ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

Decomposition of $\mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle$ into direct product of sub rings

Ashwani Kumar[1], Manju Pruthi[2]

Department of Mathematics, Indira Gandhi University, Meerpur (Rewari)

Haryana – 122502

Abstract: Let $\mathbb{F}_q$ be a finite field of q elements such that $q \equiv 3(mod 8)$ and p be an odd prime with $p^l \parallel q-1$ for integer $l>0$ and $4 \nmid q-1$. In this paper, we intend to decompose the ring $\mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle$ into direct product of sub rings. For this, we obtain irreducible factors of $x^{32}-1$ over $\mathbb{F}_q$.We also factorized $x^{32p^n}-1$ into its$17p^n$ irreduciblefactors over $\mathbb{F}_q$ and obtained the required result by proving some lemmas.

MSC:11T06, 94B05, 94B15

Keywords: Finite fields, irreducible factors, direct product, natural$\mathbb{F}_q$- algebra isomorphism.

1. Introduction

Let $\mathbb{F}_q$be a finite field with q elements. Let $\mathcal{C}$ be a [m, k] linear code over $\mathbb{F}_q$, that is, it is a $k-$ dimensional sub space of $\mathbb{F}_q^m$. A code $\mathcal{C}$ is called cyclic if any cyclic shift given to a code word is again a code word. A code word $(c_0, c_1, c_2, \dots, c_{m-1})$in $\mathcal{C}$ is identified with the polynomial $c_0+c_1x+c_2x^2+\cdots+c_{m-1}x^{m-1}$ in $\mathbb{F}_q[x]/\langle x^m-1\rangle$. In fact a code $\mathcal{C}$ of length m over$\mathbb{F}_q$is a cyclic code if and only if the corresponding sub set is an ideal of $\mathbb{F}_q[x]/\langle x^m-1\rangle$. Every cyclic code $\mathcal{C}$ of length m is generated by a unique monic divisor $g(x)$ of minimal degree in $\mathbb{F}_q$.Irreducible cyclic code of length m over $\mathbb{F}_q$ can be viewed as ideals of the ring$\mathbb{F}_q[x]/\langle x^m-1\rangle$ generated by the primitive idempotents. Decomposition of quotient rings into direct product of subrings over a finite field plays an important role to find generating idempotents.

A lot of papers in which the decomposition of quotient rings into direct product of sub rings have been done to find generating idempotents of irreducible cyclic codes given as follows: In [5] Fengwei Li and Yue et.al.found minimum Hamming distances of irreducible cyclic codes. They obtained primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^m-1\rangle$by decomposition of ring $\mathbb{F}_q[x]/\langle x^m-1\rangle$into direct product of sub rings, where $m=l_1^{n_1}l_2^{n_2}$; $l_1, l_2$are distinct primes,$n_1, n_2 \geq 1$and$l_1l_2 \mid q-1$, q is prime power. In [7] Yuqian,Yansheng Wei and Qin Yue gave the expression of decomposition of ring $R_m=\mathbb{F}_q[x]/\langle x^m-1\rangle$ to find primitive idempotents of irreducible cyclic codes of length m over $\mathbb{F}_q$, where $m=p_1^{n_1}p_2^{n_2}\dots p_l^{n_l}$; $p_i$for $1 \leq i \leq l$are distinct primes and $n_i \geq 1$for $1 \leq i \leq l$ such that $p_1p_2\dots p_l \mid q-1$and $\gcd(m,q)=1$. In [6] Fengui Li and Yue et. al. decomposed the quotient ring $\mathbb{F}_q[x]/\langle x^m-1\rangle$ into direct product of sub rings and gave explicit expressions of primitive idempotents in two rings $\mathbb{F}_q[x]/\langle x^m-1\rangle$ for $m=4p^n, 8p^n$, where $q \equiv 3(mod 8)$ and $p \mid q-1$with p an odd prime.

This paper is organized as follows: In section 2, we recall some lemmas. In section 3 we prove some lemmas and in section4, the decomposition of ring $\mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle$into direct product of sub rings is given by using the lemmas proved in section 3.

2. Preliminaries

A criterion on irreducible binomials over $\mathbb{F}_q$ was given by Serretin 1866

Lemma 2.1. Assume that $n \geq 2$. For any $a \in \mathbb{F}_q$ with $\mathrm{Ord}(a)=k$, the binomial x^n-a is irreducible over $\mathbb{F}_q$ if and only if both the following conditions are satisfied :

1. Every prime divisor of n divides k, but does not divide $\frac{q-1}{k}$;
2. If $4/n$, $then$ $4/(q-1)$.

Lemma 2.2. Let $\alpha \in \mathbb{F}_q be\ a\ root\ of\ x^n-1, where\ \gcd(q,n)=1. Then$

$$\sum_{i=0}^{n-1}\alpha^i=\begin{cases}0 & if\ \alpha \neq 1\\ n & if \alpha = 1.\end{cases}$$

Wealso have a well-known result about irreducibility for composition of polynomials.

Lemma2.3. Let l be a positive integer, $P(X) \in \mathbb{F}_q[X]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $n > 0$.Suppose that $P(0) \neq 0$ and $P(X)$ is of period d,which is equal to the order of any root of $P(X)$.Then $P(X^l)$ is irreducible over $\mathbb{F}_q$, if only if the following conditions three conditions satisfied:

1. Each prime divisor of l/d;**2.** $gcd\left(l, \frac{q^n-1}{d}\right) = 1$ **3.** if $4/l$, then$4 /(q^n - 1)$

3. Decomposition of $\mathbb{F}_q[x]/\left(x^{32p^n} - 1\right)$

Let p be an odd prime and$\mathbb{F}_q$be a finite field with q elements, where $q = 8k + 3$for some k and$p^l \parallel q - 1$ for integer $l > 0$ and $4 \nmid q - 1$.We have an irreducible factorization of $x^{32} - 1$ over $\mathbb{F}_q$as follows:

$$x^{32} - 1 = (x \pm 1)(x^2 + 1)\left(x^2 \pm \sqrt{-2}x - 1\right)\left(x^2 \pm \sqrt{-(2 - \sqrt{2})}x - 1\right)\left(x^2 \pm \sqrt{-(2 + \sqrt{2})}x - 1\right)\left(x^2 \pm \sqrt{-(2 - \sqrt{2 + \sqrt{2}})}x - 1\right)\left(x^2 \pm \sqrt{-(2 + \sqrt{2 + \sqrt{2}})}x - 1\right)\left(x^2 \pm \sqrt{-(2 - \sqrt{2 - \sqrt{2}})}x - 1\right)\left(x^2 \pm \sqrt{-(2 + \sqrt{2 - \sqrt{2}})}x - 1\right)$$

