Davenport–Hasse’s Theorem for Polynomial Gauss Sums over Finite Fields

Zhiyong Zheng∗
School of Mathematics and Systems Science,
Beihang University, Beijing, P.R. China
zhengzhiyong@buaa.edu.cn

Abstract
In this paper, we study the polynomial Gauss sums over finite fields, and present an analogue of Davenport–Hasse’s theorem for the entire polynomial Gauss sums, which is a generalization of the previous result obtained by Hayes.

2010 Mathematics Subject Classification: Primary 11T55, 11T24, 11L05
Key words: Polynomial Gauss sums, Finite fields, Davenport–Hasse’s Theorem

1 Introduction
Let \( \mathbb{F}_q \) be a finite field with \( q = p^l \) elements, where \( p \) is a prime number. Let \( \mathbb{F}_{q^n} \) be a finite extension of \( \mathbb{F}_q \) of degree \( n \), and \( \sigma \) be the Frobenius on \( \mathbb{F}_{q^n} \), given by \( \sigma(a) = a^q \) for any element \( a \) in \( \mathbb{F}_{q^n} \). We have \( \sigma^n = 1 \), and \( \sigma \) generates the Galois group of \( \mathbb{F}_{q^n}/\mathbb{F}_q \). The relative trace \( \text{tr}(a) \) and the norm \( N(a) \) of an element \( a \) in \( \mathbb{F}_{q^n} \) are defined by

\[
\text{tr}(a) = \sum_{i=1}^{n} \sigma^i(a), \quad N(a) = \prod_{i=1}^{n} \sigma^i(a) \quad (1.1)
\]

respectively. Let \( \psi \) be a (complex-valued) character of the additive group of \( \mathbb{F}_q \), and \( \chi \) a character of the multiplicative group \( \mathbb{F}_q^* \) of \( \mathbb{F}_q \). The Gauss sums of \( \mathbb{F}_q \) are defined by

\[
\tau(\chi, \psi) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi(a). \quad (1.2)
\]

∗This work was partially supported by the “973” project 2013CB834205.
If we set for every $a$ in $\mathbb{F}_{q^n}$ that

$$
\psi^{(n)}(a) = \psi(\text{tr}(a)), \quad \chi^{(n)}(a) = \chi(N(a)),
$$

then the function $\psi^{(n)}$ will be a character of additive group, and function $\chi^{(n)}$ a character of the multiplicative group of $\mathbb{F}_{q^n}$. In particular, if $a \in \mathbb{F}_q$, then we have

$$
\psi^{(n)}(a) = \psi^n(a), \quad \chi^{(n)}(a) = \chi^n(a).
$$

These characters $\psi^{(n)}$ and $\chi^{(n)}$ define a generalized Gauss sums $\tau(\chi^{(n)}, \psi^{(n)})$ on $\mathbb{F}_{q^n}$. Davenport and Hasse in [3] proved the following remarkable theorem (also see [7] and [9]) that

**Theorem 1.1 (Davenport–Hasse)** If both of $\chi$ and $\psi$ are not principal, then

$$
-\tau(\chi^{(n)}, \psi^{(n)}) = (-\tau(\chi, \psi))^n.
$$

To generalize this famous theorem to the polynomial Gauss sums, let $\mathbb{F}_q[x]$ and $\mathbb{F}_{q^n}[x]$ be the polynomial rings over $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ respectively. The Frobenius $\sigma$ of $\mathbb{F}_{q^n}$ may be extended to $\mathbb{F}_{q^n}[x]$ in the following way: If $A = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{F}_{q^n}[x]$, then we define

$$
\sigma(A) = \sigma(a_m) x^m + \cdots + \sigma(a_1) x + \sigma(a_0),
$$

which clearly is a $\mathbb{F}_q[x]$-automorphism of $\mathbb{F}_{q^n}[x]$. The relative trace and norm may be extended to $\mathbb{F}_{q^n}[x]$ by

$$
\text{tr}(A) = \sum_{i=1}^n \sigma^i(A), \quad N(A) = \prod_{i=1}^n \sigma^i(A).
$$

Then $\text{tr}(A)$ is an additive and $N(A)$ a multiplicative function from $\mathbb{F}_{q^n}[x]$ to $\mathbb{F}_q[x]$.

Let $H$ be a fixed but arbitrary polynomial in $\mathbb{F}_q[x]$ with degree $m$, $\psi$ be a (complex-valued) character of additive group of the residue class ring $\mathbb{F}_q[x]/\langle H \rangle$. We may understand that $\psi$ is a complex-valued function defined on $\mathbb{F}_q[x]$ such that

$$
\psi(A + B) = \psi(A) \cdot \psi(B), \quad \text{and} \quad \psi(A) = \psi(B), \quad \text{if} \quad A \equiv B \pmod{H}
$$

for any two polynomials $A$ and $B$ in $\mathbb{F}_q[x]$. According to Hayes [8], we call $\psi$ an additive character modulo $H$ on $\mathbb{F}_q[x]$. For example, $\psi_0$ is the principal additive character modulo $H$, where $\psi_0(A) = 1$ for all the polynomials $A$ in $\mathbb{F}_q[x]$.

