EE310 (Spring 2020) Due: 27/02/20, 23:55

Lab 1

Polynomial Multiplier Hardware in $\mathbf{Z}_{256}[x]/\langle x^4+1\rangle$

In this lab, you are required to design and implement a hardware which performs polynomial multiplication operation in ring $\mathbf{Z}_{256}[x]/\langle x^4+1\rangle$. In other words, your design takes two polynomials of degree 3 with coefficients in modulo 256 as inputs. Then, it performs polynomial multiplication operation where the resulting polynomial of degree 6 with coefficients in modulo 256 is calculated and then reduced to degree 3 with $\langle x^4+1\rangle$. Algorithm for the polynomial multiplication operation in ring $\mathbf{Z}_{256}[x]/\langle x^4+1\rangle$ is shown in Algorithm 1.

Algorithm 1 Polynomial Multiplication Operation in $\mathbf{Z}_{256}[x]/\langle x^4+1\rangle$

```
Input: $A(x) = A_3x^3 + A_2x^2 + A_1x^1 + A_0$ where $0 \le A_i < 256$
       $B(x) = B_3x^3 + B_2x^2 + B_1x^1 + B_0$ where $0 \le B_i < 256$
Output: $C(x) = C_3x^3 + C_2x^2 + C_1x^1 + C_0$ where $0 \le C_i < 256$
for $i$ from 0 to 7 do
    $T_i = 0$
end for

for $i$ from 0 to 3 do                                   ▷ Polynomial Multiplication
    for $j$ from 0 to 3 do
        $T_{i+j} = T_{i+j} + (A_i \cdot B_j) \pmod{256}$
    end for
end for

for $i$ from 0 to 3 do                                   ▷ Polynomial Reduction
    $C_i = T_i - T_{4+i} \pmod{256}$
end for
```

You are asked to design and implement two different versions of this operation: a full-combinational design and a low-area sequential design.

1. **Full-Combinational Polynomial Multiplier:** In your design, you are not allowed to use any sequential logic. Your hardware should work in 1 clock cycle. Write a behavioral Verilog model for your hardware design. In your Verilog model, your Verilog module should have the following interface:

```
module PolMulComb(A3,A2,A1,A0,B3,B2,B1,B0,C3,C2,C1,C0);
    input  [7:0]  A3,A2,A1,A0,B3,B2,B1,B0;
    output  [7:0]  C3,C2,C1,C0;

    // ...

endmodule
```

2. **Low-Area Sequential Polynomial Multiplier:** In your design, you should use sequential logic. For implementing your operation, you are allowed to use only one integer multiplier, one adder and one subtractor. Your design should start its operation after *start* input is 1 for one clock cycle. Then, it should perform the operation and set *finish* output as 1 after finishing the operation. Write a behavioral Verilog model for your hardware design. In your Verilog model, your Verilog module should have the following interface:

```verilog
module PolMulSeq(clk,rst,start,A3,A2,A1,A0,B3,B2,B1,B0,finish,C3,C2,C1,C0);
    input clk,rst,start;
    input [7:0] A3,A2,A1,A0,B3,B2,B1,B0;
    output reg finish;
    output reg [7:0] C3,C2,C1,C0;

    // ...

endmodule
```

You should also write Verilog testbenchs that verify the correctness of your Verilog models for both designs. In these testbenchs, you should apply input values to your model and compare its outputs with the expected results (check Class_Notes_Week#3.zip on SUCourse for example). You should create 50 test inputs (and their expected outputs) for your design and read these inputs/outputs from _*.txt_ files in your testbench. You can create these test inputs/outputs using any programming language you prefer (Python, C/C++, MATLAB etc.). Please note that you should generate your own test cases. Using your friend's test cases will be considered as plagiarism. After verifying the correctness of your design, synthesize and implement your design on Spartan-3E FPGA using Xilinx ISE WebPack 14.7. Then, you should write a lab report (in .pdf format) with *readable* English and good structure (dumping many figures and raw synthesis/implementation reports into a pdf file is not a lab report.). Your report should include the following information:

1. Write a summary of the assignment. Among the things to consider are: what did you learn, what are the challenges of the assignment, what are the straight-forward parts, what are the differences between two designs (in terms of design effort and approach)?

2. What is the hardware area-cost (slices, register, LUTs, DSPs, BRAMs, etc.) of your design? What is the maximum achievable frequency of your design?

3. How many clock cycles does it take to finish one polynomial multiplication operation for both designs? Compare both design in terms of speed/area.

Finally, put all of your Verilog projects, your script to generate test vectors and your report into one ".zip" file named Lab1_username1_username2.zip (e.g. Lab1_berkea_erdinco.zip) and submit this zip file using EE310 SUCourse website. Please note that we will use a plagiarism detection software for your lab assignments.