SOLUTION NOTES

Specification and Verification II 2002 Paper 9 Question 12 (MJCG)

The multiplexer `MUX`, register `REG c` (where `c` is the intial value) and combinational unit `COM f` (where `f` is the function computed) are defined to have the behavior given below.

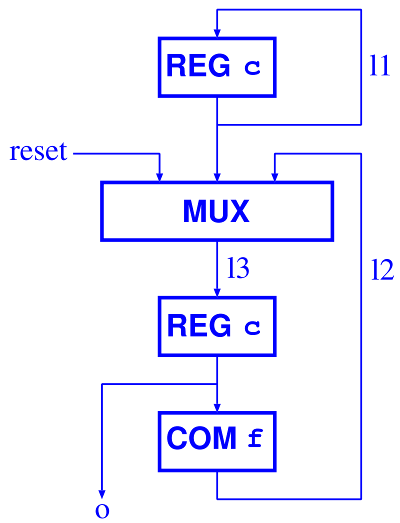
```
MUX(sw,i1,i2,o) = ∀t. o t = if sw t then i1 t else i2 t
REG c (i,o)     = (o 0 = c) ∧ ∀t. o(t+1) = i t
COM f (i,o)     = ∀t. o t = f(i t)
```

Using only instances of `MUX`, `REG c` and `COM f` design a device `DEV(c,f)` that satisfies

```
DEV(c,f)(reset,i,o) =
 (o 0 = c) ∧  ∀t. o(t+1) = if reset(t+1) then c else f(o t)
```

[8 marks]

Here is a suitable design



This design is pretty easy. The main challenge is understanding the formal logical specifications.

Prove that your design meets this specification [12 marks].

```
DEV(c,f)
 = ∃l1 l2 l3.
    REG c (l1,l1) ∧
    MUX(reset l1,l2,l3) ∧
    REG c (l3,o) ∧
    COM f (o,l2)

 = ∃l1 l2 l3.
    ((l1 0 = c) ∧ ∀t. l1(t+1) = l1 t) ∧
    (∀t. l3 t = if reset t then l1 t else l2 t) ∧
    ((o 0 = c) ∧ ∀t. o(t+1) = l3 t) ∧
    (∀t. l2 t = f(o t))

 = ∃l1 l2 l3.
    (∀t. l1 t = c) ∧ (by an induction on t)
    (∀t. l3 t = if reset t then l1 t else l2 t) ∧
    ((o 0 = c) ∧ ∀t. o(t+1) = l3 t) ∧
    (∀t. l2 t = f(o t))

 = ∃l1 l2 l3.
    (o 0 = c) ∧ (pulling ∀ out)
    ∀t. (l1 t = c) ∧
        (l3 t = if reset t then l1 t else l2 t) ∧
        (o(t+1) = l3 t) ∧
        (l2 t = f(o t))

 = ∃l1 l2 l3.
    (o 0 = c) ∧  (unwinding equations)
    ∀t. (l1 t = c) ∧
        (l3 t = if reset t then l1 t else l2 t) ∧
        (o(t+1) = if reset t then c else f(o t)) ∧
        (l2 t = f(o t))

 =  (o 0 = c) ∧ (narrowing scope of ∃)
    ∀t. o(t+1) = if reset t then c else f(o t)) ∧
    (∃l1 l2 l3. ∀t. (l1 t = c)) ∧
    (∃l1 l2 l3. ∀t. l3 t = if reset t then l1 t else l2 t) ∧
    (∃l1 l2 l3. ∀t. l2 t = f(o t))

 =  (o 0 = c) ∧ (use ∃ − law and then cancel true conjuncts)
    ∀t. o(t+1) = if reset t then c else f(o t))
```