Let $\chi$ be a (complex-valued) character of the multiplicative group of the reduced residue of $\mathbb{F}_q[x]/\langle H \rangle$, $\chi$ may be also understood as a complex-valued function of $\mathbb{F}_q[x]$, such that $\chi(A) = 0$ if $(A, H) > 1$ and

$$
\chi(AB) = \chi(A) \cdot \chi(B), \quad \text{and} \quad \chi(A) = \chi(B), \quad \text{if} \quad A \equiv B \pmod{H}.
$$
We also call \( \chi \) a multiplicative character modulo \( H \) on \( \mathbb{F}_q \). Especially, \( \chi_0 \) is the principal multiplicative character modulo \( H \), where \( \chi_0(A) = 1 \) for all \( A \in \mathbb{F}_q \) with \( (A, H) = 1 \).

With the above notations, we define a polynomial Gauss sum \( G(\chi, \psi) \) modulo \( H \) on \( \mathbb{F}_q \) as follows

\[
G(\chi, \psi) = \sum_{D \mod H} \chi(D) \psi(D),
\]

where the summation extending over a complete residue system of modulo \( H \) in \( \mathbb{F}_q \).

For a polynomial \( H \) in \( \mathbb{F}_q[x] \) and, therefore, also a polynomial in \( \mathbb{F}_{q^n}[x] \), to define a Gauss sum modulo \( H \) on \( \mathbb{F}_{q^n} \), for any \( A \in \mathbb{F}_{q^n} \), we set \( \psi^{(n)}(A) \) and \( \chi^{(n)}(A) \) by

\[
\psi^{(n)}(A) = \psi(\text{tr}(A)), \quad \chi^{(n)}(A) = \chi(N(A)).
\]

It is easy to verify that \( \psi^{(n)} \) is an additive and \( \chi^{(n)} \) a multiplicative character modulo \( H \) on \( \mathbb{F}_{q^n} \), thus we may use these characters to define a polynomial Gauss sum \( G(\chi^{(n)}, \psi^{(n)}) \) modulo \( H \) on \( \mathbb{F}_{q^n} \).

The most interesting question is that, is there an analogue of Davenport–Hasse’s theorem for the polynomial Gauss sums? Hayes [6, Theorem 2.2] shows that an analogue of Davenport–Hasse’s theorem for a special additive character \( \psi = E \), which character was essentially introduced by Carlitz (see [3]). To state Hayes’ result, for any polynomial \( A \) in \( \mathbb{F}_q \), let

\[
A \equiv a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \pmod{H},
\]

where \( m = \deg(H) \). We set an additive function modulo \( H \) on \( \mathbb{F}_q \) by \( t(A) = a_{m-1} \). By the definition, we have immediately that for any \( A, B \in \mathbb{F}_q \), \( t(A + B) = t(A) + t(B) \), and \( t(A) = t(B) \) whenever \( A \equiv B \pmod{H} \), in particular, \( t(A) = 0 \) if \( H \mid A \). To generalize that \( t \)-function modulo \( H \) on \( \mathbb{F}_q \), for a given polynomial \( G \) in \( \mathbb{F}_q \), let

\[
t_G(A) = t(GA).
\]

Clearly, \( t_G \) is an additive function modulo \( H \) on \( \mathbb{F}_q \), that is

\[
t_G(A+B) = t_G(A) + t_G(B), \quad \text{and} \quad t_G(A) = t_G(B), \quad \text{if} \quad A \equiv B \pmod{H}.
\]

Now, let \( \lambda \) be a fixed non-principal additive character on \( \mathbb{F}_q \), for example, \( \lambda(a) = e(2\pi i \text{tr}(a)/p) \), for \( a \) in \( \mathbb{F}_q \), we define the function \( E_\lambda(G, H) \) on \( \mathbb{F}_q \) by

\[
E_\lambda(G, H)(A) = \lambda(t_G(A)).
\]

It is easily seen that \( E_\lambda(G, H) \) is an additive character modulo \( H \) on \( \mathbb{F}_q \). If we set \( G = 1 \), a constant polynomial, and let \( E = E_\lambda = E_\lambda(1, H) \), then Hayes [6] shows that an analogue of Davenport–Hasse’s theorem for polynomial Gauss sums in the special case of \( \psi = E \).
Theorem 1.2 (Hayes) If $H$ is a polynomial in $\mathbb{F}_q[x]$ with $\deg(H) = m$, then for any multiplicative character $\chi$ of $\mathbb{F}_q[x]$, we have

$$(-1)^m G(\chi^{(n)}, E^{(n)}) = ((-1)^m G(\chi, E))^n. \quad (1.14)$$

The main purpose of this paper is to generalize the above theorem to all of polynomial Gauss sums, we present a completely analogue of Davenport–Hasse’s theorem in polynomial case.