3.1. when $n \leq l$

Let α^{-1} be a p^n-th primitive root of unityover $\mathbb{F}_q$, then irreducibility factorization of $x^{32p^n} - 1$ over $\mathbb{F}_q$ is as follows:

$$x^{32p^n} - 1 = \prod_{k=0}^{p^n-1}(x \pm \alpha^{-k})(x^2 + \alpha^{-2k})\left(x^2 \pm \sqrt{-2}\alpha^{-k}x - \alpha^{-2k}\right)\left(x^2 \pm \sqrt{-(2 - \sqrt{2})}\,\alpha^{-k}x - \alpha^{-2k}\right)\left(x^2 \pm \sqrt{-(2 + \sqrt{2})}\alpha^{-k}x - \alpha^{-2k}\right)\left(x^2 \pm \sqrt{-(2 - \sqrt{2 + \sqrt{2}})}\alpha^{-k}x - \alpha^{-2k}\right)\left(x^2 \pm \sqrt{-(2 + \sqrt{2 + \sqrt{2}})}\alpha^{-k}x - \alpha^{-2k}\right)\left(x^2 \pm \sqrt{-(2 - \sqrt{2 - \sqrt{2}})}\alpha^{-k}x - \alpha^{-2k}\right)\left(x^2 \pm \sqrt{-(2 + \sqrt{2 - \sqrt{2}})}\alpha^{-k}x - \alpha^{-2k}\right)$$

$$x^{32p^n} - 1 = \prod_{k=0}^{p^n-1}(x \pm \alpha^{-k})(x^2 + \alpha^{-2k})\left(x^2 \pm \sqrt{-2}\alpha^{-k}x - \alpha^{-2k}\right)(x^2 \pm \lambda_1\alpha^{-k}x - \alpha^{-2k})(x^2 \pm p_2\alpha^{-k}x - \alpha^{-2k})\,(x^2 \pm q_1\alpha^{-k}x - \alpha^{-2k})(x^2 \pm q_2\alpha^{-k}x - \alpha^{-2k})(x^2 \pm\, r_1\alpha^{-k}x - \alpha^{-2k})(x^2 \pm r_2\alpha^{-k}x - \alpha^{-2k})$$

Where$\lambda_1 p_1 = \sqrt{-(2 - \sqrt{2})},\ \lambda_2 p_2 = \sqrt{-(2 + \sqrt{2})}, \eta_1 q_1 = \sqrt{-(2 - \sqrt{2 + \sqrt{2}})},$

$$\eta_2 q_2 = \sqrt{-(2 + \sqrt{2 + \sqrt{2}})}\,, \rho_1 r_1 = \sqrt{-(2 - \sqrt{2 - \sqrt{2}})}\,, \rho_2 r_2 = \sqrt{-(2 + \sqrt{2 - \sqrt{2}})}$$

Lemma 3.1.*Let* $f_k(x) = x^2 — \eta_1\alpha^{-k}x - \alpha^{-2k},\ k = 0,1, \dots, p^n - 1\ and\ x^j \equiv a_0^{(j,k)} + a_1^{(j,k)}x\ (mod\ f_k(x)),\ j = 0, 1, \dots, 32p^n - 1$.*Then*$a_0^{(j,k)} + a_1^{(j,k)}$ *is as follows:*

$$
\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^u\eta_1\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^u\eta_1\alpha^{-(16u+3)k}+(-1)^u\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^u\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+4)k}+(-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+2)k}x, & if\ j=16u+4,\\
(-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+5)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+6)k}+(-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+7)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+6)k}x, & if\ j=16u+7.\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+8)k}+(-1)^u\sqrt{2}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+7)k}x, & if\ j=16u+8\\
(-1)^u\sqrt{2}\sqrt{2+\sqrt{2}}q_1\alpha^{-(16u+9)k}+(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+10)k}+(-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+9)k}x, & if\ j=16u+10\\
(-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+11)k}+(-1)^u\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+10)k}x, & if\ j=16u+11\\
(-1)^u\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+12)k}+(-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+13)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+14)k}+(-1)^u\eta_1\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^u\eta_1\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}
$$

Proof. Suppose β is a primitive 32nd root of unity in an extension over $\mathbb{F}_q$ i.e. it is a root of $f(x)=x^2-\eta_1 x-1$and$\beta^{15}$is another root of $f(x)$. Therefore $\beta+\beta^{15}=\eta_1$and $\beta^{16}=-1$. Hence$\alpha^{-k}\beta\ and\ \alpha^{-k}\beta^{15}$are two roots of $f_k(x)$, then

$$
\begin{cases}
(\alpha^{-k}\beta)^j=\ a_0^{(j,k)}+a_1^{(j,k)}\alpha^{-k}\beta\\
(\alpha^{-k}\beta^{15})^j=\ a_0^{(i,j)}+a_1^{(i,j)}\alpha^{-k}\beta^{15}
\end{cases}
\text{and}
\begin{cases}
a_0^{(j,k)}=\ \alpha^{-jk}.\frac{\beta^{j-1}-\beta^{15(j-1)}}{\beta-\beta^{15}}\\
a_1^{(j,k)}=\ \alpha^{-(j-1)k}.\frac{\beta^{j}-\beta^{15j}}{\beta-\beta^{15}}.
\end{cases}
\qquad \ldots\ldots\ldots (1)
$$

Therefore, from (1) for$j=16u,16u+1,16u+2,16u+3,\ldots,16u+15$,the values $a_0^{(j,k)}$and $a_1^{(j,k)}$are as follows:

If $j=16u$, then $a_0^{(j,k)}=\ \alpha^{-8uk}.\frac{\beta^{8u-1}-\beta^{15(8u-1)}}{\beta-\beta^{15}}=(-1)^u.\alpha^{-16uk}.$

$$a_1^{(j,k)}=\ \alpha^{-(16u-1)k}.\frac{\beta^{16u}-\beta^{15(16u)}}{\beta-\beta^{15}}=\alpha^{-(16u-1)k}.\frac{(-1)^u-(-1)^u}{\beta-\beta^{15}}=0$$

If $j=16u+1$, then

$$a_0^{(j,k)}=\ \alpha^{-(16u+1)k}.\frac{\beta^{16u}-\beta^{15(16u)}}{\beta-\beta^{15}}=0$$

$$a_1^{(j,k)}=\ \alpha^{-16uk}.\frac{\beta^{16u+1}-\beta^{15(16u+1)}}{\beta-\beta^{15}}=(-1)^u.\alpha^{-16uk}$$

If $j=16u+2$, then

$$a_0^{(j,k)}=\ \alpha^{-(16u+2)k}.\frac{\beta^{16u+1}-\beta^{15(16u+1)}}{\beta-\beta^{15}}=(-1)^u.\alpha^{-(16u+2)k}.$$

$$a_1^{(j,k)} = \alpha^{-(16u+1)k}.\frac{\beta^{16u+2}-\beta^{15(16u+2)}}{\beta-\beta^{15}} = (-1)^u\eta_1\alpha^{-(16u+1)k}$$

