/

p9q12
MJCG

Specification and Verification II 2003

HV2: solution notes

This question pertains to the "Introduction to formal methods for hardware" part of the course.

(a) Formalise this informal specification and point out how you have resolved any ambiguities and incompletenesses. [8 marks]

Here is a formalisation, in which words are represented by lists, with the head of the list being the most significant bit (MSB) and the last element the least significant bit (LSB).

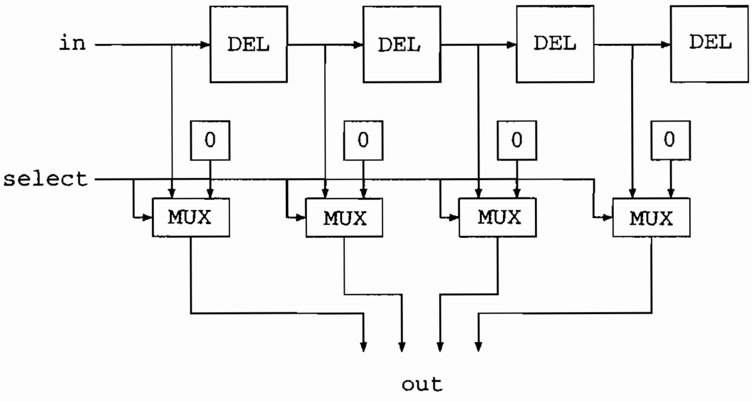
```
D(in, select, out)  =
 ∀t≥3. out(t) = if select(t)
                then [in(t);in(t-1);in(t-2);in(t-3)]
                else [0;0;0;0]
```

The specification did not make clear if the last of the "four preceding cycles" includes the current one. We assume it does.

The specification did not make clear the order of the bits in the word (e.g. whether the current input is the LSB or the MSB) We make the current input be the MSB (ass.

The specification does not specify how to interpret "four preceding cycles" during the first three cycles. We leave the specification unconstrained (i.e.*D* is underspecified).

(b) Using 1-bit unit-delay elements and multiplexers, design a device that implements your formal specification. Draw a diagram of your design.



(c) Outline how you would go about trying to formally verify your design.

To verify the design with respect to D one would first model it as a predicate, *Dimp* say, by composing (using $\exists$ and $\wedge$) the predicates corresponding to the components (ground, unit delay and multiplexer). Then one would prove a suitable correctness property, such as

$$\forall \texttt{in select out}.\ \mathit{Dimp}(\texttt{in}, \texttt{select}, \texttt{out}) \Rightarrow D(\texttt{in}, \texttt{select}, \texttt{out})$$

The proof of this would be use standard logical reasoning.