To state our result, first we note that the character $E_\lambda(G, H)$ given by (1.13) are all of additive characters $\psi$ modulo $H$ on $\mathbb{F}_q[x]$. In other words, for any additive character $\psi$ modulo $H$ on $\mathbb{F}_q[x]$, there exists a unique polynomial $G$ in $\mathbb{F}_q[x]$, such that $\deg(G) < \deg(H)$, and $\psi = E_\lambda(G, H)$ (see Lemma 2.1 below). We write $\psi = \psi_G = E_\lambda(G, H)$, and call $G$ the associated polynomial to $\psi$, then we have

Theorem 1.3 If $H$ is a polynomial in $\mathbb{F}_q[x]$ of degree $m$, $\chi$ and $\psi$ are multiplicative and additive characters, not both are principal, then we have

$$(-1)^{m-m_1} \frac{\phi(n)(N)}{\phi(n)(H)} G(\chi^{(n)}, \psi^{(n)}) = \left((-1)^{m-m_1} \frac{\phi(n)}{\phi(H)} G(\chi, \psi)\right)^n, \quad (1.15)$$

where $N = \frac{H}{(G,H)}$, and $G$ is the associated polynomial to $\psi$ ($\psi = \psi_G$), $m_1 = \deg(G, H)$, $\phi(H)$ is the Euler function on $\mathbb{F}_q[x]$, and $\phi^{(n)}(H)$ is the function on $\mathbb{F}_q^n[x]$. In particular, if $H = P^k$, a power of an irreducible $P$, then we have

$$(-1)^{m-m_1} G(\chi^{(n)}, \psi^{(n)}) = ((-1)^{m-m_1} G(\chi, \psi))^n. \quad (1.16)$$

If $G = 1$ is a constant polynomial, then equality (1.15) becomes Hayes’ result (Theorem 1.2). If $(G, H) = 1$, we also have

$$(-1)^m G(\chi^{(n)}, \psi^{(n)}) = ((-1)^m G(\chi, \psi))^n. \quad (1.17)$$

The equality above essentially belongs to Hayes [6].

As we have known, Davenport–Hasse’s theorem plays an important role for the rationality of the Zeta function associated to a hypersurface, we wish the result presented here are helpful for the congruent Zeta function. Finally, we mention a result given by Thakur that an analogue of Davenport–Hasse’s theorem for Gauss sums taking values in function fields of one variable over a finite field holds, see Thakur [10].

Throughout this paper, by positive polynomial means the polynomial of the leading coefficients is unit in $\mathbb{F}_q$, the capital letters $A, B, C, \ldots$ denote polynomials in $\mathbb{F}_q[x]$, or $\mathbb{F}_q^n[x]$, and $a, b, c, \ldots$ denote the elements in $\mathbb{F}_q$ or $\mathbb{F}_q^n$. The absolute value function $|H| = q^m$, where $m = \deg(H)$, and $|H|_n = q^{nm}$ on $\mathbb{F}_q^n[x]$, which are the numbers of a complete residue class module $H$ on $\mathbb{F}_q[x]$ and $\mathbb{F}_q^n[x]$. 

4
2 Properties of character $E_\lambda(G,H)$

In this section, we first determine the construction of the additive character group modulo $H$ on $\mathbb{F}_q[x]$ by using $E_\lambda(G,H)$.

Lemma 2.1 For any $\psi$, an additive character modulo $H$ on $\mathbb{F}_q[x]$, there exists a unique polynomial $G$ in $\mathbb{F}_q[x]$, such that $\deg(G) < \deg(H)$, and $\psi = E_\lambda(G,H)$.

Proof For the convenient sake, we write $\psi_G = E_\lambda(G,H)$. (2.1)

By (1.13), we have $\psi_{G_1} = \psi_{G_2}$, whenever $G_1 \equiv G_2 \pmod{H}$, so we may set $G$ in a complete residue class modulo $H$ in $\mathbb{F}_q[x]$, and then $\deg(G) < \deg(H)$. It is easy to show that by (1.13), for any $G_1, G_2$ in $\mathbb{F}_q[x]$ that

$$\psi_{G_1 + G_2} = \psi_{G_1} \cdot \psi_{G_2}, \quad \text{and } \bar{\psi}_G = \psi_{-G}. \quad (2.2)$$

