Assignment 1

Yara Shamali 315892141 Samih Warwar 324888155 Maias Omar 322645748

March 21,2023

Truth Table Q1

$$f_{a,4}(x) = \begin{cases} 1 & \text{if } ax \geq 4 \\ 0 & \text{otherwise} \end{cases}$$

Truth table for the function in Equation 2:

xa	0	1	2	3
0	0	0	0	0
1	0	0	0	0
2	0	0	1	1
3	0	0	1	1

Boolean Circuit Q2

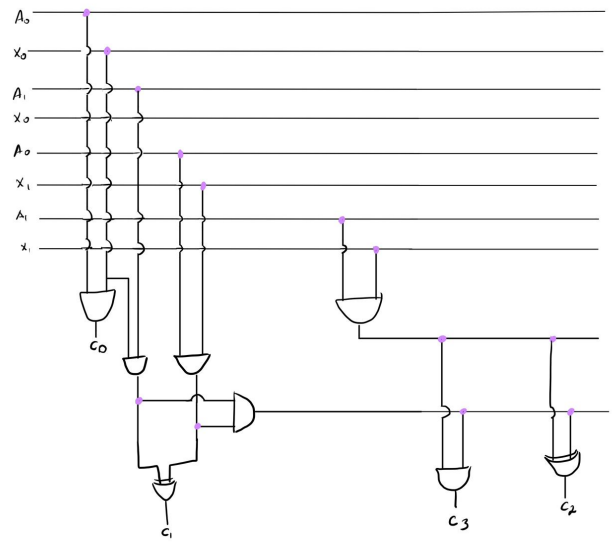
First of all, we'll use a "mul" box and an "add" box:

$$f_{\vec{a},4}(x_1, x_2) = \begin{cases} 1 & \text{if } a_1x_1 + a_2x_2 \geq 4 \\ 0 & \text{otherwise} \end{cases}$$

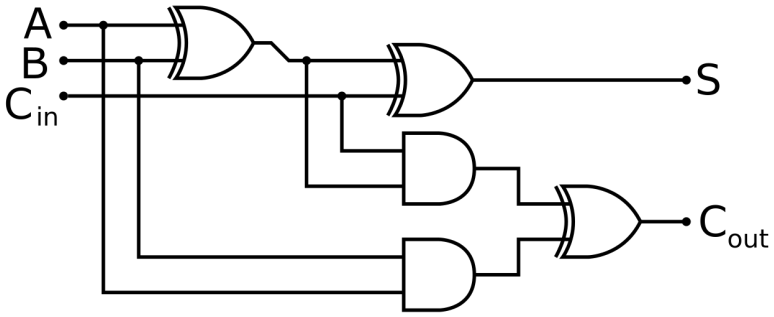
The truth table for the "mul" box is shown below:

a \ b	00	01	10	11
00	0000	0000	0000	0000
01	0000	0001	0010	0011
10	0000	0010	0100	0110
11	0000	0011	0110	1001

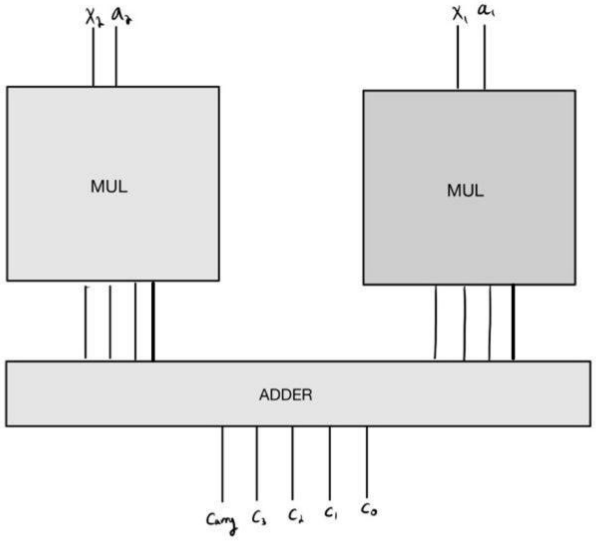
MUL implementation using XOR and AND gates:



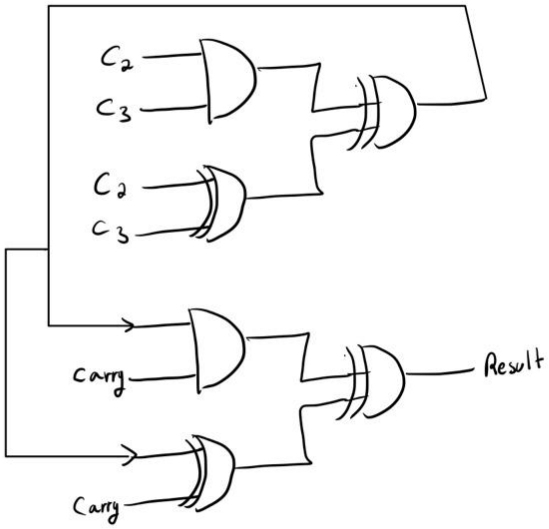
And now we'll make the full-adder



then we combine them :