If $j = 16u+3$, then

$$a_0^{(j,k)} = \alpha^{-(16u+3)k}.\frac{\beta^{16u+2}-\beta^{15(16u+2)}}{\beta-\beta^{15}} = (-1)^u.\eta_1\alpha^{-(16u+3)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+2)k}.\frac{\beta^{16u+3}-\beta^{15(16u+3)}}{\beta-\beta^{15}} = (-1)^u(\sqrt{2+\sqrt{2}}-1)\alpha^{-(16u+2)k}$$

If $j = 16u+4$, then

$$a_0^{(j,k)} = \alpha^{-(16u+4)k}.\frac{\beta^{16u+3}-\beta^{15(16u+3)}}{\beta-\beta^{15}} = (-1)^u(\sqrt{2+\sqrt{2}}-1)\,\alpha^{-(16u+4)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+3)k}.\frac{\beta^{16u+4}-\beta^{15(16u+4)}}{\beta-\beta^{15}} = (-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(8u+3)k}$$

If $j = 16u+5$, then

$$a_0^{(j,k)} = \alpha^{-(16u+5)k}.\frac{\beta^{16u+4}-\beta^{15(16u+4)}}{\beta-\beta^{15}} = (-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(8u+5)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+4)k}.\frac{\beta^{16u+5}-\beta^{15(16u+5)}}{\beta-\beta^{15}} = (-1)^u(\sqrt{2}+1-\sqrt{2+\sqrt{2}})\alpha^{-(8u+4)k}$$

If $j = 16u+6$, then

$$a_0^{(j,k)} = \alpha^{-(16u+6)k}.\frac{\beta^{16u+5}-\beta^{15(16u+5)}}{\beta-\beta^{1}} = (-1)^u(\sqrt{2}+1-\sqrt{2+\sqrt{2}})\alpha^{-(16u+6)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+5)k}.\frac{\beta^{16u+6}-\beta^{1(16u+6)}}{\beta-\beta^{15}} = (-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+5)k}$$

If $j = 16u+7$, then

$$a_0^{(j,k)} = \alpha^{-(16u+7)k}.\frac{\beta^{16u+6}-\beta^{15(16u+6)}}{\beta-\beta^{15}} = (-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+7)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+6)k}.\frac{\beta^{16u+7}-\beta^{15(16u+7)}}{\beta-\beta^{15}} = (-1)^u\left\{\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right\}\alpha^{-(16u+6)k}$$

If $j = 16u+8$, then

$$a_0^{(j,k)} = \alpha^{-(16u+8)k}.\frac{\beta^{16u+7}-\beta^{15(16u+7)}}{\beta-\beta^{15}} = (-1)^u\left\{\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right\}\alpha^{-(16u+8)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+7)k}.\frac{\beta^{16u+8}-\beta^{15(16u+8)}}{\beta-\beta^{15}} = (-1)^u\sqrt{2}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+7)k}$$

If $j = 16u+9$, then

$$a_0^{(j,k)} = \alpha^{-(16u+9)k}.\frac{\beta^{16u+8}-\beta^{15(16u+8)}}{\beta-\beta^{15}} = (-1)^u\sqrt{2}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+9)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+8)k}.\frac{\beta^{16u+9}-\beta^{15(16u+9)}}{\beta-\beta^{15}}(-1)^{u+1}\left\{\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right\}\alpha^{-(16u+8)k}$$

If $j = 16u+10$, then

$$a_0^{(j,k)} = \alpha^{-(16u+10)k}.\frac{\beta^{16u+9}-\beta^{15(16u+9)}}{\beta-\beta^{15}} = (-1)^{u+1}\left\{\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right\}\alpha^{-(16u+10)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+9)k}.\frac{\beta^{16u+10}-\beta^{15(16u+10)}}{\beta-\beta^{15}} = (-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+9)k}$$

If $j = 16u+11$, then

$$a_0^{(j,k)} = \alpha^{-(16u+11)k}.\frac{\beta^{16u+10}-\beta^{15(16u+10)}}{\beta-\beta^{15}} = (-1)^u\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+11)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+10)k}.\frac{\beta^{16u+11} - \beta^{15(16u+11)}}{\beta - \beta^{15}} = (-1)^u\left(\sqrt{2+\sqrt{2}} - \sqrt{2} - 1\right)\alpha^{-(16u+10)k}$$

If $j = 16u + 12$, then

$$a_0^{(j,k)} = \alpha^{-(16u+12)k}.\frac{\beta^{16u+11} - \beta^{15(16u+11)}}{\beta - \beta^{15}} = (-1)^u\left(\sqrt{2+\sqrt{2}} - \sqrt{2} - 1\right)\alpha^{-(16u+12)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+11)k}.\frac{\beta^{16u+12} - \beta^{15(16u+12)}}{\beta - \beta^{15}} = (-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+11)k}$$

If $j = 16u + 13$, then

$$a_0^{(j,k)} = \alpha^{-(16u+13)k}.\frac{\beta^{16u+12} - \beta^{15(16u+12)}}{\beta - \beta^{15}} = (-1)^u\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+13)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+12)k}.\frac{\beta^{16u+13} - \beta^{15(16u+13)}}{\beta - \beta^{15}} = (-1)^{u+1}\left(\sqrt{2+\sqrt{2}} - 1\right)\alpha^{-(16u+12)k}$$

If $j = 16u + 14$, then

$$a_0^{(j,k)} = \alpha^{-(16u+14)k}.\frac{\beta^{16u+13} - \beta^{15(16u+13)}}{\beta - \beta^{15}} = (-1)^{u+1}\left(\sqrt{2+\sqrt{2}} - 1\right)\alpha^{-(16u+14)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+13)k}.\frac{\beta^{16u+14} - \beta^{15(16u+14)}}{\beta - \beta^{15}} = (-1)^u\eta_1\alpha^{-(16u+13)k}$$

If $j = 16u + 15$, then

$$a_0^{(j,k)} = \alpha^{-(16u+15)k}.\frac{\beta^{16u+14} - \beta^{15(16u+14)}}{\beta - \beta^{15}} = (-1)^u\eta_1\alpha^{-(16u+15)k}$$

$$a_1^{(j,k)} = \alpha^{-(16u+14)k}.\frac{\beta^{16u+15} - \beta^{15(16u+15)}}{\beta - \beta^{15}} = (-1)^{u+1}\alpha^{-(16u+14)k}$$

Hence the lemma.

Similarly, we can also prove the following lemmas.

