JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume 23, No. 4, December 2010

GAUSS SUMS ON $\mathbb{F}_q[T]$

Sunghan Bae* and Pyung-Lyun Kang**

Abstract. We study Gauss sums on $\mathbb{F}_q[T]$ and get some functional equations for $L-$functions.

0. Introduction

Gauss sum on $\mathbb{F}_q[T]$, which is called polynomial Gauss sum, was first studied by Hayes [3] and he proved an analogue of Davenport-Hasse Theorem about Gauss sums on finite fields. In this note we study polynomial Gauss sums by studying additive characters. Polynomial Gauss sums are just the usual Gauss sums for finite fields if the modulus of the character is irreducible. It is not only a generalization of Gauss sums on finite fields, but can also be thought as an analogue of classical Gauss sums on $\mathbb{Z}$.

In the first section we associate to each additive character λ a matrix Λ which enables us to do some linear algebra. Our first result is to determine the absolute values of Gauss sums (Theorem 1.5). We then prove an analogue of Polya inequality for character sums by using Gauss sums and additive character sums.

In the second section, we fix a specific additive character λ and express Dirichlet L-function on $\mathbb{F}_q[T]$ in a simple and explicit way (Theorem 2.1) with the help of the associated matrix Λ and Gauss sum. We use this expression to get functional equations for L-functions (Theorem 2.2). The more general form of functional equations for even characters was known before ([2]), but our method is very elementary and also covers the case of odd characters.

In the third section we use Gauss sums and the methods in the previous sections to deduce certain analogues of large sieve inequalities.

Received September 03, 2010; Accepted November 25, 2010.
2010 *Mathematics Subject Classifications*: Primary 11R24.
Correspondence should be addressed to Pyung-Lyun Kang, plkang@cnu.ac.kr.

Notations

p : an odd prime number, q : a power of p.
$\mathbb{F}_q$: the finite field with q elements containing a subfield $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.
$\mathbb{A} := \mathbb{F}_q[T]$, $\mathbb{A}^+ := \{M \in \mathbb{A} : \textit{monic}\}$.
For an integer $r \geq 0$,
$\mathbb{A}_r := \{M \in \mathbb{A} : \deg M = r\}$, $\mathbb{A}_r^+ = \mathbb{A}_r \cap \mathbb{A}^+$,
$\mathbb{A}_{\leq r} := \{M \in \mathbb{A} : \deg M \leq r\}$, $\mathbb{A}_{\leq r}^+ = \mathbb{A}_{\leq r} \cap \mathbb{A}^+$,
$\mathbb{A}_{<r} := \{M \in \mathbb{A} : \deg M < r\}$, $\mathbb{A}_{<r}^+ = \mathbb{A}_{<r} \cap \mathbb{A}^+$.
For $F \in \mathbb{A}_f^+$,
$\mathbb{A}(F) := \{M \in \mathbb{A} : \deg M < \deg F\}$, $\mathbb{A}^+(F) := \mathbb{A}(F) \cap \mathbb{A}^+$.
For $M \in \mathbb{A}$,
$M_F :=$ the polynomial of degree $< \deg F$, which is congruent to M modulo F,
$c_{F,i}(M) :=$ the coefficient of T^i in M_F,
$\mathbf{c}_F(M) := (c_{F,0}(M), c_{F,1}(M), \ldots, c_{F,f-1}(M))$.
ζ_p : a fixed primitive p-th root of unity in $\mathbb{C}$.
$Tr = Tr_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ the trace map.

1. Basic properties of polynomial Gauss sums

For a multiplicative character χ and an additive character λ modulo F of degree f, define *Gauss sum* $\tau(\chi, \lambda)$ by

$$\tau(\chi, \lambda) := \sum_{M \mod F} \chi(M)\lambda(M) = \sum_{M \in \mathbb{A}(F)} \chi(M)\lambda(M). \tag{1.1}$$

Note that when F is irreducible, then our $\tau(\chi, \lambda)$ is just the usual Gauss sum on the finite field $\mathbb{F}_{p^{\deg F}}$. Hence we may view our Gauss sum as a generalization of classical Gauss sum for finite field.

