PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 7, July 2009, Pages 2191–2200
S 0002-9939(09)09747-0
Article electronically published on January 13, 2009

ON THE NUMBER OF SOLUTIONS OF THE LINEAR EQUATION IN FINITE CARLITZ MODULES

CHIH-NUNG HSU AND TING-TING NAN

(Communicated by Ken Ono)

Abstract. We deduce an accurate formula for the number of solutions of the linear equation in generators of finite Carlitz modules, and the equation always has solutions except for some cases. Therefore, we have a criterion for the existence of the solutions of the linear equation. Moreover, we have a similar result in normal bases when we apply our main theorem to a special case.

1. Introduction

In the 1950s, Carlitz [1],[2] proved that in a finite field $\mathbb{F}_p$ with p elements where p is a prime number, for any fixed integer n, the linear equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = a \quad (a \in \mathbb{F}_p, a_i \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\})$$

such that $x_1, \cdots, x_n$ are primitive roots in $\mathbb{F}_p$ has solutions for a sufficiently large prime p. The basic technique for estimating the number of solutions, which are all primitive roots in terms of Gauss sums over $\mathbb{F}_p$, yields the estimation that depends on the number of positive divisors of $p-1$. However, if the solutions play another important role in finite Carlitz modules, generators for example, then we may receive not only an estimation but a beautiful formula.

In this paper, let $\mathbb{F}_q$ denote the finite field with q elements where q is a prime power and let $\mathbf{A} = \mathbb{F}_q[T]$ be the polynomial ring with coefficients in $\mathbb{F}_q$. The degree of the polynomial a in $\mathbf{A}$ is denoted by $\deg a$, and the valuation of a is denoted by $|a| = q^{\deg a}$.

Let $\mathbf{k} = \mathbb{F}_q(T)$ be the quotient field of $\mathbf{A}$ and let τ^i be the $q^{i^{\text{th}}}$-power Frobenius mapping, i.e., $\tau^i(x) = x^{q^i}$ for all x in $\mathbf{k}$. Let $\mathbf{A}\{\tau\}$ be the ring of $\mathbb{F}_q$-linear polynomials in one indeterminant x with coefficients in $\mathbf{A}$ under composition, that is, for $p(x)$ in $\mathbf{A}\{\tau\}$, $p(x+y) = p(x) + p(y)$ and $p(cx) = cp(x)$ for all x, y in $\mathbf{k}$, c in $\mathbb{F}_q$. The Carlitz $\mathbf{A}$-module defined over $\mathbf{A}$ is the $\mathbb{F}_q$-algebra homomorphism ψ from $\mathbf{A}$ to $\mathbf{A}\{\tau\}$ defined by

$$\psi(1) = \tau^0, \psi(T) = T\tau^0 + \tau^1.$$

Received by the editors June 12, 2008, and, in revised form, September 1, 2008.
2000 *Mathematics Subject Classification.* Primary 11G09; Secondary 11T55, 11T24.

The structure of the Carlitz $\mathbf{A}$-module $\mathbf{A}$ is given by

$$\begin{array}{ccc} \mathbf{A}\times\mathbf{A} & \to & \mathbf{A} \\ (a\ ,\ b) & \mapsto & b^a \end{array}$$

where b^a is defined by $\psi(a)(b)$.

Throughout this paper, we fix a monic prime f in $\mathbf{A}$ of degree d. Then $E_1 = \mathbf{A}/(f)$ is a finite field with q^d elements. Let E_m be the finite extension of E_1 of degree m. We have a canonical projection ι from $\mathbf{A}$ to $E_1 = \mathbf{A}/(f)$, i.e., $\iota(a) = \overline{a}$ for all $a \in A$. Applying ι to the coefficients of $\psi(a)$ for all a in $\mathbf{A}$, we obtain elements in $E_1\{\tau\}$ where $L\{\tau\}$ is the ring of $\mathbb{F}_q$-linear polynomials in one indeterminant x with coefficients in L under composition for any field L containing $\mathbb{F}_q$. Thus, a finite Carlitz $\mathbf{A}$-module is the $\mathbb{F}_q$-algebra homomorphism $\Psi : \mathbf{A} \overset{\psi}{\to} \mathbf{A}\{\tau\} \to E_1\{\tau\}$ defined by

$$\Psi(1) = \tau^0, \quad \Psi(T) = \overline{T}\tau^0 + \tau^1,$$

and the structure of the finite Carlitz $\mathbf{A}$-module E_m, denoted by $\mathcal{C}(E_m)$, is

$$\begin{array}{ccc} \mathbf{A}\times E_m & \to & E_m \\ (a\ ,\ \alpha) & \mapsto & \alpha^a \end{array}$$

where α^a is defined by $\alpha^a = \Psi(a)(\alpha)$ for all a in $\mathbf{A}$, α in $\mathcal{C}(E_m)$.

