preservation proofs (if any) would have failed in each of the following cases (every item below corresponds to a different, separate situation):

1. If we modify invariant I_2 to be I_2: $r > 0$.
2. If we modify invariant I_3 to be I_3: $a \times c - r = b$.
3. If we do not include $c > 0$ among the axioms.

You can either find out a counterexample (a scenario / variable valuation that is consistent with the hypotheses but makes the goal false) or redo the proofs and show where it would be obviously impossible to prove the goal.

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

Figure 2: Model of an algorithm to square a natural number.

2 An Odd Way to Calculate n^2

Given a natural number $n \in \mathbb{N}$, we are asked to calculate its square r, i.e., $r = n^2$ (with the usual definition of square). The Event B model in Fig. 2 (hopefully) leaves in r the value n^2 for a given n when the `Finish` event is enabled.

Your tasks are:

1. Identify the constants and variables.
2. Determine axioms and suitable invariants. Please take into account point 6, below, to determine invariants.
3. Prove that the `INITIALISATION` 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. Prove that the `Progress` event eventually terminates.
6. 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.

Use sequent calculus for the proofs, as we did with in the classroom slides.

3 Russian Multiplication

Given constants $a \in \mathbb{N}$, $b \in \mathbb{N}$ and variables $x \in \mathbb{N}$, $y \in \mathbb{N}$, $r \in \mathbb{N}$, the (sequential) events shown below are expected to calculate `r = a × b` when `x` reaches the value `0`:

```
Event INIT
  x,y,r := a,b,0
end
```

```
Event Finish
  when x = 0
  then skip
end
```

```
Event ProgressOdd
  when (x > 0 ∧ x mod 2 = 1)
  then
    r, x, y := r + y, x ÷ 2, y × 2
end
```

```
Event ProgressEven
  when (x > 0 ∧ x mod 2 = 0)
  then
    x, y := x ÷ 2, y × 2
end
```

where '÷' means integer division. We assume here that we know how to divide, but only by two (i.e., we can right-shift bits).

The type axioms and invariants are:

$$\begin{array}{llll} A_1: & a \in \mathbb{N} & I_1: & x \in \mathbb{N} \\ A_2: & b \in \mathbb{N} & I_2: & y \in \mathbb{N} \\ & & I_3: & r \in \mathbb{N} \end{array}$$

However, these are not enough to prove correctness. You have to find out an invariant $I_4(a,b,x,y,r)$ for the model such that:

1. When the event `Finish` is enabled (i.e., when $x = 0$), it implies that $r = a \times b$:

   $$A_1, A_2, I_1, I_2, I_3, I_4, G_{\texttt{Finish}} \vdash r = a \times b$$

   Determine the invariant and prove the sequent.

2. Prove that I_4 is an inductive invariant, e.g., that the sequents

   $$A_1(c), A_2(c), I_{1\ldots4}(v,c), G_i(v,c) \vdash I_4(E_i(v,c),c)$$

   are true for all guards G_i and events E_i that change the state of the model (i.e., for `INIT`, `ProgressEven`, and `ProgressOdd`).

Use sequent calculus for the proofs, as we did with in the classroom slides.