We need to investigate the properties of additive characters. Note that an additive character λ modulo F is completely determined by the additive characters $\lambda^{(i)} : \mathbb{F}_q \to \mathbb{C}^*$ for $i = 0, \cdots, f-1$, $f = \deg F$, where

$$\lambda^{(i)}(\alpha) = \lambda(\alpha T^i).$$

Since the bilinear form $< \alpha, \beta >= \zeta_p^{Tr(\alpha\beta)}$ is nondegenerate, each additive character $\lambda^{(i)}$ is determined by $\lambda_i \in \mathbb{F}_q$ such that

$$\lambda^{(i)}(\alpha) = \zeta_p^{Tr(\alpha\lambda_i)}.$$

Thus we say that an additive character modulo F is determined by $(\lambda_0, \dots, \lambda_{f-1}) \in \mathbb{F}_q^f$ if

$$\lambda(\sum_{i=0}^{f-1} \alpha_i T^i) = \prod_{i=0}^{f-1} \zeta_p^{Tr(\alpha_i\lambda_i)}.$$

For an additive character λ and $A \in \mathbb{A}$, λ_A is an additive character defined by $\lambda_A(M) = \lambda(AM)$. We say that an additive character λ modulo F is said to be *primitive* if the $\mathbb{F}_p$-bilinear form $<,>$ defined by $< A, B >:= \lambda(AB)$ is nondegenerate. It is clear from the definition that if λ is primitive, then any additive character modulo F is of the form λ_A for some $A \in \mathbb{A}$, and λ_A is primitive if and only if g.c.d.$(A, F) = 1$. We get easily, for g.c.d.$(A, F) = 1$,

$$\tau(\chi, \lambda_A) = \overline{\chi}(A)\tau(\chi, \lambda). \tag{1.2}$$

where $\overline{\chi}(A) = \overline{\chi(A)}$, the conjugate of $\chi(A)$ in $\mathbb{C}$. In fact, this will be generalized in Lemma 1.4 for all $A \in \mathbb{A}$.

We are going to associate an $f \times f$ matrix Λ to each additive character λ modulo F. Write

$$F = T^f - b_{f-1}T^{f-1} - \cdots - b_1 T - b_0.$$

Write $c_{F,j}(M)$ by $c_j(M)$ to simplify notations. For $i \geq 0$, write

$$T_F^{f+i} \equiv \sum_{k=0}^{f-1} \epsilon_{i,k} T^k \mod F.$$

Then we have the following recursive formula

$$\epsilon_{i+1,j} = \epsilon_{i,j-1} + b_j \epsilon_{i,f-1},$$

where $\epsilon_{i,j} = 0$ for $j < 0$, $\epsilon_{0,j} = 0$ for $j < f-1$, $\epsilon_{0,f-1} = 1$ and $\epsilon_{1,j} = b_j$. Define $\lambda_{i,j}$ for $0 \leq i, j \leq f-1$ by the following:

$$\lambda_{i,j} = \lambda_{i+j} \quad \text{if } 0 \leq j < f - i$$

$$\lambda_{i,f-i+k} = \sum_{j=0}^{f-1} \epsilon_{k,j}\lambda_j \quad \text{for } 0 \leq k < i.$$

Let Λ be the $f \times f$ matrix with entries $\lambda_{i,j}$. Then we can easily see that

$$\lambda(AX) = \zeta_p^{Tr(\sum_{k=0}^{f-1} c_k(AX)\lambda_k)} = \zeta_p^{Tr(\mathbf{c}_F(A)\Lambda\mathbf{c}_F(X)^t)}. \tag{1.3}$$

Thus we have the following lemma. Note that Λ is symmetric, since $\lambda(AX) = \lambda(XA)$. In fact, $\lambda_{i,j} = \lambda_{k,\ell}$ whenever $i + j = k + \ell$.

Lemma 1.1. *An additive character λ is primitive if and only if the associated matrix Λ is nonsingular.*

Example 1.2. Let λ be the additive character determined by $(0, \ldots, 0, 1)$. Then the associated matrix Λ is given by

$$\Lambda = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 1 & \epsilon_{0,d-1} \\ 0 & 0 & \ldots & \epsilon_{0,d-1} & \epsilon_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \epsilon_{0,d-1} & \ldots & \epsilon_{d-3,d-1} & \epsilon_{d-2,d-1} \end{pmatrix}.$$

Therefore Λ is nonsingular and so λ is primitive.

Lemma 1.3. *Let λ be an additive character modulo F of degree f and Λ its associated matrix. Then*

$$\sum_{A \mod F} \lambda(AX) = \begin{cases} q^f & \text{if } \Lambda\mathbf{x}^t = \mathbf{0} \\ 0 & \text{otherwise} \end{cases} \tag{1.4}$$

In particular, if λ is primitive, then

$$\sum_{A \mod F} \lambda(AX) = \begin{cases} q^f & \text{if } X = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{1.4'}$$

As in [6], Lemma 4.7, we have the following lemma.