It is known that the finite Carlitz $\mathbf{A}$-module $\mathcal{C}(E_m)$ is isomorphic to $\mathbf{A}/(f^m-1)$ as an $\mathbf{A}$-module; i.e., $\mathcal{C}(E_m)$ is a cyclic $\mathbf{A}$-module. More details can be found in D. Goss [3].

For any α in $\mathcal{C}(E_m)$, we define the order of α, denoted by $\operatorname{ord}(\alpha)$, to be the monic polynomial g in $\mathbf{A}$ of the least degree such that $\alpha^g = 0$. Since $\mathcal{C}(E_m)$ is isomorphic to $\mathbf{A}/(f^m-1)$, $\operatorname{ord}(\alpha)$ divides f^m-1. Particularly, any generator of $\mathcal{C}(E_m)$ is of order f^m-1.

The main theorem of this paper is

Theorem 3.1. Let n be a fixed integer, α be an element in $\mathcal{C}(E_m)$ of order H, $G = \frac{f^m-1}{H}$, $d = \deg f$, and N be the number of solutions in E_m^n of the linear equation

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = \alpha$$

with $c_i \in \mathbb{F}_q^*$ such that $x_1, \cdots, x_n$ are generators of the finite Carlitz $\mathbf{A}$-module $\mathcal{C}(E_m)$. Then N is

$$q^{(n-1)md}\left(\prod_{P|H, P\nmid G}\left[\left(1-\frac{1}{|P|}\right)^n - \frac{(-1)^n}{|P|^n}\right]\right)\left(\prod_{P|G}\left[\left(1-\frac{1}{|P|}\right)^n + \frac{(-1)^n\phi(P)}{|P|^n}\right]\right),$$

where P runs over all monic primes in $\mathbf{A}$ and ϕ is the Euler ϕ-function for polynomials.

Further, we can deduce that N is always positive if q is greater than 2.

A normal basis of E_m over E_1 is a basis of the form $\{\beta, \beta^{q^d}, \cdots, \beta^{q^{(m-1)d}}\}$, and the element β is called a normal element of E_m over E_1. For any α in E_m, we also establish some similar results for the number of solutions in E_m^n of the linear equation

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = \alpha$$

with $c_i \in \mathbb{F}_q^*$ such that $x_1, \cdots, x_n$ are normal elements of E_m over E_1.

Unless otherwise stated, $D, g, h, f_i, g_i, g_i', h_i$ will denote the monic polynomials in $\mathbf{A}$ and P will denote the monic prime in $\mathbf{A}$.

2. Auxiliary lemmas

In this section, we present some lemmas that will be used in section 3.

Lemma 2.1. *Let α be an element in $\mathcal{C}(E_m)$ and c in $\mathbb{F}_q^*$. Then α and $c\alpha$ have the same order in $\mathcal{C}(E_m)$. Moreover, α and $c\alpha$ are generators of $\mathcal{C}(E_m)$ simultaneously if one of them is.*

Proof. Since c is in $\mathbb{F}_q^*$, we have $c^q = c$ and $(c\alpha)^a = c\alpha^a$ for any a in $\mathbf{A}$. Thus, α and $c\alpha$ have the same order in $\mathcal{C}(E_m)$. □

Lemma 2.2. *Let N be the number of solutions in E_m^n of the linear equation*

$$c_1x_1 + \cdots + c_nx_n = \alpha \tag{2.1}$$

with $c_i \in \mathbb{F}_q^*$ such that $x_1, \cdots, x_n$ are generators of $\mathcal{C}(E_m)$.

Let N' be the number of solutions in E_m^n of the linear equation

$$x_1 + \cdots + x_n = \alpha \tag{2.2}$$

such that $x_1, \cdots, x_n$ are generators of $\mathcal{C}(E_m)$. Then we have $N = N'$.