Lemma 3.2. We have supposed thatβ is a 32^{nd}primitive root of unity, then β^{31} and β^{17} are two roots of $g(x) = x^2 + \eta_1 x - 1$.Therefore $\beta^{31} + \beta^{17} = -\eta_1$ and $\beta^{48} = \beta^{16} - 1$. Let $g_k(x) = x^2 + \eta_1\alpha^{-k}x - \alpha^{-2k}$, $k = 0,1, \dots, p^n - 1$and $x^j \equiv b_0^{(j,k)} + b_1^{(j,k)}x(mod\ g_k(x)), j = 0, 1, \dots, 32p^n - 1$. So$\alpha^{-k}\beta^{31}\ and\ \alpha^{-k}\beta^{17}$are two roots of $g_k(x)$. Then $b_0^{(j,k)} + b_1^{(j,k)}x$ is as follows:

$$
\begin{cases}
(-1)^{u}\alpha^{-16uk}, & if\ j=16u,\\
(-1)^{u}\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^{u}\alpha^{-(16u+2)k}+(-1)^{u+1}\eta_1\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^{u+1}\eta_1\alpha^{-(16u+3)k}+(-1)^{u}\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^{u}\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+4)k}+(-1)^{u+1}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^{u+1}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+5)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+6)k}+(-1)^{u+1}\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^{u+1}\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+7)k}+(-1)^{u}\left[\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+6)k}x, & if\ j=16u+7.\\
(-1)^{u}\left[\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+8)k}+(-1)^{u+1}\sqrt{2}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+7)k}x, & if\ j=16u+8\\
(-1)^{u+1}\sqrt{2}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+9)k}+(-1)^{u+1}\left[\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^{u+1}\left[\sqrt{2}\left(\sqrt{2+\sqrt{2}}-1\right)-1\right]\alpha^{-(16u+10)k}+(-1)^{u+1}\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+9)k}x, & if\ j=16u+10\\
(-1)^{u+1}\left(\sqrt{2}+1\right)\eta_1\alpha^{-(16u+11)k}+(-1)^{u}\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+10)k}x, & if\ j=16u+11\\
(-1)^{u}\left(\sqrt{2+\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+12)k}+(-1)^{u+1}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^{u+1}\sqrt{2+\sqrt{2}}\eta_1\alpha^{-(16u+13)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}-1\right)\alpha^{-(16u+14)k}+(-1)^{u+1}\eta_1\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^{u+1}\eta_1\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}
$$

Lemma: 3.3. Let $h_k(x)=x^2-\eta_2\alpha^{-k}x-\alpha^{-2k},\ k=0,1,\dots,p^n-1$.Suppose that $x^j\equiv c_0^{(j,k)}+c_1^{(j,k)}x\ (mod\ h_k(x)),\ j=0,1,\dots,32p^n-1$. As$\beta$ is a 32nd primitive root of unity in an extension over $\mathbb{F}_q$. Thereforeβ^7 and β^9 are two roots of$h(x)=x^2-\eta_2x-1$ such that $\beta^7+\beta^9=\eta_2$and $\beta^7\beta^9=-1$. Hence $\alpha^{-k}\beta^7\ and\ \alpha^{-k}\beta^9$are two roots of $h_k(x)$.Then$c_0^{(j,k)}+c_1^{(j,k)}x$ is as follows:

$$
\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^u\eta_2\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^u\eta_2\alpha^{-(16u+3)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+4)k}+(-1)^{u+1}\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^{u+1}\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+5)k}+(-1)^u\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^u\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+6)k}+(-1)^u\left(\sqrt{2}+1\right)\eta_2\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^u\left(\sqrt{2}+1\right)\eta_2\alpha^{-(16u+7)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+6)k}x, & if\ j=16u+7.\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+8)k}+(-1)^{u+1}\sqrt{2}\sqrt{2+\sqrt{2}}\,\eta_2\alpha^{-(16u+7)k}x\ if\ j=16u+8\\
(-1)^{u+1}\sqrt{2}\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+9)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+8)k}x, if\ j=16u+9\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+10)k}+(-1)^u\left(\sqrt{2}+1\right)\eta_2\alpha^{-(16u+9)k}x, if\ j=16u+10\\
(-1)^u\left(\sqrt{2}+1\right)\eta_2\alpha^{-(16u+11)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+10)k}x, if\ j=16u+11\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+12)k}+(-1)^u\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+11)k}x, if\ j=16u+12\\
(-1)^u\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+13)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+14)k}+(-1)^u\eta_2\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^u\eta_2\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}
$$

Lemma 3.4. Let $p_k(x)=x^2+\eta_2\alpha^{-k}x-\alpha^{-2k}, k=0,1,\dots,p^n-1$. Suppose that $x^j\equiv d_0^{(j,k)}+d_1^{(j,k)}x\ (mod\ p_k(x)),\ j=0,1,\dots,32p^n-1$. We have supposed that$\beta$ is a 32[nd]primitive root of unity, soβ^{25} and β^{23} are roots of $p(x)=x^2+q_2x-1$. Therefore, $\beta^{25}+\beta^{23}=-\eta_2$ and $\beta^{25}\beta^{23}=-1$.Hence $\alpha^{-k}\beta^{25}$ and $\alpha^{-k}\beta^{23}$ are two rootsof $p_k(x)$.Then $d_0^{(j,k)}+d_1^{(j,k)}x$ is as follows:

$$\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^{u+1}\eta_2\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^{u+1}\eta_2\alpha^{-(16u+3)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+4)k}+(-1)^u\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^u\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+5)k}+(-1)^u\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^u\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+6)k}+(-1)^{u+1}(\sqrt{2}+1)\eta_2\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^{u+1}(\sqrt{2}+1)\eta_2\alpha^{-(16u+7)k}+(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+6)k}x, & if\ j=16u+7.\\
(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+8)k}+(-1)^u\sqrt{2}\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+7)k} & if\ j=16u+8\\
(-1)^u\sqrt{2}\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+9)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2+\sqrt{2}}+1\right)+1\right]\alpha^{-(16u+10)k}+(-1)^{u+1}(\sqrt{2}+1)\eta_2\alpha^{-(16u+9)k}x, & if\ j=16u+10\\
(-1)^{u+1}(\sqrt{2}+1)\eta_2\alpha^{-(16u+11)k}+(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+10)k}x & if\ j=16u+11\\
(-1)^{u+1}\left(\sqrt{2+\sqrt{2}}+\sqrt{2}+1\right)\alpha^{-(16u+12)k}+(-1)^u\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^u\sqrt{2+\sqrt{2}}\eta_2\alpha^{-(16u+13)k}+(-1)^u\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^u\left(\sqrt{2+\sqrt{2}}+1\right)\alpha^{-(16u+14)k}+(-1)^{u+1}\eta_2\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^{u+1}\eta_2\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}$$