Lemma 1.4. *Let χ be a primitive multiplicative character and λ an additive character modulo F of degree f. Then we have, for $N \in \mathbb{A}$,*

$$\chi(N)\tau(\overline{\chi}, \lambda) = \sum_{M \mod F} \overline{\chi}(M)\lambda(MN) = \tau(\overline{\chi}, \lambda_N) \tag{1.5}$$

and

$$\lambda(A) = \frac{1}{\phi(F)} \sum_{\chi \mod F} \overline{\chi}(A)\tau(\chi, \lambda). \tag{1.6}$$

The main theorem of this section is the following.

Theorem 1.5. *Let χ be a primitive multiplicative character and λ an additive character modulo F of degree f. Then*

$$|\tau(\chi,\lambda)| = \begin{cases} q^{\frac{f}{2}} & \text{if } \lambda \text{ is primitive} \\ 0 & \text{if } \lambda \text{ is not primitive.} \end{cases} \tag{1.7}$$

Proof. By Lemma 1.4 above, we have

$$\begin{aligned}
|\tau(\chi,\lambda)|^2 &= \tau(\chi,\lambda)\overline{\tau(\chi,\lambda)} \\
&= \tau(\chi,\lambda) \sum_{N \mod F} \overline{\chi}(N)\lambda(-N) \\
&= \sum_{N \mod F} \sum_{M \mod F} \chi(M)\lambda(M)\overline{\chi}(N)\lambda(-N) \\
&= \sum_{N \mod F} \sum_{M \mod F} \chi(M)\lambda(N(M-1)) \\
&= \sum_{M \mod F} \chi(M) \sum_{N \mod F} \lambda(N(M-1)).
\end{aligned}$$

When λ is primitive, the result follows at once from (1.4'). Suppose now that λ is not primitive. Let $G(\not\equiv 0 \mod F)$ be a polynomial of minimal degree with $\Lambda \mathbf{c}_F(G)^t = 0$. By the minimality, we see that $G \mid F$ and any B with $\Lambda \mathbf{c}_F(B)^t = 0$ is divisible by G. Then, by (1.4),

$$|\tau(\chi,\lambda)|^2 = q^f \sum_{H\equiv 1 \mod G} \chi(H). \tag{*}$$

But since χ is primitive, the right hand side of (*) must be 0. □

Corollary 1.6. *Let χ be a primitive multiplicative character and λ a primitive additive character modulo F of degree f. Then*

$$\chi(N) = \frac{\tau(\chi,\lambda_N)}{q^f} \sum_{M \mod F} \overline{\chi}(M)\lambda(-MN) = \frac{\tau(\chi,\lambda)\tau(\overline{\chi},\overline{\lambda}_N)}{q^f}. \tag{1.7}$$

Proof. Note that $\overline{\tau(\chi,\lambda)} = \tau(\overline{\chi},\overline{\lambda})$. The result follows from Lemma 1.4 and Theorem 1.5. □

For the later use we need to compute the following sums associated to the primitive additive character λ modulo F. Let r be a nonnegative integer and $X \in \mathbb{A}$.

$$\alpha_r(\lambda, X) := \sum_{N \in \mathbb{A}_r^+(F)} \lambda(-NX)$$

$$\beta_r(\lambda, X) := \sum_{N \in \mathbb{A}_r(F)} \lambda(-NX)$$

Note that $\alpha_r(\lambda, X) = 0$ for $r \geq f$ and $\beta_r(\lambda, X) = 0$ for $r \geq f - 1$, unless $X = 0$.

Lemma 1.7. *Let the notations be as before and write*

$$\Lambda \mathbf{c}_F(X) = (D_0(X), D_1(X), \ldots, D_{f-1}(X)).$$

Then we have

i) *for* $r < f$,

$$\alpha_r(\lambda, X) = \begin{cases} q^r \zeta_p^{Tr(D_r(X))} & \text{if } D_0(X) = \cdots = D_{r-1}(X) = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{1.8}$$

ii) *for* $r < f - 1$,

$$\beta_r(\lambda, X) = \begin{cases} (q-1)q^r & \text{if } D_0(X) = \cdots = D_r(X) = 0 \\ -q^r & \text{if } D_0(X) = \cdots = D_{r-1}(X) = 0 \text{ and } D_r(X) \neq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{1.9}$$