Proof. If $(\alpha_1, \cdots, \alpha_n)$ is a solution of the equation (2.1), then by Lemma 2.1, $(c_1\alpha_1, \cdots, c_n\alpha_n)$ is a solution of the equation (2.2). Hence, $N \leq N'$.

Conversely, we can get $N \geq N'$, and this concludes the proof. □

Let $\widehat{E_m}$ be the group of additive characters of E_m and let λ_0 be the trivial character in $\widehat{E_m}$. For any a in $\mathbf{A}$ and λ in $\widehat{E_m}$, λ^a is an additive character of E_m defined by $\lambda^a(\alpha) = \lambda(\alpha^a)$ for all α in $\mathcal{C}(E_m)$. Then $\widehat{E_m}$ has the $\mathbf{A}$-module structure defined by

$$\begin{array}{ccc} \mathbf{A} \times \widehat{E_m} & \rightarrow & \widehat{E_m} \\ (a\ ,\ \lambda) & \mapsto & \lambda^a. \end{array}$$

We define the order of λ in $\widehat{E_m}$, denoted by $\mathrm{Ord}(\lambda)$, to be the monic polynomial g in $\mathbf{A}$ of the least degree such that $\lambda^g = \lambda_0$. Since $\lambda^{f^m-1}(\alpha) = \lambda(\alpha^{f^m-1}) = \lambda(0) = 1$ for all λ in $\widehat{E_m}$, α in E_m, $\lambda^{f^m-1} = \lambda_0$, and hence $\mathrm{Ord}(\lambda)$ divides f^m-1.

For any monic polynomial g in $\mathbf{A}$ dividing f^m-1, let

$$\widehat{E_m}[g] = \{\lambda \in \widehat{E_m} : \lambda^g = \lambda_0\}$$

and let

$$E_m\left[\frac{f^m-1}{g}\right] = \{\alpha \in \mathcal{C}(E_m) : \alpha^{\frac{f^m-1}{g}} = 0\}.$$

We know that $\widehat{E_m}[g]$ is an $\mathbf{A}$-submodule of $\widehat{E_m}$ and $E_m[\frac{f^m-1}{g}]$ is an $\mathbf{A}$-submodule of $\mathcal{C}(E_m)$. Moreover, viewed as an $\mathbf{A}$-module, $\widehat{E_m}[g]$ is isomorphic to $E_m/\widehat{E_m[\frac{f^m-1}{g}]}$ and $E_m[\frac{f^m-1}{g}]$ is isomorphic to $\mathbf{A}/(\frac{f^m-1}{g})$. Therefore, $\#(\widehat{E_m}[g]) = |g|$, where $\#(S)$ denotes the cardinality of a set S (cf. D. Goss [3]). Combining the above discussion with the formula $\sum_{h|g} \phi(h) = |g|$, we have

$$\#\{\lambda \in \widehat{E_m} : \mathrm{Ord}(\lambda) = g\} = \phi(g),$$

where ϕ is the Euler ϕ-function for polynomials. Hence, $\widehat{E_m}$ is a cyclic $\mathbf{A}$-module and is isomorphic to $\mathbf{A}/(f^m-1)$.

Letting μ be the Möbius μ-function for polynomials, we define the characteristic function $\Omega : E_m \to \mathbb{C}$ by

$$\Omega(\alpha) = \sum_{g \mid f^m - 1} \frac{\mu(g)}{|g|} \sum_{\lambda \in \widehat{E_m}, \lambda^g = \lambda_0} \lambda(\alpha). \tag{2.3}$$

Lemma 2.3. *For any α in the finite Carlitz $\mathbf{A}$-module $\mathcal{C}(E_m)$, we have*

$$\Omega(\alpha) = \begin{cases} 1 & \textit{if } \alpha \textit{ is a generator of } \mathcal{C}(E_m), \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let H be the order of α in $\mathcal{C}(E_m)$. Since $\{\lambda \in \widehat{E_m} : \lambda^g = \lambda_0\}$ is isomorphic to $E_m/\widehat{E_m[\frac{f^m-1}{g}]}$, we have

$$\sum_{\lambda \in \widehat{E_m}, \lambda^g = \lambda_0} \lambda(\alpha) = \begin{cases} |g| & \text{if } \alpha \in E_m[\frac{f^m-1}{g}], \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$\sum_{\lambda \in \widehat{E_m}, \lambda^g = \lambda_0} \lambda(\alpha) = \begin{cases} |g| & \text{if } H \mid \frac{f^m-1}{g}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