Lemma 3.5. Let $q_k(x)=x^2-\rho_1\alpha^{-k}x-\alpha^{-2k}, k=0,1,\dots,p^n-1$. Suppose that $x^j\equiv e_0^{(j,k)}+e_1^{(j,k)}x\ (modq(x)),\ j=0,1,\dots,32p^n-1$. We have assumed that β is a 32[nd]primitive root of unity over $\mathbb{F}_q$. Then β^3 and β^{13} are roots of $q(x)=x^2-\rho_1x-1$ such that $\beta^3+\beta^{13}=\rho_1$ and $\beta^3\beta^{13}=-1$.Hence $\alpha^{-k}\beta^3$ and $\alpha^{-k}\beta^{13}$ are two roots of $q_k(x)$.Then$e_0^{(j,k)}+e_1^{(j,k)}x$ is as follows:

$$
\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^u\rho_1\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^u\rho_1\alpha^{-(16u+3)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^u\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+4)k}+(-1)^u\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^u\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+5)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+6)k}+(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+7)k}+(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}-1\right)+1\right]\alpha^{-(16u+6)k} & if\ j=16u+7.\\
(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}-1\right)+1\right]\alpha^{-(16u+8)k}+(-1)^{u+1}\sqrt{2}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+7)k}x, & if\ j=16u+8\\
(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+9)k}+(-1)^u\sqrt{2}\left\{\left(\sqrt{2-\sqrt{2}}-1\right)+1\right\}\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^u\sqrt{2}\left\{\left(\sqrt{2-\sqrt{2}}-1\right)+1\right\}\alpha^{-(16u+10)k}+(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+9)k}x, & if\ j=16u+10\\
(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+11)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+10)k}x, & if\ j=16u+11\\
(-1)^u\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+12)k}+(-1)^u\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^u\sqrt{2-\sqrt{2}}r_1\alpha^{-(16u+13)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+14)k}+(-1)^u\rho_1\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^u\rho_1\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}
$$

Lemma 3.6. Let $r_k(x)=x^2+\rho_1\alpha^{-k}x-\alpha^{-2k}, k=0,1,\dots,p^n-1$. Suppose that $x^j\equiv m_0^{(j,k)}+m_1^{(j,k)}x\ (modq(x)),\ j=0,1,\dots,32p^n-1$. β is a 32[th] primitive root of unity. Soβ^{29} and β^{19} are roots of $r(x)=x^2+\rho_1x-1$ such that$\beta^{29}+\beta^{19}=-\rho_1$ and $\beta^{29}\beta^{19}=\beta^{16}=-1$.Hence $\alpha^{-k}\beta^{29}$ and $\alpha^{-k}\beta^{19}$ are two roots of $r_k(x)$.Then$m_0^{(j,k)}+m_1^{(j,k)}x$ is as follows:

$$\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^{u+1}\rho_1\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^{u+1}\rho_1\alpha^{-(16u+3)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^u\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+4)k}+(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+5)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+6)k}+(-1)^u\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^u\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+7)k}+(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}-1\right)+1\right]\alpha^{-(16u+6)k} & if\ j=16u+7.\\
(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}-1\right)+1\right]\alpha^{-(16u+8)k}+(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+7)k}x & if\ j=16u+8\\
(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+9)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}-1\right)+1\right]\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}-1\right)+1\right]\alpha^{-(16u+10)k}+(-1)^u\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+9)k}x, & if\ j=16u+10\\
(-1)^u\left(\sqrt{2}-1\right)\rho_1\alpha^{-(16u+11)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+10)k}x, & if\ j=16u+11\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+\sqrt{2}-1\right)\alpha^{-(16u+12)k}+(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_1\alpha^{-(16u+13)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-1\right)\alpha^{-(16u+14)k}+(-1)^{u+1}\rho_1\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^{u+1}\rho_1\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}$$

Lemma:3.7 We have assumed that β is a 32nd primitive root of unity. Soβ^5 and β^{11} are rootsof $s(x)=x^2-\rho_2x-1$and $\beta^5+\beta^{11}=\rho_2$.Let $s_k(x)=x^2-\rho_2\alpha^{-k}x-\alpha^{-2k}, k=0,1,\dots,p^n-1andx^j\equiv n_0^{(j,k)}+n_1^{(j,k)}x\ (mod\ s(x)),\ j=0,1,\dots,32p^n-1$.Hence $\alpha^{-k}\beta^5$ and $\alpha^{-k}\beta^{11}$ are two roots of $s_k(x)$.Then$n_0^{(j,k)}+n_1^{(j,k)}x$ is as follows:

$$
\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^u\rho_2\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^u\rho_2\alpha^{-(16u+3)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+4)k}+(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+5)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^u\left(\sqrt{2-\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+6)k}+(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+7)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+6)k} & if\ j=16u+7.\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+8)k}+(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+7)k}x & if\ j=16u+8\\
(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+9)k}+(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+10)k}+(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+9)k}x, & i\,j=16u+10\\
(-1)^{u+1}\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+11)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-\sqrt{2}+1\right)\alpha^{-(16u+10)k}x, & if\ j=16u+11\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-\sqrt{2}+1\right)\alpha^{-(16u+12)k}+(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^{u+1}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+13)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^u\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+14)k}+(-1)^u\rho_2\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^u\rho_2\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}
$$

Lemma 3.8. β is a 32[th] primitive root of unity over $\mathbb{F}_q$. Soβ^{27} and β^{21} are roots of $t(x)=x^2+\rho_2x-1$. Therefore, $\beta^{27}+\beta^{21}=-\rho_2$ and $\beta^{27}\beta^{21}=\beta^{16}=-1$.Let $t_k(x)=x^2+\rho_2\alpha^{-k}x-\alpha^{-2k},k=0,1,\dots,p^n-1$.Suppose that $x^j\equiv t_0^{(j,k)}+t_1^{(j,k)}x\ (mod\ t(x)),\ j=0,1,\dots,32p^n-1$ .Hence $\alpha^{-k}\beta^{27}$ and $\alpha^{-k}\beta^{21}$ are two roots of $t_k(x)$.Then$t_0^{(j,k)}+t_1^{(j,k)}x$ is as follows:

$$\begin{cases}
(-1)^u\alpha^{-16uk}, & if\ j=16u,\\
(-1)^u\alpha^{-16uk}x, & if\ j=16u+1,\\
(-1)^u\alpha^{-(16u+2)k}+(-1)^{u+1}\rho_2\,\alpha^{-(16u+1)k}x, & if\ j=16u+2,\\
(-1)^{u+1}\rho_2\alpha^{-(16u+3)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+2)k}x, & if\ j=16u+3,\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+4)k}+(-1)^u\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+3)k}x, & if\ j=16u+4,\\
(-1)^u\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+5)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+4)k}x, & if\ j=16u+5,\\
(-1)^u\left(\sqrt{2-\sqrt{2}}-\sqrt{2}-1\right)\alpha^{-(16u+6)k}+(-1)^u\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+5)k}x, & if\ j=16u+6,\\
(-1)^u\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+7)k}+(-1)^u\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+6)k} & if\ j=16u+7.\\
(-1)^u\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+8)k}+(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+7)k}x & if\ j=16u+8\\
(-1)^u\sqrt{2}\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+9)k}+(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+8)k}x, & if\ j=16u+9\\
(-1)^{u+1}\sqrt{2}\left[\left(\sqrt{2-\sqrt{2}}+1\right)-1\right]\alpha^{-(16u+10)k}+(-1)^u\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+9)k}x, & if\ j=16u+10\\
(-1)^u\left(\sqrt{2}-1\right)\rho_2\alpha^{-(16u+11)k}+(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-\sqrt{2}+1\right)\alpha^{-(16u+10)k}x, & if\ j=16u+11\\
(-1)^{u+1}\left(\sqrt{2-\sqrt{2}}-\sqrt{2}+1\right)\alpha^{-(16u+12)k}+(-1)^u\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+11)k}x, & if\ j=16u+12\\
(-1)^u\sqrt{2-\sqrt{2}}\rho_2\alpha^{-(16u+13)k}+(-1)^u\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+12)k}x, & if\ j=16u+13\\
(-1)^u\left(\sqrt{2-\sqrt{2}}+1\right)\alpha^{-(16u+14)k}+(-1)^{u+1}\rho_2\alpha^{-(16u+13)k}x, & if\ j=16u+14\\
(-1)^{u+1}\rho_2\alpha^{-(16u+15)k}+(-1)^{u+1}\alpha^{-(16u+14)k}x, & if\ j=16u+15
\end{cases}$$

4 Decomposition of $\mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle$ into product of sub rings

Theorem4.1: Let $\mathbb{F}_q$ be a finite field of q elements, where $q=8k+3$ for some k and $p^l \parallel q-1$ for integer $l>0$ and $4\nmid q-1$. Then decomposition of $\mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle$ into direct product of its sub rings over $\mathbb{F}_q$ is as follows:

$$\mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle \longrightarrow \prod_{k=0}^{p^n-1}\left(\mathcal{R}_k^{(1)}\times\mathcal{R}_k^{(2)}\times\mathcal{R}_k^{(3)}\times\ldots\times\mathcal{R}_k^{(17)}\right)$$

$$\sum_{j=0}^{32p^n-1}a_jx^j \longrightarrow \left(\prod_{k=0}^{p^n-1}r_k^{(1)},\prod_{k=0}^{p^n-1}r_k^{(2)},\prod_{k=0}^{p^n-1}r_k^{(3)},\ldots,\prod_{k=0}^{p^n-1}r_k^{(17)}\right)$$

Proof. The irreducible factorization of $x^{32p^n}-1$ over $\mathbb{F}_q$is as follows:

$$x^{32p^n}-1=\prod_{k=0}^{p^n-1}(x\pm\alpha^{-k})(x^2+\alpha^{-2k})\left(x^2\pm\sqrt{-2}\alpha^{-k}x-\alpha^{-2k}\right)(x^2\pm\lambda_1\alpha^{-k}x-\alpha^{-2k})(x^2\pm\lambda_2\alpha^{-k}x-\alpha^{-2k})\,(x^2\pm\eta_1\alpha^{-k}x-\alpha^{-2k})(x^2\pm\eta_2\alpha^{-k}x-\alpha^{-2k})(x^2\pm\rho_1\alpha^{-k}x-\alpha^{-2k})(x^2\pm\rho_2\alpha^{-k}x-\alpha^{-2k})$$

where α^{-1} is p^n-th primitive root of unity over $\mathbb{F}_q$.

Now by Chinese Remainder Theoremwe define a natural $\mathbb{F}_q$- algebra isomorphismψas:

$$\psi:\ \mathbb{F}_q[x]/\langle x^{32p^n}-1\rangle \longrightarrow \prod_{k=0}^{p^n-1}\left(\mathcal{R}_k^{(1)}\times\mathcal{R}_k^{(2)}\times\mathcal{R}_k^{(3)}\times\ldots\times\mathcal{R}_k^{17)}\right)$$

$$\sum_{j=0}^{32p^n-1} a_j x^j \longrightarrow \left(\prod_{k=0}^{p^n-1} r_k^{(1)}, \prod_{k=0}^{p^n-1} r_k^{(2)}, \prod_{k=0}^{p^n-1} r_k^{(3)}, \dots, \prod_{k=0}^{p^n-1} r_k^{(17)}\right)$$

Where

$$\mathcal{R}_k^{(1)} = \mathbb{F}_q[x]/\langle x-\alpha^{-k}\rangle, \mathcal{R}_k^{(2)} = \mathbb{F}_q[x]/\langle x+\alpha^{-k}\rangle, \mathcal{R}_k^{(3)} = \mathbb{F}_q[x]/\langle x^2+\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(4)} = \mathbb{F}_q[x]/\langle x^2-\sqrt{-2}\,\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(5)} = \mathbb{F}_q[x]/\langle x^2+\sqrt{-2}\,\alpha^{-k}x-\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(6)} = \mathbb{F}_q[x]/\langle x^2-\lambda_1\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(7)} = \mathbb{F}_q[x]/\langle x^2+\lambda_1\alpha^{-k}x-\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(8)} = \mathbb{F}_q[x]/\langle x^2-\lambda_2\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(9)} = \mathbb{F}_q[x]/\langle x^2+\lambda_2\alpha^{-k}x-\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(10)} = \mathbb{F}_q[x]/\langle x^2-\eta_1\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(11)} = \mathbb{F}_q[x]/\langle x^2+\eta_1\alpha^{-k}x-\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(12)} = \mathbb{F}_q[x]/\langle x^2-\eta_2\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(13)} = \mathbb{F}_q[x]/\langle x^2+\eta_2\alpha^{-k}x-\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(14)} = \mathbb{F}_q[x]/\langle x^2-\rho_1\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(15)} = \mathbb{F}_q[x]/\langle x^2+\rho_1\alpha^{-k}x-\alpha^{-2k}\rangle$$

$$\mathcal{R}_k^{(16)} = \mathbb{F}_q[x]/\langle x^2-\rho_2\alpha^{-k}x-\alpha^{-2k}\rangle, \mathcal{R}_k^{(17)} = \mathbb{F}_q[x]/\langle x^2+\rho_2\alpha^{-k}x-\alpha^{-2k}\rangle$$