Proof. From (1.2) and (1.3), we see that

$$\alpha_r(\lambda, X) = \zeta_p^{Tr(D_r(X))} \prod_{i=0}^{r-1} \left(\sum_{a_i \in \mathbb{F}_q} \zeta_p^{Tr(a_i D_i(X))} \right)$$

and the result for α follows. Also,

$$\beta_r(\lambda, X) = (\sum_{a \in \mathbb{F}_q^*} \zeta_p^{Tr(a D_r(X))}) \prod_{i=0}^{r-1} \left(\sum_{a_i \in \mathbb{F}_q} \zeta_p^{Tr(a_i D_i(X))} \right)$$

Now the result follows from the fact that

$$\sum_{a\in\mathbb{F}_q} \zeta_p^{Tr(aD_r(X))} = \begin{cases} q & \text{if } D_r(X)=0 \\ 0 & \text{otherwise.} \end{cases}$$

$\square$

Now we will prove the following analogue of Polya inequality ([1], Theorem 8.21).

PROPOSITION 1.8. *Let χ be a primitive multiplicative character modulo F of degree f. Then*

i) $|\sum_{N\in\mathbb{A}_r^+}\chi(N)| \le q^{f/2}$ *and* $|\sum_{N\in\mathbb{A}_{\le r}^+}\chi(N)| \le fq^{f/2}$

ii) $|\sum_{N\in\mathbb{A}_r}\chi(N)| \le 2q^{f/2}$ *and* $|\sum_{N\in\mathbb{A}_{\le r}}\chi(N)| \le 2fq^{f/2}$.

Proof. Note that, for $r \ge f$, $\sum_{N\in\mathbb{A}_r^+}\chi(N) = 0 = \sum_{N\in\mathbb{A}_r}\chi(N)$. We thus assume that $r < f$. Let λ be a primitive additive character modulo F. By Theorem 1.5 and Corollary 1.6 we have, for any subset $\mathbb{B}$ of $\mathbb{A}$,

$$\begin{aligned} q^{\frac{f}{2}}|\sum_{N\in\mathbb{B}}\chi(N)| &= |\sum_{N\in\mathbb{B}}\sum_{M \mod F}\overline{\chi}(M)\lambda(-MN)| \\ &\le \sum_{M \mod F}|\sum_{N\in\mathbb{B}}\lambda(-MN)|. \end{aligned}$$

We have to determine the sum $C_{\mathbb{B}}(M) := \sum_{N\in\mathbb{B}}\lambda(-MN)$ for each M. First let $\mathbb{B} = \mathbb{A}_r^+$. Then $|C_{\mathbb{B}}(M)| = |\alpha_r(\lambda, M)| = q^r$ if and only if M satisfies $D_i(M) = 0$ for $i = 0,\dots,r-1$, and 0 otherwise. Thus $\mathbf{c}_F(M) = (c_0(M),\dots,c_{f-1}(M))$ satisfies r linearly independent relations, and so there are q^{f-r} possible M's with $|C_{\mathbb{A}_r^+}(M)| = q^r$. Hence we get the result in this case. Similarly, by Lemma 1.7, $|C_{\mathbb{A}_r}(M)| = (q-1)q^r$ for q^{f-r-1} possible M's, and $|C_{\mathbb{A}_r}(M)| = q^r$ for $q^{f-r}\frac{q-1}{q}$ possible M's and 0 otherwise. Hence

$$q^{\frac{f}{2}}|\sum_{N\in\mathbb{A}_r}\chi(N)| \le 2(q-1)q^{f-1} < 2q^f,$$

and we get the result in this case too. The other cases follows from these by summing over r. $\square$

2. Application to Dirichlet L-series

In this section we consider the Dirichlet L-series

$$L(s,\chi) := \sum_{N\in\mathbb{A}^+} \frac{\chi(N)}{|N|^s},$$

where $|N| = q^{\deg N}$.