Applying (2.3) and (2.4), we have

$$\begin{aligned} \Omega(\alpha) &= \sum_{g \mid f^m - 1} \frac{\mu(g)}{|g|} \sum_{\lambda \in \widehat{E_m}, \lambda^g = \lambda_0} \lambda(\alpha) \\ &= \sum_{g \mid f^m - 1, H \mid \frac{f^m-1}{g}} \frac{\mu(g)}{|g|} |g| \\ &= \sum_{g \mid \frac{f^m-1}{H}} \mu(g) \\ &= \begin{cases} 1 & \text{if } H = f^m - 1, \\ 0 & \text{if } H \neq f^m - 1, \end{cases} \\ &= \begin{cases} 1 & \text{if } \alpha \text{ is a generator of } \mathcal{C}(E_m), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

□

Lemma 2.4. *Let n be a positive integer and let M be a monic polynomial in $\mathbf{A}$. Then we have*

$$\sum_{\substack{h_1, \cdots, h_n \mid M \\ (h_1, \cdots, h_n) = 1}} \prod_{i=1}^{n} \frac{\mu(h_i)}{|h_i|} = \prod_{P \mid M} \left[\left(1 - \frac{1}{|P|}\right)^n - \frac{(-1)^n}{|P|^n} \right],$$

where $(h_1, \cdots, h_n)$ denotes the greatest common divisor of $h_1, \cdots, h_n$ in $\mathbf{A}$.

Proof. Let $F_1(M) = \sum_{\substack{h_1,\cdots,h_n|M \\ (h_1,\cdots,h_n)=1}} \prod_{i=1}^{n} \frac{\mu(h_i)}{|h_i|}$. For any monic prime P in $\mathbf{A}$ and positive integer k, we have

$$\begin{aligned} F_1(P^k) &= \sum_{\substack{h_1,\cdots,h_n|P^k \\ (h_1,\cdots,h_n)=1}} \prod_{i=1}^{n} \frac{\mu(h_i)}{|h_i|} \\ &= 1 + \binom{n}{1}\frac{(-1)}{|P|} + \binom{n}{2}\frac{(-1)^2}{|P|^2} + \cdots + \binom{n}{n-1}\frac{(-1)^{n-1}}{|P|^{n-1}} \\ &= \left(1 - \frac{1}{|P|}\right)^n - \frac{(-1)^n}{|P|^n}. \end{aligned}$$

Since F_1 is a multiplicative function of $\mathbf{A}$ into $\mathbb{R}$, we obtain

$$\sum_{\substack{h_1,\cdots,h_n|M \\ (h_1,\cdots,h_n)=1}} \prod_{i=1}^{n} \frac{\mu(h_i)}{|h_i|} = \prod_{P|M} \left[\left(1 - \frac{1}{|P|}\right)^n - \frac{(-1)^n}{|P|^n}\right].$$

□

Lemma 2.5. *Let n be a positive integer and G a monic polynomial in $\mathbf{A}$. We have*

$$\sum_{D|G} \frac{\mu(D)^n}{|D|^{n-1}} \sum_{\substack{f_1,\cdots,f_n|\frac{G}{D} \\ (f_i,D)=1,(f_1\cdots,f_n)=1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|} = \prod_{P|G} \left[\left(1 - \frac{1}{|P|}\right)^n + \frac{(-1)^n \phi(P)}{|P|^n}\right].$$

Proof. Let $F_2(G) = \sum_{D|G} \frac{\mu(D)^n}{|D|^{n-1}} \sum_{\substack{f_1,\cdots,f_n|\frac{G}{D} \\ (f_i,D)=1,(f_1\cdots,f_n)=1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|}$. For any monic prime P in $\mathbf{A}$ and positive integer k, we have

$$\begin{aligned} F_2(P^k) &= \sum_{D|P^k} \frac{\mu(D)^n}{|D|^{n-1}} \sum_{\substack{f_1,\cdots,f_n|\frac{P^k}{D} \\ (f_i,D)=1,(f_1\cdots,f_n)=1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|} \\ &= 1 \times \sum_{\substack{f_1,\cdots,f_n|P^k \\ (f_1\cdots,f_n)=1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|} + \frac{(-1)^n}{|P|^{n-1}} \cdot \sum_{\substack{f_1,\cdots,f_n|P^{k-1} \\ (f_i,P)=1,(f_1\cdots,f_n)=1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|} \\ &= \sum_{\substack{f_1,\cdots,f_n|P^k \\ (f_1\cdots,f_n)=1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|} + \frac{(-1)^n}{|P|^{n-1}}. \end{aligned}$$