And $r_k^{(1)} = \sum_{j=0}^{16p^n-1} u_j\,(\alpha^{-k})^j$, $r_k^{(2)} = \sum_{j=0}^{16p^n-1} u_j\,(-\alpha^{-k})^j$, $r_k^{(3)} = \sum_{j=0}^{8p^n-1} u_{2j}\,(-\alpha^{-2k})^j + \sum_{j=0}^{8p^n-1} u_{2j+1}\,(-\alpha^{-2k})^j x$, $r_k^{(4)} = \sum_{j=0}^{16p^n-1} u_j\left(e_0^{(j,k)} + e_1^{(j,k)}x\right)$, $r_k^{(5)} = \sum_{j=0}^{16p^n-1} u_j\left(m_0^{(j,k)} + m_1^{(j,k)}x\right)$, $r_k^{(8)} = \sum_{j=0}^{16p^n-1} u_j\left(c_0^{(j,k)} + c_1^{(j,k)}x\right)$, … , $r_k^{(17)} = \sum_{j=0}^{32p^n-1} u_j\left(\tau_0^{(j,k)} + \tau_1^{(j,k)}x\right)$,

Where $a_i^{(j,k)}, b_i^{(j,k)}, c_i^{(j,k)}$ *and* $\tau_i^{(j,k)}$ for $i = 0,1$ are defined in Lemmas 3.1, 3.2, 3.3, 3.4. 3.5,3.6, 3.7 and 3.8.

The case when $n \geq l$, then $n = vl + s,\ 0 \leq s < l$.

Lemma 4.2 If $v = 1$ then $n = l + s$ and we have the factorization of $x^{32p^n} - 1$ over $\mathbb{F}_q$ is as follows

$$x^{32p^{l+s}} - 1 = \prod_{k=0}^{p^l-1}\left(x^{p^s} \pm \alpha^{-k}\right)\left(x^{2p^s} + \alpha^{-2k}\right)\left(x^{2p^s} \pm \sqrt{-2}\,\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)\left(x^{2p^s} \pm \lambda_1\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)\left(x^{2p^s} \pm \lambda_2\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)\left(x^{2p^s} \pm \eta_1\,\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)\left(x^{2p^s} \pm \eta_2\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)\left(x^{2p^s} \pm \rho_1\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)\left(x^{2p^s} \pm \rho_2\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$$

Where α^{-1} is a p^l-th primitive root of unity over $\mathbb{F}_q$. Also , consider $k = p^t.c$ and $\gcd(p,c) = 1$ then using Lemma 2.1 :

i. For $t = 0$ we have $k = c$. So the polynomials $\left(x^{p^s} \pm \alpha^{-k}\right)$,$\left(x^{p^s} + \alpha^{-k}\right)$, $\left(x^{2p^s} \pm \sqrt{-2}\,\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$,$\left(x^{2p^s} \pm \lambda_1\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$,$\left(x^{2p^s} \pm \lambda_2\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$,$\left(x^{2p^s} \pm \eta_1\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$, $\left(x^{2p^s} \pm \eta_2\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$, $\left(x^{2p^s} \pm \rho_1\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$ *and* $\left(x^{2p^s} \pm \rho_2\alpha^{-k}x^{p^s} - \alpha^{-2k}\right)$are irreducible over $\mathbb{F}_q$.
ii. For $0 \leq t < s$, the irreducible factorization over $\mathbb{F}_q$ is given as follows:

$$x^{p^s} \pm \alpha^{-k} = \left(x^{p^{s-t}}\right)^{p^t} \pm (\alpha^{-c})^{p^t} = \prod_{i=0}^{p^t-1}\left(x^{p^{s-t}} \pm \xi_{p^t}^{-i}\alpha^{-c}\right)$$

$$x^{2p^s} + \alpha^{-2k} = \left(x^{2p^{s-t}}\right)^{p^t} - (\alpha^{-2c})^{p^t} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} + \xi_{p^t}^{-i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \sqrt{-2}\,\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \sqrt{-2}\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \lambda_1\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \lambda_1\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \lambda_2\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \lambda_2\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \eta_1\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \eta_1\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \eta_2\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \eta_2\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \rho_1\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \rho_1\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

$$x^{2p^s} \pm \rho_2\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^t-1}\left(x^{2p^{s-t}} \pm \rho_2\xi_{p^t}^{-i}\alpha^{-c}x^{p^{s-t}} - \xi_{p^t}^{-2i}\alpha^{-2c}\right)$$

iii. For $t \geq s$, the irreducible factorization over $\mathbb{F}_q$ is given as follows:

$$x^{p^s} \pm \alpha^{-k} = x^{p^s} \pm \left(\alpha^{-cp^{t-s}}\right)^{p^s} = \prod_{i=0}^{p^s-1}\left(x \pm \xi_{p^s}^{-i}\alpha^{-cp^{t-s}}\right)$$

$$x^{2p^s} + \alpha^{-2k} = x^{2p^s} + \left(\alpha^{-2cp^{t-s}}\right)^{p^s} = \prod_{i=0}^{p^s-1}\left(x^2 + \xi_{p^s}^{-i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \sqrt{-2}\,\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \sqrt{-2}\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \lambda_1\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \lambda_1\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \lambda_2\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \lambda_2\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \eta_1\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \eta_1\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \eta_2\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \eta_2\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \rho_1\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \rho_1\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

$$x^{2p^s} \pm \rho_2\alpha^{-k}x^{p^s} - \alpha^{-2k} = \prod_{i=0}^{p^s-1}\left(x^2 \pm \rho_2\xi_{p^s}^{-i}\alpha^{-cp^{t-s}}x - \xi_{p^s}^{-2i}\alpha^{-2cp^{t-s}}\right)$$

Theorem 4.3 If $n \geq l$, then $n = vl + s$. Let $v = 1$ and $k = p^t.c$ with $\gcd(p, c) = 1$. Then decomposition of $\mathbb{F}_q[x]/\langle x^{32p^{l+s}} - 1\rangle$ is given below.:

$$\psi\colon \mathbb{F}_q[x]\Big/\langle (x^{\mu})^{32p^l} - 1\rangle \longrightarrow \prod_{k=0}^{p^l-1}\left(\mathcal{R}_k^{(1)} \times \mathcal{R}_k^{(2)} \times \ldots \times \mathcal{R}_k^{(17)}\right)$$

Defined as

$$\sum_{j=0}^{32p^l-1} a_j x^{\mu.j} \longrightarrow \left(\prod_{k=0}^{p^l-1} r_k^{(1)}, \prod_{k=0}^{p^l-1} r_k^{(2)}, \ldots \prod_{k=0}^{p^l-1} r_k^{(17)}\right)$$