Since $\psi_G = \psi_0$ the principal character modulo $H$ on $\mathbb{F}_q[x]$, if $G = 0$, or $H \mid G$. Conversely, we have $\psi_G = \psi_0$, if and only if $H \nmid G$. Since $\lambda$ is a non-principal character on $\mathbb{F}_q$ by assumption, then there is an element $a$ in $\mathbb{F}_q$, so that $\lambda(a) \neq 1$. Now if $H \nmid G$, we may let

$$R = (G, H) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x], \quad (2.3)$$

where $0 \leq k \leq m - 1$, and $a_k \neq 0$. It follow that

$$a \cdot a_k^{-1} x^{m-1-k} R = ax^{m-1} + \cdots.$$

We note that the congruent equation in variable $T$ that

$$GT \equiv a \cdot a_k^{-1} x^{m-1-k} R \pmod{H}, \quad (2.4)$$

is solvable in $\mathbb{F}_q[x]$, therefore, there exists a polynomial $A$ in $\mathbb{F}_q[x]$, such that

$$GA \equiv a \cdot a_k^{-1} x^{m-1-k} R \pmod{H}, \quad (2.5)$$

and we see that $t_G(A) = a$ by the definition of (1.11), and $\psi_G(A) = \lambda(t_G(A)) = \lambda(a) \neq 1$, and $\psi_G \neq \psi_0$. By (2.2), we have immediately that

$$\psi_{G_1} \neq \psi_{G_2}, \quad \text{if } G_1 \neq G_2 \pmod{H}. \quad (2.6)$$

Since if $\psi_{G_1} = \psi_{G_2}$, then $\psi_{G_1 - G_2} = \psi_0$, and $G_1 \equiv G_2 \pmod{H}$. This shows that $\psi_G$ are different from each other when $G$ running through a complete residue system of modulo $H$, hence there are exactly $|H| = q^m$ different characters $\psi_G$, but the number of additive characters modulo $H$ on $\mathbb{F}_q[x]$ exactly is $q^m$, thus every additive character $\psi$ is just the form of $\psi_G$. We complete the proof of Lemma 2.1. \qed
The next lemma is not new, one may find in Carlitz [3] (see [3](2.4), (2.5), and (2.6)), but we give a more explicit expression.

**Lemma 2.2** If $A$ is a positive polynomial in $\mathbb{F}_q[x]$, then we have

$$E_\lambda(GA, HA) = E_\lambda(G, H). \quad (2.7)$$

**Proof** For any $B \in \mathbb{F}_q[x]$, let

$$GB \equiv a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \pmod{H}.$$ 

Then

$$AGB \equiv A(a_{m-1}x^{m-1} + \cdots + a_1x + a_0) \pmod{AH}.$$ 

Because of $A$ a positive polynomial, we see that the function $t_{GA}$ modulo $HA$ just is the function $t_G$ modulo $H$. Since that $t_{GA}(B) = a_{m-1} \pmod{HA}$, which is just $t_G(B) \pmod{H}$. It follows that

$$E_\lambda(GH, HA)(B) = \lambda(t_G(B)) = E_\lambda(G, H)(B), \quad (2.8)$$

and we have the lemma at once. □

**Lemma 2.3** For any $A$ in $\mathbb{F}_q[x]$, we have

$$\sum_{G \mod H} \psi_G(A) = \begin{cases} |H|, & \text{if } H \mid A \\ 0, & \text{otherwise} \end{cases},$$

where the summation extending over a complete residue system modulo $H$.

**Proof** By Lemma 2.1 it just is the orthogonal property of characters. We have the lemma immediately. □

### 3 The separable polynomial Gauss sums

The theory for conductors of modulo a polynomial parallels the theory for conductors of Dirichlet characters defined on the integers (see, e.g., [1, pp. 165–172]), but for proving our theorem, we still state and prove a few basic results. First by Lemma 2.1 all of the Gauss sums on $\mathbb{F}_q[x]$ may be written by

$$G(\chi, \psi) = G(\chi, \psi_G) = \sum_{D \mod H} \chi(D)\psi_G(D), \quad (3.1)$$

where $G \in \mathbb{F}_q[x]$ is the polynomial associated to $\psi$. If $(G, H) = 1$, it is easy to verify that

$$G(\chi, \psi_G) = \bar{\chi}(G)G(\chi, \psi_1). \quad (3.2)$$

**Definition 3.1** A Gauss sum $G(\chi, \psi_G)$ is said to be separable if $G(\chi, \psi_G) = \bar{\chi}(G)G(\chi, \psi_1)$.
By (3.2), if \((G,H) = 1\), then \(G(\chi, \psi_G)\) is separable. For the case of \((G,H) > 1\), then \(G(\chi, \psi_G)\) is separable if and only if \(G(\chi, \psi_G) = 0\). The following lemma gives an important consequence of separability.