Applying Lemma 2.4, we get

$$F_2(P^k) = \left(1 - \frac{1}{|P|}\right)^n + \frac{(-1)^n \phi(P)}{|P|^n}.$$

Since F_2 is a multiplicative function of $\mathbf{A}$ into $\mathbb{R}$, we obtain

$$\sum_{D|G}\frac{\mu(D)^n}{|D|^{n-1}}\sum_{\substack{f_1,\cdots,f_n|\frac{G}{D}\\(f_i,D)=1,(f_1\cdots,f_n)=1}}\prod_{i=1}^{n}\frac{\mu(f_i)}{|f_i|}=\prod_{P|G}\left[\left(1-\frac{1}{|P|}\right)^n+\frac{(-1)^n\phi(P)}{|P|^n}\right].$$

□

3. The main theorem

Let f be a monic irreducible polynomial in $\mathbf{A}$ of degree d. Then $E_1=\mathbf{A}/(f)$ is a finite field with q^d elements. Let E_m be the finite extension of E_1 of degree m. The finite Carlitz $\mathbf{A}$-module $\mathcal{C}(E_m)$ is a cyclic $\mathbf{A}$-module and $\mathcal{C}(E_m)$ is isomorphic to $\mathbf{A}/(f^m-1)$. Our main theorem in this paper is

Theorem 3.1. *Let n be a fixed integer, α be an element in $\mathcal{C}(E_m)$ of order H, $G=\frac{f^m-1}{H}$, $d=\deg f$, and N be the number of solutions in E_m^n of the linear equation*

$$c_1x_1+c_2x_2+\cdots+c_nx_n=\alpha$$

with $c_i\in\mathbb{F}_q^*$ such that $x_1,\cdots,x_n$ are generators of the finite Carlitz $\mathbf{A}$-module $\mathcal{C}(E_m)$. Then N is

$$q^{(n-1)md}\left(\prod_{P|H,P\nmid G}\left[\left(1-\frac{1}{|P|}\right)^n-\frac{(-1)^n}{|P|^n}\right]\right)\left(\prod_{P|G}\left[\left(1-\frac{1}{|P|}\right)^n+\frac{(-1)^n\phi(P)}{|P|^n}\right]\right).$$

Proof. According to Lemma 2.2, without loss of generality we may assume that $c_1=\cdots=c_n=1$. By Lemma 2.3 and the definition of Ω in (2.3), the number N is

$$\begin{aligned}
&\sum_{\substack{(\alpha_1,\cdots,\alpha_n)\in E_m^n\\ \alpha_1+\cdots+\alpha_n=\alpha}}\Omega(\alpha_1)\cdots\Omega(\alpha_n)\\
=&\sum_{\alpha_1,\cdots,\alpha_{n-1}\in E_m}\Omega(\alpha_1)\cdots\Omega(\alpha_{n-1})\Omega(\alpha-\alpha_1-\cdots-\alpha_{n-1})\\
=&\sum_{\alpha_1,\cdots,\alpha_{n-1}\in E_m}\sum_{g_1,\cdots,g_n|f^m-1}\left(\prod_{i=1}^{n}\frac{\mu(g_i)}{|g_i|}\right)\sum_{\substack{\lambda_i\in\widehat{E_m}\\ \lambda_i^{g_i}=\lambda_0}}\lambda_1(\alpha_1)\cdots\lambda_{n-1}(\alpha_{n-1})\lambda_n(\alpha-\alpha_1-\cdots-\alpha_{n-1})\\
=&\sum_{g_1,\cdots,g_n|f^m-1}\left(\prod_{i=1}^{n}\frac{\mu(g_i)}{|g_i|}\right)\sum_{\substack{\lambda_i\in\widehat{E_m}\\ \lambda_i^{g_i}=\lambda_0}}\lambda_n(\alpha)\left(\sum_{\alpha_1\in E_m}\lambda_1\lambda_n^{-1}(\alpha_1)\right)\cdots\left(\sum_{\alpha_{n-1}\in E_m}\lambda_{n-1}\lambda_n^{-1}(\alpha_{n-1})\right).
\end{aligned}$$

