HW-4:-

VIKAS KUMAR RAO
U10725966.

1) 3-bit Mastrovito multiplier over galois field $F_8 = F_{2^3} = F_2(x) (\bmod p(x))$.

a) mastrovito matrix

$$
\begin{array}{ccccc}
 & & a_2 & a_1 & a_0 \\
 & & b_2 & b_1 & b_0 \\
\hline
 & & a_2b_0 & a_1b_0 & a_0b_0 \\
 & a_2b_1 & a_0b_2 & a_0b_1 & \\
a_2b_2 & a_1b_2 & a_1b_1 & & \\
\hline
s_4 & s_3 & s_2 & s_1 & s_0
\end{array}
$$

poly expression:-

$$S = s_0 + s_1x + s_2x^2 + s_3x^3 + s_4x^4$$

Since irreducible polynomial is suggested to be degree 3, let $p(x) = x^3 + x + 1$.

s_0, s_1, s_2 are not reducible & hence retained

$$s_3x^3 (\bmod(p(x))) = s_3(x+1) = s_3x + s_3$$
$$s_4x^4 (\bmod(p(x))) = s_4(x+1)x = s_4x^2 + s_4x.$$

for word-level representation.

$Z = z_0 + z_1x + z_2x^2$

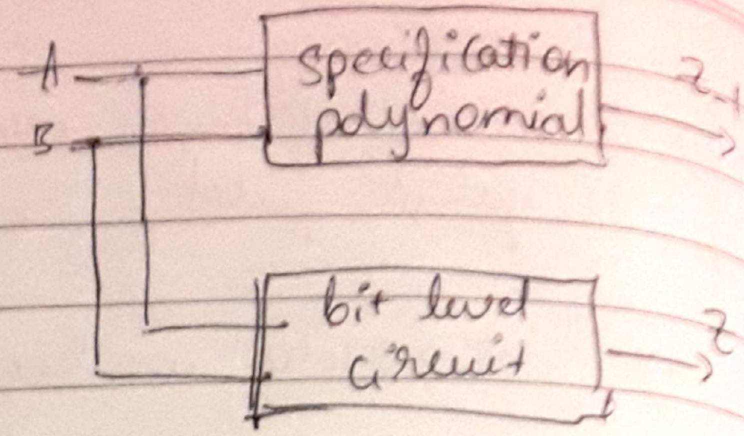
inputs

$A = a_0 + a_1x + a_2x^2$

$B = b_0 + b_1x + b_2x^2$

$$
\begin{array}{cccl}
x^2 & x^1 & x^0 & \\
s_2 & s_1 & s_0 & \\
 & s_3 & s_3 & // s_3x^3 \\
s_4 & s_4 & & // s_4x^4 \\
\hline
z_2 & z_1 & z_0 &
\end{array}
$$

b) verification over strong null etellen lat z.



To verify the above circuit equivalence we will do a membership testing of specification polynomial and see if the actual circuit implements the same. To check for equivalence using strong nullstellensatz, we need to see if the specification polynomial vanishes on all solutions of the circuit implementation.

Specification polynomial:-

$$f = Z_1 - A * B.$$

where, A & B are word level inputs.

Implementation polynomial:-

polynomial for each implemented gate is written in terms of 'AND' & 'XOR'.

Attached "hw-4-masthovito.sing" contains the singular implementation of the same with all equations.

once we have the ideals for all the circuit & vanishing polynomials we will find the Gröbner basis and see if the remainder vanishes to '0' when divided recursively.

$$f \xrightarrow{GB(J+J_0)}_{+} 0$$

$J+J_0 \rightarrow$ ideal from the circuit & specification polynomial & vanishing polynomials.

If the remainder is '0', Then the equivalence is proved.

(2)

a_2	a_1	a_0	A	z_2	z_1	z_0	Z
0	0	0	0	0	0	0	0
0	0	1	1	0	0	1	1
0	1	0	x	0	1	0	x^2+x+1
0	1	1	$x+1$	0	1	1	x^2+x+1
1	0	0	x^2	1	0	0	x^2+1
1	0	1	x^2+1	1	0	1	$x+1$
1	1	0	x^2+x	1	1	0	x^2+1
1	1	1	x^2+x+1	1	1	1	x^2+1

Lagrange's interpolation formula is used to obtain 'Z' in terms of A as the polynomial representation of the function.

minimal canonical polynomial representation is derived using

$Z = FA.$

Lagrange's formula is given as

$$F(x) = \sum_{n=1}^{q} \frac{\Pi_{i\neq n}(x-x_i)}{\Pi_{i\neq n}(x_n-x_i)} f(x_n).$$

* Canonical representation.