Proof. If $n \geq l$, then $n = vl + s$ and for $v = 1$, taking α^{-1} primitive p^l-th root of unity, the factorization of $x^{32p^{l+s}} - 1$ over $\mathbb{F}_q$, computed in Lemma 4.2, is given as

$$x^{32p^{l+s}}-1=\prod_{k=0}^{p^l-1}\left(x^{p^s}\pm\alpha^{-k}\right)\left(x^{2p^s}+\alpha^{-2k}\right)\left(x^{2p^s}-\pm\sqrt{-2}\,\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\lambda_1\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\lambda_2\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\eta_1\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\eta_2\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\rho_1\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\rho_2\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)$$

Now consider $k=c\,p^t$, with $gcd\,(c,p)=1$, then as in Lemma 4.2 we have three cases:

Case 1. For $t=0\ we\ have\ \ k=c$. So all the factor polynomials $\sigma(x)=x^{p^s}\pm\alpha^{-k}$, $x^{2p^s}+\alpha^{-2k}$, $x^{2p^s}\pm\sqrt{-2}\,\alpha^{-k}x^{p^s}-\alpha^{-2k}$, $x^{2p^s}\pm\lambda_1\alpha^{-k}x^{p^s}-\alpha^{-2k}$, $x^{2p^s}\pm\lambda_2\alpha^{-k}x^{p^s}-\alpha^{-2k}\left(x^{2p^s}\pm\eta_1\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\eta_2\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\rho_1\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)\left(x^{2p^s}\pm\rho_2\alpha^{-k}x^{p^s}-\alpha^{-2k}\right)$of $x^{32p^{l+s}}-1$ are irreducible over $\mathbb{F}_q$.

Now, let $p^s=\mu$, then by Chinese Remainder Theorem , there is a natural $\mathbb{F}_q$ −algebra isomorphism

$$\psi:\ \mathbb{F}_q[x]\Big/\langle(x^{\mu})^{32p^l}-1\rangle\longrightarrow\prod_{k=0}^{p^l-1}\left(\mathcal{R}_k^{(1)}\times\mathcal{R}_k^{(2)}\times\ldots\times\mathcal{R}_k^{(17)}\right)$$

Defined as

$$\sum_{j=0}^{32p^l-1}a_jx^{\mu.j}\longrightarrow\left(\prod_{k=0}^{p^l-1}r_k^{(1)},\prod_{k=0}^{p^l-1}r_k^{(2)},\ldots\prod_{k=0}^{p^l-1}r_k^{(17)}\right)$$

Where $\mathcal{R}_k^{(1)}=\ \mathbb{F}_q[x]/\langle x^{\mu}-\alpha^{-k}\rangle$, $\mathcal{R}_k^{(2)}=\ \mathbb{F}_q[x]/\langle x^{\mu}+\alpha^{-k}\rangle$, $\mathcal{R}_k^{(3)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\alpha^{-2k}\rangle$

$\mathcal{R}_k^{(4)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\sqrt{-2}\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(5)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\sqrt{-2}\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

$\mathcal{R}_k^{(6)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\lambda_1\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(7)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\lambda_1\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

$\mathcal{R}_k^{(8)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\lambda_2\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(9)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\lambda_2\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

$\mathcal{R}_k^{(10)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\eta_1\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(11)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\eta_1\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

$\mathcal{R}_k^{(12)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\eta_2\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(13)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\eta_2\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

$\mathcal{R}_k^{(14)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\rho_1\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(15)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\rho_1\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

$\mathcal{R}_k^{(16)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}-\rho_2\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$, $\mathcal{R}_k^{(17)}=\ \mathbb{F}_q[x]/\langle x^{2\mu}+\rho_2\,\alpha^{-k}x^{\mu}-\ \alpha^{-2k}\rangle$

And $r_k^{(1)}=\sum_{j=0}^{32p^l-1}u_j(\,\alpha^{-k})^j$, $r_k^{(2)}=\sum_{j=0}^{32p^l-1}u_j(-\,\alpha^{-k})^j$,$r_k^{(3)}=\sum_{j=0}^{16p^l-1}u_{2j}(-\alpha^{-2k})^j+\sum_{j=0}^{16p^l-1}u_{2j+1}(-\alpha^{-2k})^j\,x$, $r_k^{(4)}=\sum_{j=0}^{32p^l-1}u_j\left(e_0^{(j,k)}+e_1^{(j,k)}x\right),\ldots,r_k^{(17)}=\sum_{j=0}^{32p^l-1}u_j\left(d_0^{(j,k)}+d_1^{(j,k)}x\right)$, Where $e_i^{(j,k)}$, $m_i^{(j,k)}$ are defined as in Lemma 5.1 and 5.2 of [6] .$a_i^{(j,k)}$, $b_i^{(j,k)}$, $c_i^{(j,k)}$ and $d_i^{(j,k)}$ for $i=0,1$ are defined as in Lemma 3.1, 3.2, 3.3,…, 3.8 . u_0,u_1, … , u_{32p^l-1} are polynomials of degree $\leq\mu-1$ in $\mathbb{F}_q[x]$. Similarly, we can have the cases 2 and 3.

References

[1] S. K. Arora, S. Batra , S. D. Cohen and M. Pruthi, The primitive idempotents of cyclic group algebra, Southeast Asian Bull.Math.26 (2002) 197-208.

[2] S. K. Arora, S. Batra, S. D. Cohen, The primitive idempotents of a cyclic group algebra II, Southeast Asian Bull. Math. 29 (2005) 549-557.

[3] S. Batra, S. K. Arora, Minimal quadratic residue cyclic codes of length 2^n, J. Appl. Math.Comput. 18 (2005) 25-43 (old KGCAM).

[4] S. Batra, S. K. Arora, Some cyclic codes of length $2p^n$, Des. Codes Cryptography 61 (2011) 41-69.

[5] F.Li, Q. Yue, C. Li, The minimum Hamming distances of irreducible cyclic codes, Finite Fields Appl. 29 (2014) 225-242.

[6] F. Li, Q. Yue, C. Li, Irreducible cyclic codes of length $4p^n$ and $8p^n$, Finite Fields Appl. 34 (2015) 208-234.

[7] Yuqian Lin, Qin Yue, Yansheng Win, Primitive idempotents of irreducible cyclic codes of length n, Mathematical Problems in Engineering ,Vol.2018.

[8] M. Pruthi, Cyclic codes of length 2^m, Proc. Indian Acad. Sci. Math. Sci. 111 (2001) 371-379.

[9] Manju Pruthi, Pankaj, The minimum Hamming distances of the irreducible cyclic codes of length $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, Journal of Discrete Mathematical Sciences & cryptography, vol.19,(2006).

[10] R. Singh, M. Pruthi, Primitive Idempotents of irreducible quadratic residue cyclic codes of length $p^n q^m$, Int. J. Algebra 5 (2011) 285-294.