For any λ in $\widehat{E_m}$, since $\#(E_m)=q^{md}$, the character sum

$$\sum_{\alpha\in E_m}\lambda(\alpha)=\begin{cases}q^{md} & \text{if }\lambda=\lambda_0,\\ 0 & \text{otherwise.}\end{cases}$$

Combining these, we obtain

$$\begin{aligned} N &= \sum_{g_1,\cdots,g_n | f^m - 1} \left(\prod_{i=1}^{n} \frac{\mu(g_i)}{|g_i|} \right) \sum_{\substack{\lambda_n \in \widehat{E_m} \\ \lambda_n^{g_1} = \cdots = \lambda_n^{g_n} = \lambda_0}} \lambda_n(\alpha) \left(q^{md}\right)^{n-1} \\ &= q^{(n-1)md} \sum_{g_1,\cdots,g_n | f^m - 1} \left(\prod_{i=1}^{n} \frac{\mu(g_i)}{|g_i|} \right) \sum_{\substack{\lambda \in \widehat{E_m} \\ \lambda^{(g_1,\cdots,g_n)} = \lambda_0}} \lambda(\alpha). \end{aligned}$$

By (2.4), we get

$$\begin{aligned} N &= q^{(n-1)md} \sum_{\substack{g_1,\cdots,g_n | f^m - 1 \\ H | \frac{f^m - 1}{(g_1,\cdots,g_n)}}} \left(\prod_{i=1}^{n} \frac{\mu(g_i)}{|g_i|} \right) |(g_1, \cdots, g_n)| \\ &= q^{(n-1)md} \sum_{\substack{g_1,\cdots,g_n | f^m - 1 \\ (g_1,\cdots,g_n) | G}} \left(\prod_{i=1}^{n} \frac{\mu(g_i)}{|g_i|} \right) |(g_1, \cdots, g_n)|. \end{aligned}$$

Putting $D = (g_1, \cdots, g_n)$ and $g_i' = \frac{g_i}{D}$ for all i, we have

$$\begin{aligned} N &= q^{(n-1)md} \sum_{\substack{D | G, g_1',\cdots,g_n' | \frac{f^m - 1}{D} \\ (g_1',\cdots,g_n') = 1}} \left(\prod_{i=1}^{n} \frac{\mu(g_i' D)}{|g_i' D|} \right) |D| \\ &= q^{(n-1)md} \sum_{D|G} \frac{\mu(D)^n}{|D|^{n-1}} \sum_{\substack{g_1',\cdots,g_n' | \frac{f^m - 1}{D} \\ (g_i', D) = 1, (g_1',\cdots,g_n') = 1}} \prod_{i=1}^{n} \frac{\mu(g_i')}{|g_i'|}. \end{aligned}$$

Define $H^* = \prod_{P | H, P \nmid G} P$. By the definition of μ and H^*, we obtain

$$\begin{aligned} N &= q^{(n-1)md} \sum_{D|G} \frac{\mu(D)^n}{|D|^{n-1}} \sum_{\substack{h_1,\cdots,h_n | H^* \\ (h_1,\cdots,h_n) = 1}} \sum_{\substack{f_1,\cdots,f_n | \frac{G}{D} \\ (f_i, D) = 1, (f_1,\cdots,f_n) = 1}} \prod_{i=1}^{n} \frac{\mu(h_i)\mu(f_i)}{|h_i||f_i|} \\ &= q^{(n-1)md} \left(\sum_{\substack{h_1,\cdots,h_n | H^* \\ (h_1,\cdots,h_n) = 1}} \prod_{i=1}^{n} \frac{\mu(h_i)}{|h_i|} \right) \left(\sum_{D|G} \frac{\mu(D)^n}{|D|^{n-1}} \sum_{\substack{f_1,\cdots,f_n | \frac{G}{D} \\ (f_i, D) = 1, (f_1,\cdots,f_n) = 1}} \prod_{i=1}^{n} \frac{\mu(f_i)}{|f_i|} \right). \end{aligned}$$

Applying Lemma 2.4 and Lemma 2.5, we get

$$N = q^{(n-1)md} \left(\prod_{P | H, P \nmid G} \left[\left(1 - \frac{1}{|P|}\right)^n - \frac{(-1)^n}{|P|^n} \right] \right) \left(\prod_{P|G} \left[\left(1 - \frac{1}{|P|}\right)^n + \frac{(-1)^n \phi(P)}{|P|^n} \right] \right).$$

This completes the proof. □

Here, we illustrate two examples.

