Matt Drummond
Final Project
ECE 645

Montgomery Multiplication
Verification Report: Arch1

Strategy for Verification:

The first architecture for this project involved only two VHDL modules that were not standard components. Standard in this instance refers to registers, shift registers, RAMs, and basic logic components. This leaves the Processing Elements (PEs) and then the logic that surround s the PEs.

Testing of the PE was rather straightforward, as it only really needed to test the results of additions as well as the selction of the output in the following clock cycle. This requires only 3 inputs, S_IN, Y, and M, where only the LSB of S_IN matters for selectoin of output.

The overall architecture was more difficult to test, but still simple. Y and M were the main inputs since many other signals are handled internally. Due to a testing issue (noted below) the method for verification of the overall circuit was changed from trying to match the test program's output. Instead, the circuit was tested for consistency given different inputs. The two test vectors have Y values which, when combined with the appropriate X input value, are expected to yield the same result. The result of the first is stored and compared to the result of the second, word-by-word. If this is a success, then the architecture is functioning consistantly.

Highest Level Tested:

Verification of the Surrounding Logic

- Entity Name: MontyMult_Arch1
- Testbench: MontyMult_Arch1_tb
- Vectors: MontyMult_vectorTable_first and MontyMult_vectorTable_second
- Result: Success, no errors reported. Multiplier does function consistantly and gives the expected results of consecutive equivalent multiplications.
- Sources of Error: None

Lower Level Verifications:

Verification of PEs

- Entity Name: PE_arch1
- Testbench: PE_arch1_tb
- Vectors: PE_vectorTable
- Result: Success. Addition results and output selection based on next cycle S_0 were correct.
- Sources of Error: None

Issues:

The expectation was that the tested architecture would output the same result as given by the test rogram provided. For neither Arch1 nor Arch2 was this the case. For this architecture the logic was written exactly as described by the Huang IEEE document but the results never matched. Very much of the available time was devoted to debugging this issue, but we were unable to fix it.