ARJYA DAS
Email: arjyadas@iisc.ac.in
SR No. : 04-04-00-10-51-21-1-19516
Assignment 3
Course: E0 272: Formal Methods in Software Engineering
Term: January-April 2022

Virtual Memory Scheme Implementation using Rodin:

The abstract system (machine) named *memory* contains the events $read1$, $read2$, $write1$ and $write2$.

- $read1$ returns the address stored at $addr$ of $vmem1$. $read2$ has same functionality for $vmem2$.
- $write1$ updates the value stored at $addr$ of $vmem1$ by val. $write2$ has same functionality for $vmem2$.

The concrete system named *memoryMMU* contains the events $read1$, $read2$, $write1$ and $write2$.

- $read1$ returns the address stored at $ptable1(addr)$ of $pmem$. $read2$ has same functionality for $ptable2$.
- $write1$ updates the value stored at $ptable1(addr)$ of $pmem$ by val. $write2$ has same functionality for $ptable2$.
- Here the number of gluing relation is 3. $glue1$ depicts that for all the $adress$ between location [0,1023], the value stored at $vmem1(address)$ should be same as $pmem(ptable1(address))$.
- $glue2$ depicts that the value stored at $vmem2(address)$ should be same as $pmem(ptable2(address))$.
- $glue3$ depicts that $retval2$ should be same as $retval$.

For unknown reasons, some of the proof obligations are not satisfied. But, according to rodin's version of refinement they must be satisfied as they are logically valid.

- In *memory*, event $write1$ and $write2$ both must satisfy invariant 1 and 2 as all the actions defined inside those 2 actions clearly obey the invariant criterion defined.
- In $memoryMMU$ the actions 1, 2, 3 of $INITIALISATION$ must satisfy the invariant 1, 2, 3 as they are defined in such a way.
- In $memoryMMU$ both $read1$ and $read2$ should satisfy $gluin3$ as from the gluing relation $gluing1$ and $gluing2$, $vmem1(addr)$ produces the same value as of $pmem(ptable1(addr))$ as they are glued to each other and $vmem2(addr)$ produces the same value as of $pmem(ptable2(addr))$ as they are glued to each other.
- Similarly, In $memoryMMU$ both $write1$ and $write2$ should satisfy $gluing1$ and $gluing2$ as both are initialized in such a way keeping in mind the separate address space for the page tables. They should satisfy the initialisation too as from the glued state theoretically, abstract memory is simulating the concrete virtual memory.

All the proof obligations are theoretically satisfying and so the concrete machine refines the abstract.