Example 3.2. We know that $f = T^3 + T + 1$ is an irreducible function of degree 3 in $\mathbf{A} = \mathbb{F}_2[T]$ and $\overline{T^2}$, $\overline{T^2 + T + 1}$ are the two generators of the cyclic $\mathbf{A}$-module $\mathcal{C}(E_1)$.

By a simple computation, there is no solution in E_1^2 of the linear equation $x_1 + x_2 = \overline{T}$ such that x_1, x_2 are generators of $\mathcal{C}(E_1)$. In fact, the order of $\overline{T}$ in $\mathcal{C}(E_1)$ is T, and N is indeed zero according to our formula for N in Theorem 3.1 with $m = 1$, $n = 2$, $\alpha = \overline{T}$, $H = T$, and $G = T^2 + 1$.

If we consider another equation $x_1 + x_2 + x_3 = \overline{T^2 + 1}$ such that x_1, x_2, x_3 are generators of $\mathcal{C}(E_1)$, then N is zero again. Actually, the order of $\overline{T^2 + 1}$ in $\mathcal{C}(E_1)$ is $T^2 + 1$, and $N = 0$ also satisfies our formula in Theorem 3.1 with $m = 1$, $n = 3$, $\alpha = \overline{T^2 + 1}$, $H = T^2 + 1$, and $G = T$.

Example 3.3. We know that $f = T^2 + 1$ is an irreducible function of degree 2 in $\mathbf{A} = \mathbb{F}_3[T]$ and $\overline{1}$, $\overline{2}$, $\overline{T}$, $\overline{T + 2}$, $\overline{2T}$, $\overline{2T + 1}$ are the six generators of the cyclic $\mathbf{A}$-module $\mathcal{C}(E_1)$.

By simple computation, $(\overline{T + 2}, \overline{2})$, $(\overline{2T}, \overline{T})$, and $(\overline{1}, \overline{2T + 1})$ are the three solutions in E_1^2 of the linear equation $x_1 + 2x_2 = \overline{T}$ such that x_1, x_2 are generators of $\mathcal{C}(E_1)$. In fact, the order of $\overline{T}$ in $\mathcal{C}(E_1)$ is T^2, and $N = 3$ by Theorem 3.1 with $m = 1$, $n = 2$, $\alpha = \overline{T}$, $H = T^2$, and $G = 1$.

Corollary 3.4. *Suppose the hypotheses of Theorem* 3.1 *are satisfied. Then* $N = 0$ *if and only if* $q = 2$ *and there exists a monic prime* P *of degree* 1 *in* $\mathbf{A}$ *satisfying one of the following conditions:*

(1) *When n is even, P divides H but P does not divide G.*
(2) *When n is odd, P divides G.*

Proof. When n is even, by Theorem 3.1, we obtain that $N = 0$ if and only if there is a monic prime P such that $P \mid H$, $P \nmid G$, and $1 - \frac{1}{|P|} = \frac{1}{|P|}$, that is, $|P| = 2$. This leads to the conclusion that $q = 2$ and $\deg P = 1$.

When n is odd, by Theorem 3.1 again, we obtain that $N = 0$ if and only if there is a monic prime P such that $P \mid G$ and $\left(1 - \frac{1}{|P|}\right)^n = \frac{\phi(P)}{|P|^n}$, that is, $|P| = 2$. This implies that $q = 2$ and $\deg P = 1$. □

According to Corollary 3.4, we have

Corollary 3.5. *Suppose the hypotheses of Theorem* 3.1 *are satisfied. If* $q > 2$*, then* N *is always positive.*

4. Application to normal bases

Now, taking $f = T$, we have $E_1 = \mathbf{A}/(T)$ is $\mathbb{F}_q$; E_m is $\mathbb{F}_{q^m}$, the finite field with q^m elements; and the $\mathbb{F}_q$-algebra homomorphism $\Psi : \mathbf{A} \xrightarrow{\psi} \mathbf{A}\{\tau\} \rightarrow \mathbb{F}_q\{\tau\}$ is given by

$$\Psi(1) = \tau^0, \Psi(T) = \tau^1, \Psi(T^2) = \tau^2, \cdots .$$

In this case, the structure of a finite Carlitz $\mathbf{A}$-module is $\alpha^{T^i} = \tau^i(\alpha) = \alpha^{q^i}$ for all α in $\mathcal{C}(E_m)$.