**Lemma 3.1** If \(G(\chi, \psi_G)\) is separable for every \(G\) in \(F_q[x]\), then

\[ |G(\chi, \psi_1)|^2 = |H| = q^m. \]  \quad (3.3)

**Proof**

\[ |G(\chi, \psi_1)|^2 = G(\chi, \psi_1) \overline{G(\chi, \psi_1)} \]
\[ = G(\chi, \psi_1) \sum_{D \mod H} \bar{\chi}(D)\psi_1(-D) \]
\[ = \sum_{D \mod H} G(\chi, \psi_D)\psi_D(-1) \]
\[ = \sum_{A \mod H} \chi(A) \sum_{D \mod H} \psi_D(A-1). \]  \quad (3.4)

The inner sum in above is zero by Lemma 2.3, if \(A \not\equiv 1 (\mod H)\), so we have Lemma 3.1. \(\square\)

**Lemma 3.2** If \(G(\chi, \psi_G) \neq 0\) for some \(G\) in \(F_q[x]\) with \((G,H) > 1\), then there exists a polynomial \(N\) in \(F_q[x]\), such that \(N|H, \deg(N) < \deg(H)\), and

\[ \chi(A) = 1, \text{ whenever } (A,H) = 1, \text{ and } A \equiv 1 (\mod N). \]  \quad (3.5)

**Proof** For given \(G\), and \(G(\chi, \psi_G) \neq 0\), \((G,H) > 1\). Let \(N = H \cdot (G,H)^{-1}\), thus \(N|H\), and \(\deg(N) < \deg(H)\). If \((A,H) = 1\), then

\[ G(\chi, \psi_G) = \sum_{D \mod H} \chi(AD)\psi_G(AD) \]
\[ = \chi(A) \sum_{D \mod H} \chi(D)\psi_G(AD). \]  \quad (3.6)

If \(A \equiv 1 (\mod N)\), we write

\[ A = 1 + BN, \text{ for some } B \in F_q[x], \]
and then

\[ AG = G + BNG = G + BHG(H,G)^{-1}. \]

So we have \(AG \equiv G(\mod H)\), and \(\psi_G(AD) = \psi_{GA}(D) = \psi_G(D)\). Therefore, equation (3.6) becomes that

\[ G(\chi, \psi_G) = \chi(A) \sum_{D \mod H} \chi(D)\psi_G(D), \]  \quad (3.7)

and we have \(\chi(A) = 1\) because of \(G(\chi, \psi_G) \neq 0\). We complete the proof of Lemma 3.2. \(\square\)
Definition 3.2 A polynomial $N$ in $F_q[x]$ is called an induced modulu of $\chi$ if $N|H$, and for $(A, H) = 1$

\[ \chi(A) = 1, \text{ whenever } A \equiv 1 (\text{mod } N). \]  

(3.8)

By the definition, we see that $H$ itself is an induced modulu of any $\chi$. Moreover, as a direct consequence of Lemma 3.2, we also have

Corollary 3.3 If $(G, H) > 1$, and $G(\chi, \psi_G) \neq 0$, then $N = H(G, H)^{-1}$ is an induced modulu of $\chi$.

Lemma 3.4 Let $N \mid H$, then $N$ is an induced modulu of $\chi$ if and only if for any $A, B$ in $F_q[x]$, and $(AB, H) = 1$, we have

\[ \chi(A) = \chi(B), \text{ whenever } A \equiv B (\text{mod } N). \]  

(3.9)

Proof If (3.9) holds, let $B = 1$, then $N$ is an induced modulu of $\chi$. Conversely, if $N$ is an induced modulu of $\chi$, suppose $(A, H) = (B, H) = 1$, $A \equiv B (\text{mod } N)$, and let $B \cdot B^{-1} \equiv 1 (\text{mod } H)$. Then $BB^{-1} \equiv 1 (\text{mod } N)$, and $AB^{-1} \equiv 1 (\text{mod } N)$. Thus $\chi(AB^{-1}) = 1$, and $\chi(A) = \chi(B)$, the lemma follows.

Lemma 3.5 If $N|H$, and $N$ is an induced modulu of $\chi$, then $\chi$ can be expressed as a product

\[ \chi = \chi_0 \delta, \]  

(3.10)

where $\chi_0$ is the principal multiplicative modulo $H$, and $\delta$ is a multiplicative character modulo $N$.

Proof If $\chi = \chi_0 \delta$, trivially, $N$ is an induced modulu of $\chi$. Conversely, if $N$ is an induced modulu of $\chi$, we may determine a character $\delta$ modulo $N$ by setting $\delta(A) = 0$, if $(A, N) > 1$. If $(A, N) = 1$, one may find a polynomial $B$ in $F_q[x]$, so that

\[ (B, H) = 1, \text{ and } B \equiv A (\text{mod } N). \]  

(3.11)

Since the arithmetic progress \{ $A + RN | R \in F_q[x]$ \} contains infinitely many irreducibles (see Artin [2], or [8, Theorem 4.7]), so we may choose one that does not divide $H$ and call this $B$, which is unique modulo $N$ clearly. Now we define $\delta(A) = \chi(B)$. The number $\delta(A)$ is well-defined because $\chi$ takes equal values at polynomials which are congruent modulo $N$ and relatively prime to $H$. By this determination, we can easily verify that $\delta$ is, indeed, a character modulo $N$, and (3.11) holds. This is the proof of Lemma 3.5.