K-map:

$$Z = (x^2+x+1)A^7 + (x^2+1)A^6 + xA^5 + (x+1)A^4 + (x^2+x+1)A^3 + (x^2+1)A.$$

Z_0

$a_2 \backslash a_1a_0$	00	01	10	11
0	0	1	1	1
1	1	1	1	1

$Z_0 = a_0 + a_1 + a_2$

Z_1

$a_2 \backslash a_1a_0$	00	01	10	11
0	0	0	1	1
1	0	1	0	0

$Z_1 = a_1\bar{a}_2 + a_0\bar{a}_1a_2.$

Z_2

$a_2 \backslash a_1a_0$	00	01	10	11
0	0	0	1	1
1	1	0	1	1

$Z_2 = a_1 + \bar{a}_0a_2.$

All The circuit ~~in~~ equations are implemented in Singular and verified for equivalence.

We apply weak nullstellensatz on ~~that~~ the equations to verify equivalence.

We check if $G = GB(J) = \{1\}$ to verify if specification polynomial & implementation polynomials are same

(3) $\alpha_1, \alpha_2, \ldots \alpha_t \to$ arbitrary elements in F_{2^k}.

to prove,

$$(\alpha + \alpha_2 + \cdots + \alpha_t)^{2^i} = \alpha_1^{2^i} + \alpha_2^{2^i} + \cdots + \alpha_t^{2^i}$$

for $i = 1, 2, \ldots$

let $S(n) = (\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{2^i}$.

By induction, let's try to prove

i) $S(1)$ is true

ii) If $S(k)$ is true, then $S(k+1)$ is also true

$$S(1) = (\alpha_1 + \alpha_2 + \cdots + \alpha_t)^2$$

$$= \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_t^2 + (2\alpha_1\alpha_2 + 2\alpha_2\alpha_3 + \cdots + 2\alpha_{t-1}\alpha_t).$$

Since, $\alpha_1, \alpha_2, \ldots \alpha_t$ are in F_{2^k}

$(2\alpha_1\alpha_2 + 2\alpha_2\alpha_3 + \cdots + 2\alpha_t\alpha_{t+1})$. (mod 2) will be zero.

Thus, $S(1) = \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_t^2$.

$$\therefore \underline{(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^2 = \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_t^2} \longrightarrow (1)$$

let's assume $S(k)$ to be true.

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{2^k} = \alpha_1^{2^k} + \alpha_2^{2^k} + \cdots + \alpha_t^{2^k} \longrightarrow (2)$$

$S(k+1)$

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{2^{k+1}} = \left[(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{2^k}\right]^2$$

$$= \left[(\alpha_1^{2^k} + \alpha_2^{2^k} + \cdots + \alpha_t^{2^k})^2\right] \text{ from (1) \& (2)}$$

$(\alpha_1 + \alpha_2 + \ldots + \alpha_t)^{2^{k+1}} = \alpha_1^{2^{k+1}} + \alpha_2^{2^{k+1}} + \ldots + \alpha_t^{2^{k+1}}$

is true for all positive integers for

$\therefore$

$(\alpha_1 + \alpha_2 + \ldots + \alpha_t)^{2^i} = \alpha_1^{2^i} + \alpha_2^{2^i} + \ldots + \alpha_t^{2^i}$

(4) for $F_{16} = F_2(x)$ (mod $p(x)$).

$p(x) = x^4 + x^3 + x^2 + x + 1$. & $p(\alpha) = 0$.

primitive element of a field is an element which generates rest of the elements in the field.

All non-zero elements can be generated from α^i for some integer i

clearly α is not a primitive element of this irreducible polynomial $p(x)$.

Since $\alpha^5 = 1$, the elements repeat after α^5 and prevents from further generation of elements.

But $(\alpha + 1)$ can generate all other elements in the field.

Irrespective of any irreducible polynomial, the exponential representation of element in

$F_{2^4} = F_{16}$ is the same.

Thus $(\alpha+1)$ can be represented as α^{12}. ~~from the~~

we can derive them using

$$p(x) = x^4 + x^3 + 1.$$

$$\therefore (\alpha+1) = \alpha^{12} = \beta.$$

$$\underline{\underline{\beta = \alpha^{12}.}}$$

$(\alpha+1)$ can be checked as follows.

$$(\alpha+1)^2 = \alpha^2+1$$

$$(\alpha+1)^3 = \alpha^3+\alpha^2+\alpha+1$$

$$(\alpha+1)^4 = \alpha^3+\alpha^2+\alpha$$

$$(\alpha+1)^5 = \alpha^3+\alpha^2+1$$

$\vdots$ and so on...

Thus $(\alpha+1)$ can be used to generate the entire field.