Solution to HW 4:

2) K-map for output $Z_0, Z_1$ and $Z_2$:

$Z_0$

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

$a_2$, $a_0$, $a_1$

$Z_0 = a_0 \vee a_1 \vee a_2$

$Z_1$

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

$a_1\bar{a}_2$, $a_0\bar{a}_1a_2$

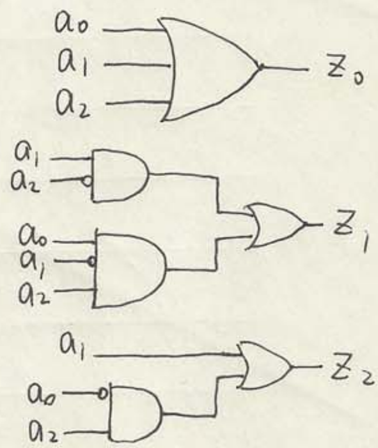
$Z_1 = (a_1\bar{a}_2) \vee (a_0\bar{a}_1a_2)$

$Z_2$

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

$a_1$, $\bar{a}_0a_2$

$Z_2 = a_1 \vee (\bar{a}_0 \wedge a_2)$




Draw a circuit based these Boolean functions.

Lagrange's interpolation: given N pairs of $(x, y)$ coordinates, fit them to a $(N-1)$ degree (at most) polynomial function, $f(x)$, this function can be written as:

$$f(x) = \sum_{k=1}^{N}\left[\frac{\prod_{i\neq k}(x - x_i)}{\prod_{i\neq k}(x_k - x_i)} \cdot y_k\right]$$

In this problem, $x \leftarrow A$, $y \leftarrow Z$. Write $(A, Z)$ in form of elements from $F_{2^3}$, we have 8 pairs of $(x, y)$ in total:

$(a_2\alpha^2+a_1\alpha+a_0,\ z_2\alpha^2+z_1\alpha+z_0) \leftarrow (A, Z)$

e.g. $(\alpha,\ \alpha^2+\alpha+1) \leftarrow (010, 111)$

$(\alpha^2+\alpha,\ \alpha^2+1) \leftarrow (110, 101)$

...

Use Lagrange's interpolation, we get function $f(x)$ as a polynomial about A at most degree 7.

We can write several lines of Singular script to do this work.

Result is: $f(A) = (\alpha^2+\alpha+1)A^7 + (\alpha^2+1)A^6 + \alpha A^5 + (\alpha+1)A^4 + (\alpha^2+\alpha+1)A^3 + (\alpha^2+1)A$.

Miter building: let specification word-level variable $Z\_1 = f(A)$

polynomial $t\cdot(Z - Z\_1) - 1 = 0$ guarantees that $Z$ is different from $Z\_1$: $Z - Z\_1$ can take any value from $F_{2^3}$ except 0.

If Gröbner basis reduced to 1, according to Weak Nullstellensatz it means no solution to this system unless miter output is always 0, i.e. circuit's function is equivalent to specification function.

3) First, prove $(a+b)^2 = a^2+b^2$, $a,b \in F_{2^k}$

↳ $(a+b)^2 = a^2+b^2+2ab$

Assume $a = C_{k-1}\alpha^{k-1} + C_{k-2}\alpha^{k-2} + \cdots + C_0$, $C_i \in F_2$

then $2a = 2C_{k-1}\alpha^{k-1} + 2C_{k-2}\alpha^{k-2} + \cdots + 2C_0 = 0$ $(2C_i \equiv 0)$

$\therefore a^2+b^2+2ab = a^2+b^2$.

Then, expand: prove $(a+b)^{2^i} = a^{2^i} + b^{2^i}$, $a,b \in F_{2^k}$.

↳ $(a+b)^2, \cdots, (a+b)^{2^{i-1}}, (a+b)^{2^i} \in F_{2^k}$

$$\therefore (a+b)^{2^i} = (\cdots((a+b)^2\underbrace{)^2\cdots)^2}_{i}$$

$$= (\cdots(a^2+b^2\underbrace{)^2\cdots)^2}_{i-1}$$

$$= (\cdots(a^{2^2}+b^{2^2}\underbrace{)^2\cdots)^2}_{i-2}$$

$$\cdots$$

$$= (a^{2^{i-1}}+b^{2^{i-1}})^2 = a^{2^i}+b^{2^i}$$

Final expansion: prove $(a_1+a_2+\cdots+a_t)^{2^i} = a_1^{2^i}+a_2^{2^i}+\cdots+a_t^{2^i}$,

$a_1, \cdots, a_t \in F_{2^k}$.

↳ $a_2+\cdots+a_t \in F_{2^k}$, $\therefore (a_1+(a_2+\cdots+a_t))^{2^i} = a_1^{2^i} + (a_2+\cdots a_t)^{2^i}$

Subsequently, $(a_2+(a_3+\cdots+a_t))^{2^i} = a_2^{2^i} + (a_3+\cdots+a_t)^{2^i}$

$\cdots$

$(a_1+a_2+\cdots+a_t)^{2^i} = a_1^{2^i}+a_2^{2^i}+\cdots+a_t^{2^i}$. ∎

4) $x^4+x^3+x^2+x+1$ is a minimal polyromial, but NOT a primitive polyromial for $F_{2^4}$, because:

$$x^5 = x(x^4) = x\cdot(x^3+x^2+x+1)$$
$$= x^4+x^3+x^2+x = 1 = x^0$$

But it is possible to represent a primitive element by a linear combination of powers of non-primitive element.

Assume $\beta = C_3\alpha^3 + C_2\alpha^2 + C_1\alpha^1 + C_0$ , $C_i \in F_2$

Do exhaustive search.

We know $x^4+x^3+1$ is a primitive polyromial, which means if $\beta$ is ~~primitive~~ a root of $x^4+x^3+1=0$ $\beta$ must be primitive element.

Check when $\beta^4+\beta^3+1=0$, record $\beta$ as primitive element.

Result: $\beta = \alpha^3+\alpha^2+\alpha$. or $\alpha^3+1$ or $\alpha^2+1$ or $\alpha+1$

If use another primitive polynomial $x^4+x+1$, results are:

$\beta = \alpha^2+\alpha$, or $\alpha^2+\alpha+1$, or $\alpha^3+\alpha$, or $\alpha^3+\alpha+1$

Thus we find primitive elements represented by non-primitive elements.