Definition 3.3 An induced modulu $N$ of $\chi$ is called the conductor of $\chi$, if $N$ is positive, and an induced modulu of $\chi$, and the degree of $N$ is least among all of induced modulus of $\chi$. We denote by $C_\chi$ the conductor of $\chi$. If $C_\chi = H$, then we call $\chi$ a primitive character.
As a consequence of Lemma 3.5, we have

**Corollary 3.6** If $C_\chi$ is the conductor of $\chi$, then $\chi$ can be expressed as a product $\chi = \chi_0 \delta$, where $\delta$ is a primitive character modulo $C_\chi$.

The following lemma is well-known that

**Lemma 3.7** The conductor of $\chi$ divides every induced modulu of $\chi$.

**Proof** See Hayes [6, Theorem 4.2]. □

We have an alternate description of primitive character as the case of Dirichlet characters.

**Lemma 3.8** Let $\chi$ be a character modulo $H$, then $\chi$ is primitive, if and only if the Gauss sums $G(\chi, \psi_G)$ is separable for every polynomial $G$.

**Proof** If $\chi$ is primitive, then $G(\chi, \psi_G)$ is separable by Lemma 3.2, so we only prove the converse. It suffices to prove that if $\chi$ is not primitive, then there exists some $G$ with $(G, H) > 1$, and $G(\chi, \psi_G) \neq 0$. If $\chi$ is not primitive, let $C_\chi$ be the conductor of $\chi$, $N = \frac{H}{C_\chi}$, then $(N, H) > 1$ by $\deg(C_\chi) < \deg(H)$, moreover $G(\chi, \psi_N) \neq 0$. Since $\chi = \chi_0 \delta$, where $\delta$ is primitive character modulo $C_\chi$. By Lemma 2.2, we have

\[
G(\chi, \psi_N) = \sum_{D \mod H} \chi_0(D) \delta(D) \psi_N(D) = \sum_{D \mod H, (D, H) = 1} \delta(D) E_\chi(N, H)(D) = \sum_{D \mod H, (D, H) = 1} \delta(D) E_\chi(1, C_\chi)(D) = \frac{\phi(H)}{\phi(C_\chi)} \sum_{D \mod C_\chi} \delta(D) \psi_1(D) = \frac{\phi(H)}{\phi(C_\chi)} G(\delta, \psi_1),
\]

where $G(\delta, \psi_1)$ is a Gauss sum modulo $C_\chi$. By Lemma 3.1

\[
|G(\delta, \psi_1)|^2 = |C_\chi|. \tag{3.13}
\]

So we have $G(\chi, \psi_N) \neq 0$, and the lemma follows. □
4 Separable Gauss sums on $\mathbb{F}_{q^n}[x]$

For a polynomial $H$ in $\mathbb{F}_q[x]$, and also a polynomial in $\mathbb{F}_{q^n}[x]$. Let $\psi_G^{(n)}$ be an additive character, $\chi^{(n)}$ a multiplicative character modulo $H$ on $\mathbb{F}_q[x]$ given by (1.10). We recall that $\psi_G = E_\lambda(G, H)$ in $\mathbb{F}_q[x]$, it still holds in $\mathbb{F}_{q^n}[x]$, namely

$$\psi_G^{(n)}(n) = E_\lambda^{(n)}(G, H)$$  \hspace{1cm} (4.1)

Since for any polynomial $A$ in $\mathbb{F}_{q^n}[x]$,

$$E_\lambda^{(n)}(G, H)(A) = E_\lambda(G, H)(\text{tr}(A)) = \lambda(t_G(\text{tr}(A))) = \psi_G^{(n)}(A).$$

The last equality is because of $\text{tr}(G \cdot A) = G \text{tr}(A)$ for $G \in \mathbb{F}_q[x]$. So we have if $G \in \mathbb{F}_q[x]$ then

$$\psi_G^{(n)}(A) = \psi_G(n)(GA).$$  \hspace{1cm} (4.2)

Now, Lemma 2.2 becomes that

**Lemma 4.1** If $A \in \mathbb{F}_q[x]$ is a positive polynomial, and $G \in \mathbb{F}_q[x]$, then

$$E_\lambda^{(n)}(GA, HA) = E_\lambda^{(n)}(G, H).$$  \hspace{1cm} (4.3)

**Proof** For any $B \in \mathbb{F}_{q^n}[x]$, let

$$G \text{tr}(B) \equiv a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \pmod{H}.$$