A normal basis of E_m over E_1 is a basis of the form

$$\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\} = \{\beta^1, \beta^T, \cdots, \beta^{T^{m-1}}\},$$

and the element β is called a normal element of E_m over E_1.

The following is an important relationship between the normal element β of E_m over E_1 and the order of β in $\mathcal{C}(E_m)$, mentioned in Lenstra and Schoof [4].

Lemma 4.1. *Let β be an element in $\mathcal{C}(E_m)$. Then β is a normal element of E_m over E_1 if and only if the order of β in $\mathcal{C}(E_m)$ is T^m-1.*

Proof. See Lenstra and Schoof [4], (1.9). □

Applying Theorem 3.1 and Lemma 4.1, we obtain

Theorem 4.2. *Let α be an element in $\mathcal{C}(E_m)$ of order H, let $G = \frac{T^m-1}{H}$, and let N be the number of solutions in E_m^n of the linear equation*

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = \alpha$$

with $c_i \in \mathbb{F}_q^*$ such that $x_1, \cdots, x_n$ are normal elements of E_m over E_1. Then N is

$$q^{(n-1)m}\left(\prod_{P|H, P\nmid G}\left[\left(1-\frac{1}{|P|}\right)^n - \frac{(-1)^n}{|P|^n}\right]\right)\left(\prod_{P|G}\left[\left(1-\frac{1}{|P|}\right)^n + \frac{(-1)^n\phi(P)}{|P|^n}\right]\right).$$

Corollary 4.3. *Under the conditions in Theorem 4.2, let m be in the form of $2^sm'$ with nonnegative integer s and odd m'. Let α be an element in $\mathcal{C}(E_m)$ of order H, and let $G = \frac{T^m-1}{H}$. Then we have $N = 0$ if and only if $q = 2$ and H satisfies one of the following conditions:*

(1) *When n is even, $(T-1)^{2^s}$ divides H.*
(2) *When n is odd, $(T-1)^{2^s}$ doesn't divide H.*

Proof. Applying Corollary 3.4, we only consider the case for $q = 2$. Since $T^m-1 = (T^{m'}-1)^{2^s}$ and $T^{m'}-1$ is separable, the only monic prime P of degree 1, dividing T^m-1, is $T-1$ and the multiplicity of 1 in T^m-1 is 2^s.

When n is even, $N = 0$ if and only if $T-1$ divides H, but $T-1$ doesn't divide G. That is, $(T-1)^{2^s}$ divides H.

When n is odd, $N = 0$ if and only if $T-1$ divides G; i.e., $(T-1)^{2^s}$ doesn't divide H. □

According to Corollary 4.3, we have

Corollary 4.4. *Suppose the hypotheses of Theorem 4.2 are satisfied. If $q > 2$, then N is always positive.*

References

1. L. Carlitz, *Sums of Primitive Roots in a Finite Field*, Duke Math. J., **19** (1952), 459–469. MR0050628 (14:357c)
2. L. Carlitz, *Sets of Primitive Roots*, Compositio Math., **13** (1956), 65–70. MR0083002 (18:642e)
3. D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag (1996). MR1423131 (97i:11062)

4. H. W. Lenstra and R. J. Schoof, *Primitive Normal Bases for Finite Fields*, Math. Comp., **48** (1987), 217–231. MR866111 (88c:11076)
5. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press (1997). MR1429394 (97i:11115)

Department of Mathematics, National Taiwan Normal University, 88 Sec. 4, Ting-Chou Road, Taipei, Taiwan, Republic of China
E-mail address: maco@math.ntnu.edu.tw

Department of Mathematics, National Taiwan Normal University, 88 Sec. 4, Ting-Chou Road, Taipei, Taiwan, Republic of China
E-mail address: ayanami-nan@math.ntnu.edu.tw