EE577A Fall 2019 – VLSI System Design

Instructor: Prof. Massoud Pedram TA: Hongxiang Gao

Final Project Part I:

Montgomery Modular Multiplication Unit Based on reduction algorithm

---

Notes:

- This project is group work, 2 students at most in a team.
- The cells you designed in this lab are going to be used in your final project
- Submit your final report on the Blackboard website.
- Ask questions only on blackboard discussion forum or in the office hours. DO NOT send email asking technical questions.
- Start as soon as possible.

Introduction

Design a modulo operation unit based on Barrett Reduction Algorithm. Figure 1 shows the schematic diagram of the design.

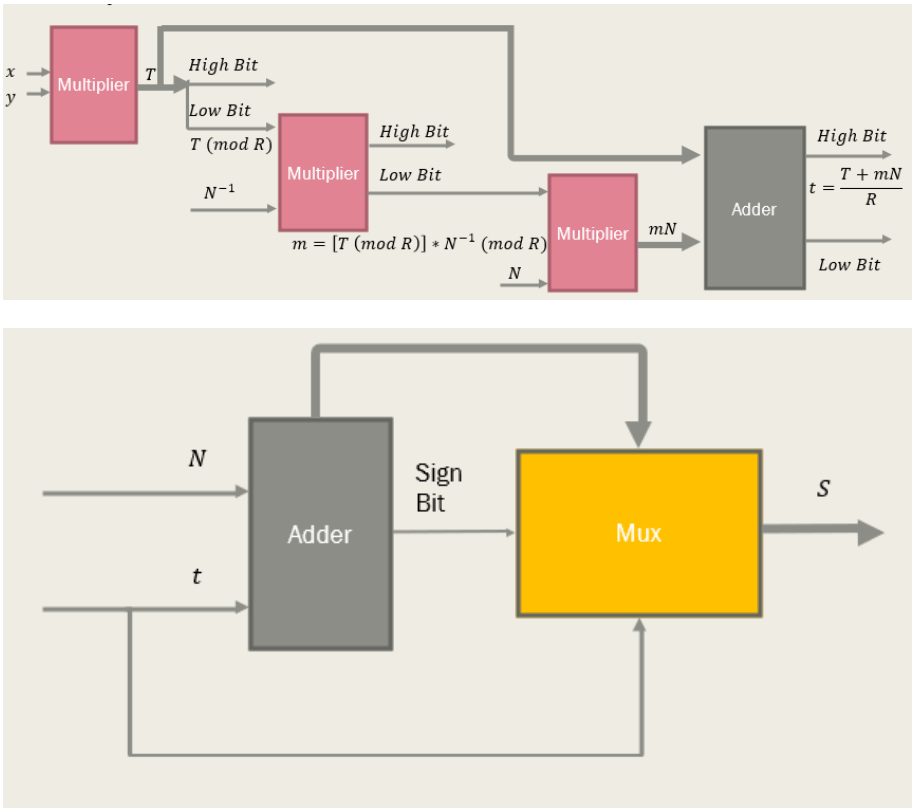

Figure 1: Design flow of modular multiplication unit

General Instructions

a) Use $\beta = \mu_n/\mu_p = 4$ for all gates in your design.
b) You may use the multiplier unit you designed in lab 1.
c) You are not required to sizing the transistors at this time. For simplicity, you can size all NMOS as 300 nm and all PMOS as 1.2 µm.
d) Use $V_{DD} = 1.8V$.
e) All inputs and outputs of the modulo unit need to be registered with positive-edge triggered master-slave flip-flops.
f) Use rise/fall time = 10 ps.
g) You are not required to measure the worst cases delay, but the clock you set of FFs should be large enough to avoid the setup-time violation.

Layout Guidelines

a) The height of all your designs of one level should be 50-60 lambdas which is 5-6 µm in NCSU_TechLib_tsmc02 technology. The height of one level is measure from the middle of power rail to the middle of ground rail.
b) VDD and GND should be routed in metal 1 at top and bottom of the cell. The metal width of VDD and GND should be 10 lambdas (1 µm).
c) For the internal routing you can use poly (usually for short routing) or metal layer. (you may use any metal layer up to metal 4.) We recommend you use metal 1 for horizontal and metal 2 for vertical connections or vice versa. Try to use as few metal layers as possible therefore routing would be more convenient for your future assignments which may use this part.
d) You will have to try building your layout looks like a square shape. All the input signals should be given from the sides and all the output signal should be connected at the right-hand side.

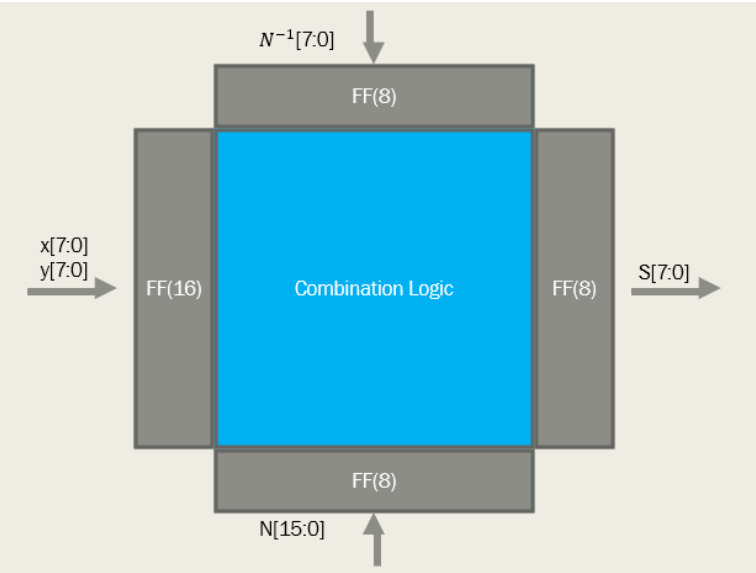

Figure 2: Block diagram of layout

Functionality Test

You will have to perform the functionality test using the input patterns generated by Perl or Python:

a) Design the Perl/Python script which can randomly generates input pattern and its corresponding result in both decimal and binary format.

b) For the value of N^{-1}, you can directly calculate it in your Python/Perl program and convert it to the 8-bit value as a part of the input pattern.

c) Fill in the table given below (a sample is given) after running your script. (You will have to generate other four different test cases)

x (dec)	y (dec)	N (dec)	N^{-1} (dec)	S (dec)	x (bin)	y (bin)	N (bin)	N^{-1} (bin))	s (bin)
8	57	5	51	2	00001000	00111001	00000101	00110011	00000010

d) Apply the patterns in Cadence and compare the waveforms with the result generated above. You can either use vector file or directly set the input patterns in Cadence while vector file is preferred since in future lab assignments the input patterns will be much more complicated.

Report Checklist

a) Schematics and layout of the modulo unit.

b) LVS match report of the modulo unit.

c) Completed Perl/Python script and table of test patterns generated by your script. (It would be appreciated if you can add some comments in your script.)

d) Functionality test waveforms of both schematics and layout of the modulo unit.

e) A summary of key parameters of your design, including the minimum clock, height, width and area of your layout.

Submission Guidelines

a) Briefly explain your work.

b) Name your report file in following format:
"firstname_lastname_studentID_Final_Part1_EE577A_Fall19.pdf", for example:
"Hongxiang_Gao_1111111111_Final_Part1_EE577A_Fall19.pdf"