Then

$$AG \text{tr}(B) \equiv A(a_{m-1}x^{m-1} + \cdots + a_1x + a_0) \pmod{AH}.$$

By definition of $E_\lambda(G, H)$ and $E_\lambda^{(n)}(G, H)$, it follows that

$$E_\lambda^{(n)}(GA, HA)(B) = E_\lambda(GA, HA)(\text{tr}(B)) = \lambda(t_{GA}(\text{tr}(B))) = \lambda(a_{m-1}),$$

and

$$E_\lambda^{(n)}(G, H)(B) = E_\lambda(G, H)(\text{tr}(B)) = \lambda(t_G(\text{tr}(B))) = \lambda(a_{m-1}).$$

This lemma follows at once. \hfill $\Box$

**Lemma 4.2** If $N \in \mathbb{F}_q[x]$ is an induced modulu of $\chi$, then $N$ is also an induced modulu of $\chi^{(n)}$ on $\mathbb{F}_{q^n}[x]$.

**Proof** Suppose $A \in \mathbb{F}_{q^n}[x]$, $(A, H) = 1$, and $A = 1 \pmod{N}$, it is easily seen that if $N(A)$ is the norm that

$$N(A) \equiv 1 \pmod{N}.$$  \hspace{1cm} (4.4)

This equality is the Theorem 2.1 of Hayes [8]. Then $\chi^{(n)}(A) = \chi(N(A)) = 1$, and $N$ is an induced modulu of $\chi^{(n)}$ on $\mathbb{F}_q[x]$. \hfill $\Box$
The following lemmas is due to Hayes \cite{hayes} that

**Lemma 4.3** Let $C_\chi$ be the conductor of $\chi$ on $\mathbb{F}_q[x]$, and $C_{\chi(n)}$ be the conductor of $\chi^{(n)}$ on $\mathbb{F}_{q^n}[x]$, then we have $C_\chi = C_{\chi(n)}$.

**Proof** See Hayes \cite[Theorem 4.5]{hayes}. \hfill \square

As a direct corollary of the above lemma and Lemma 3.8, we have

**Corollary 4.4** Let $G(\chi, \psi)$ be the Gauss sums modulo $H$ on $\mathbb{F}_q[x]$, $G(\chi^{(n)}, \psi^{(n)})$ the Gauss sums modulo $H$ on $\mathbb{F}_{q^n}[x]$, then $G(\chi^{(n)}, \psi^{(n)})$ is separable if and only if $G(\chi, \psi)$ is separable.

**Lemma 4.5** Suppose $G$ and $H$ are in $\mathbb{F}_q[x]$, and $(G, H) > 1$, if $G(\chi, \psi_G) \neq 0$, or $G(\chi^{(n)}, \psi^{(n)}_G) \neq 0$, then $N = \frac{H}{(G, H)}$ is an induced modulu of both $\chi$ and $\chi^{(n)}$.

**Proof** It is easily seen that if $N$ is an induced modulu of $\chi$, then any multiple of $N$ which divides $H$, again is an induced modulu of $\chi$. To prove the lemma, first suppose $G(\chi, \psi_G) \neq 0$, because $(G, H) > 1$, then by Lemma 3.2 and Corollary 3.3, $N$ is an induced modulu of $\chi$. By Lemma 4.1, $N$ is also an induced modulu of $\chi^{(n)}$, the lemma holds. If $G(\chi^{(n)}, \psi^{(n)}_G) \neq 0$, then $N$ is an induced modulu of $\chi^{(n)}$. Let $C_{\chi(n)}$ be the conductor of $\chi^{(n)}$, then by Lemma 3.7, we have $C_{\chi(n)}|N$, and then $C_\chi |N$, where $C_\chi$ is the conductor of $\chi$. Therefore $N$ is an induced modulu of $\chi$. We complete the proof of Lemma 4.5. \hfill \square

## 5. Proof of Theorem 1.3

We consider two cases to prove this theorem. First, if $(G, H) = 1$, then $(G, H) = 1$ in $\mathbb{F}_{q^n}[x]$. The Gauss sums on $\mathbb{F}_q[x]$ is that

$$G(\chi^{(n)}, \psi^{(n)}_G) = \bar{\chi}^{(n)}(G)G(\chi^{(n)}, \psi^{(n)}_1), \quad (5.1)$$

and the Gauss sums $G(\chi, \psi_G)$ on $\mathbb{F}_q[x]$ is following

$$G(\chi, \psi_G) = \bar{\chi}(G)G(\chi, \psi_1). \quad (5.2)$$

We note that $\chi^{(n)}(G) = \chi^n(G)$, $\psi_1 = E$, by Theorem 1.2, we have

$$(-1)^mG(\chi^{(n)}, \psi^{(n)}_G) = (-1)^m\bar{\chi}^{(n)}(G)G(\chi^{(n)}, \psi_1^{(n)})$$

