Q 3

Design of a 3-bit Mastrovito Multiplier.

$F_8 = F_2[x] \pmod{P(x) = x^3+x+1}$

$\alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$

$\alpha^4 = \alpha^2 + \alpha$

$Z = A \cdot B$.

$A = a_0 + a_1\alpha + a_2\alpha^2$

$B = b_0 + b_1\alpha + b_2\alpha^2$

$$A \cdot B = \left(\sum_{i=0}^{2} a_i \alpha^i\right) \cdot \left(\sum_{i=0}^{2} b_i \alpha^i\right) = (a_0 + a_1\alpha + a_2\alpha^2)(b_0 + b_1\alpha + b_2\alpha^2)$$

$$= a_0b_0 + a_0b_1\alpha + a_0b_2\alpha^2 + a_1b_0\alpha + a_1b_1\alpha^2 + a_1b_2\alpha^3 + a_2b_0\alpha^2 + a_2b_1\alpha^3 + a_2b_2\alpha^4$$

$$= \begin{pmatrix} a_0b_0 \\ + \\ a_1b_2 \\ + \\ a_2b_1 \end{pmatrix} + \begin{pmatrix} a_0b_1 \\ + \\ a_1b_0 \\ + \\ a_1b_2 \\ + \\ a_2b_1 \\ + \\ a_2b_2 \end{pmatrix}\alpha + \begin{pmatrix} a_0b_2 \\ + \\ a_1b_1 \\ + \\ a_2b_0 \\ + \\ a_2b_2 \end{pmatrix}\alpha^2$$

$$= z_0 + z_1\alpha + z_2\alpha^2$$

[See the singular file of the design + miter]