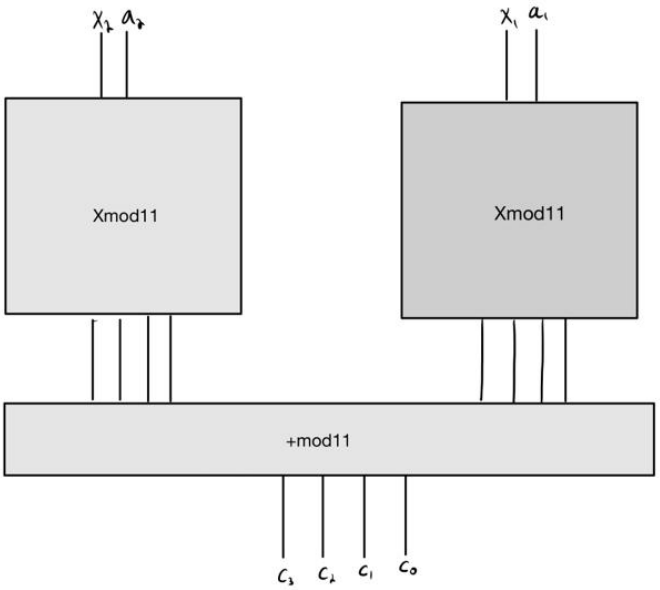


Now to check if the number is greater or equal to 4 we'll take the 3 MSB (including the carry) carry, C3 , C2

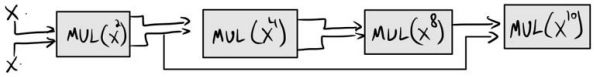


Arithmetic Circuit Q3

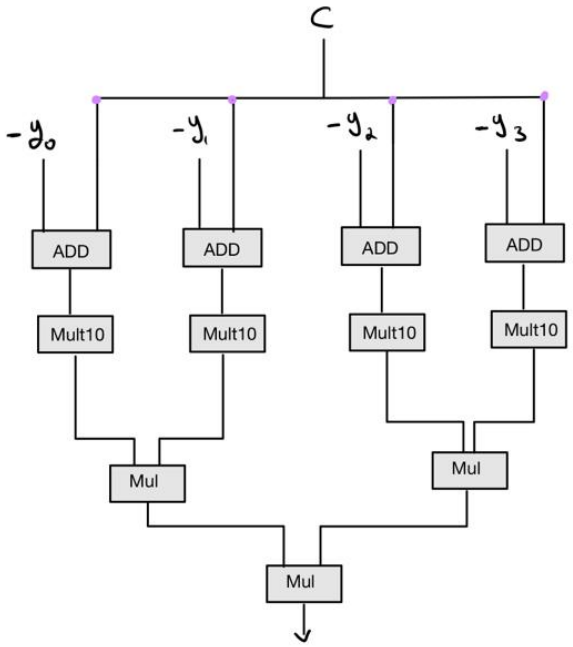
So first of all we want the output after the mul and the add which is:



Now we want to compute MUL10



to check if the number is greater or equal to 4 we'll check if the number is 0 or 1 or 2 or 3 and return 0 Based on Fermat's little theorem , if two numbers x,y are equal in GF(11) if and only if : $(x-y)^n$
for every y=0,1,2,3 if none if these result is 0 we want to return 1.
well define C=c3c2c1c0 , y0=0, y1=1, y2=2, y3=3



Analyze the complexity Q4

in Arithmetic Circuit there is Four mul10, in every mul10 there is 4mult and in the final circuit there is 4 more so #MULT = 21
and the x-depth= 7
in addition there is 5 adders so the total size is 26 and the total depth is 9

in the Boolean circuit we used 2 "muls" of depth 3 consisting of 6 AND gates + 2 XOR gates each ,with total of 16 in size.
we also used 4 full consecutive adders each of depth 3 making the 4 adders of depth 12, each consisting of 2 AND gates +3 XOR gates , with total of 20 in size .
lastly the "MSB checks" consisted of 2 AND gates + 4 XOR gates of depth 4 .
to summarize our boolean circuit is of depth 17 and size 42.