$$= (\bar{\chi}(G)G(\chi, \psi_1))^n \quad (5.3)$$

Because of $(G, H) = 1$, then $m_1 = \deg(G, H) = 0$, and $\phi^{(n)}(H) = \phi^{(n)}(N)$, $\phi(H) = \phi(N)$, \cite[1.15]{mybook} of Theorem 1.3 holds in the case of $(G, H) = 1$. \hfill 11
Next, we suppose \((G, H) > 1\), and let \(H_1 = \frac{H}{(G, H)}\), \(G_1 = \frac{G}{(G, H)}\), thus \((G_1, H_1) = 1\). If both of \(G(\chi, \psi_G)\) and \(G(\chi^{(n)}, \psi_G^{(n)})\) are zero, then \((1.15)\) is trivial. Therefore, we may assume \(G(\chi, \psi_G) \neq 0\), or \(G(\chi^{(n)}, \psi_G^{(n)}) \neq 0\). By this assumption, then \(H_1\) is an induced modulu of both \(\chi\) and \(\chi^{(n)}\). By Lemma 3.4 we may write

\[
\chi = \chi_0 \delta, \quad \text{and} \quad \chi^{(n)} = \chi_0^{(n)} \delta^{(n)},
\]

(5.4) where \(\delta\) is a multiplicative character modulo \(H_1\), and \(\delta^{(n)}(A) = \delta(N(A))\) is a multiplicative character modulo \(H_1\) on \(\mathbb{F}_{q^n}[x]\). The Gauss sums on \(\mathbb{F}_{q^n}[x]\) is that

\[
G(\chi^{(n)}, \psi_G^{(n)}) = \sum_{D \mod H_1, D \in \mathbb{F}_q^n[x]} \chi_0^{(n)}(D)\delta^{(n)}(D)\psi_G^{(n)}(D)
\]

(5.5)

where summation \(\sum'\) means \((D, H_1) = 1\), and \(G(\delta^{(n)}, \psi_G^{(n)})\) is a Gauss sums modulo \(H_1\). The Gauss sums \(G(\chi, \psi_G)\) modulo \(H\) on \(\mathbb{F}_q[x]\) is that

\[
G(\chi, \psi_G) = \sum_{D \mod H} \delta(D)\psi_G(D)
\]

(5.6)

where \(G(\delta, \psi_G)\) is a Gauss sums modulo \(H_1\). Because of \((G_1, H_1) = 1\), the discussion for first case gives us that

\[
(-1)^{m-m_1} G(\delta^{(n)}, \psi_G^{(n)}) = \left((-1)^{m-m_1} G(\delta, \psi_G)\right)^n,
\]

(5.7)

where \(m - m_1 = \deg(H_1)\), and the equality \((1.15)\) of Theorem 1.3 follows immediately.
To prove (1.16) of Theorem 1.3, if $H|G$, then $\psi_G = \psi_0$ is the principal character modulo $H$, then both sides of (1.16) are zero, if $\chi$ is non-principal, then we may suppose that $H \nmid G$.

Since $H = P^k$, where $k \geq 1$, and $P$ is an irreducible in $\mathbb{F}_q[x]$, it is well-known that $P$ is product of exactly $(h, n)$ irreducibles in $\mathbb{F}_{q^n}[x]$, where $h = \deg(P)$ (see [5, Theorem 2.1], for example). If $H \nmid G$, then $\frac{H}{(G,H)} = N = P^{k_1}$, where $1 \leq k_1 \leq k$; it is easy to verify that

$$\phi(n)(\phi(n)(H))^{-1} = (\phi(N)\phi^{-1}(H))^n.$$ (5.8)

So (1.16) follows from (1.15), we complete the proof of Theorem 1.3.

References

[1] T. Apostol, *Introduction to Analytic Number Theory*, Springer–Verlag, New York Heidelberg Berlin, 1976.
[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. II*, Math. Z., 19 (1924), pp. 207–246.
[3] L. Carlitz, *The singular series for sums of squares of polynomials*, Duke Math. J., 14 (1947), pp. 1105–1120.
[4] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in Gewissen Zyklischen Fällen*, J. Reine. Angew. Math., 172 (1934), pp. 151–182.
[5] D. Hayes, *The distribution of irreducibles in GF[q, x]*, Trans. Amer. Math. Soc., 117 (1965), pp. 1017–1033.
[6] ———, *A polynomial generalized Gauss sum.*, J. Reine. Angew. Math., 222 (1966), pp. 113–119.
[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, vol. 84 of GTM, Springer–Verlag, New York Heidelberg Berlin, 1982.
[8] M. Rosen, *Number Theory in Function Fields*, vol. 210 of GTM, Springer–Verlag, New York Heidelberg Berlin, 2002.
[9] H. Schmid, *Relationen zwischen verallgemeinerten Gaußschen Summen.*, J. Reine. Angew. Math., 176 (1937), pp. 189–191.
[10] D. Thakur, *Gauss sums for $F_q[T]$*, Invent. Math., 94 (1988), pp. 105–112.