Thus for primitive λ, we have, using Lemma 1.2,

$$\begin{aligned}
L(s,\chi) &= \sum_{A\in\mathbb{A}(F)} \chi(A) \sum_{N\equiv A,\ \text{monic}} \frac{1}{|N|^s} \\
&= \sum_{A\in\mathbb{A}(F)} \chi(A) \sum_{N\ \text{monic}} \frac{1}{q^f} \sum_{X\in\mathbb{A}(F)} \lambda((A-N)X)\frac{1}{|N|^s} \\
&= \frac{1}{q^f} \sum_{A\in\mathbb{A}(F)} \sum_{X\in\mathbb{A}(F)} \chi(A)\lambda(AX) \sum_{N\in\mathbb{A}^+} \frac{\lambda(-NX)}{|N|^s} \\
&= \frac{\tau(\chi,\lambda)}{q^f} \sum_{X\in\mathbb{A}(F)} \overline{\chi}(X) \sum_{N\in\mathbb{A}^+} \frac{\lambda(-NX)}{|N|^s}.
\end{aligned} \tag{2.1}$$

Since $\sum_{N\in\mathbb{A}_r^+} \lambda(NB) = 0$ for $B \not\equiv 0 \mod F$ and $r \geq f$, we have

$$L(s,\chi) = \frac{\tau(\chi,\lambda)}{q^f} \sum_{X\in\mathbb{A}(F)} \overline{\chi}(X) \sum_{N\in\mathbb{A}^+_{<f}} \frac{\lambda(-NX)}{|N|^s}. \tag{2.2}$$

Now let λ be the primitive additive character given in Example 1.2. In this case it is easy to see that $D_i(X) = 0$ for $i = 0,\dots,r-1$ is equivalent to the condition that $c_{f-1}(X) = \cdots = c_{f-r}(X) = 0$. Then $D_r(X) = c_{f-r}(X)$ in this case. Therefore, by Lemma 1.7,

$$\alpha_r(\lambda, X) = \begin{cases} q^r \zeta_p^{Tr(c_{f-r}(X))} & \text{if } \deg X < f-r, \\ 0 & \text{otherwise.} \end{cases}$$

Write $\ell(X)$ for the leading coefficient of X. Then, for $X \in \mathbb{A}(F)$,

$$\begin{aligned}
&\sum_{N\in\mathbb{A}^+(F)} \frac{\lambda(-NX)}{|N|^s} \\
&= 1 + q^{1-s} + \cdots + q^{(f-\deg X-2)(1-s)} + \zeta_p^{Tr(\ell(X))} q^{(f-\deg X-1)(1-s)}.
\end{aligned}$$

Therefore we get the following theorem, which is analogous to [5], Theorem 2.1.

THEOREM 2.1. *Let χ be a multiplicative character with conductor F of degree f. Let λ be the additive character modulo F defined by $\lambda_i = 0$ for $0 \le i < f-1$ and $\lambda_{f-1} = 1$. Then we have*

$$L(s,\chi) = \frac{\tau(\chi,\lambda)}{q^f} \sum_{X \in \mathbb{A}(F)} \overline{\chi}(X) Z(X,s), \tag{2.3}$$

where

$$\begin{aligned} &Z(X,s) \\ &= 1 + q^{1-s} + \cdots + q^{(f-\deg X-2)(1-s)} + \zeta_p^{Tr(\ell(X))} q^{(f-\deg X-1)(1-s)}. \end{aligned} \tag{2.4}$$

Now we will derive the functional equation for L-functions. Suppose that χ is a nontrivial character of conductor F of degree f. Since $\sum_{N \in \mathbb{A}_r^+} \chi(N) = 0$ for $r \ge f$, we have

$$L(s,\chi) = \sum_{X \in \mathbb{A}(F)^+} \chi(X)|X|^{-s} = \sum_{X \in \mathbb{A}(F)^+} \chi(X) q^{-s \deg X}. \tag{2.5}$$

By Theorem 2.1, we see that

$$\begin{aligned} &L(1-s,\overline{\chi}) \\ &= \frac{\tau(\overline{\chi},\lambda)}{q^f} \sum_{X \in \mathbb{A}(F)} \chi(X) \left((1 + q^s + \cdots + q^{(f-\deg X-2)s} + q^{(f-\deg X-1)s} \zeta_p^{Tr(\ell(X))} \right) \\ &= \frac{\tau(\overline{\chi},\lambda)}{q^f} \sum_{X \in \mathbb{A}(F)} \chi(X) \left(\frac{q^{(f-\deg X-1)s} - 1}{q^s - 1} + q^{(f-\deg X-1)s} \zeta_p^{Tr(\ell(X))} \right). \end{aligned} \tag{2.6}$$

We say that a multiplicative character χ is *even* if $\chi(a) = 1$ for any $a \in \mathbb{F}_q^*$. Otherwise, χ is said to be *odd.* Note that χ is odd if and only if $\sum_{a \in \mathbb{F}_q^*} \chi(a) = 0$. Assume first that χ is even. Then (2.6) becomes, since $\sum_{a \in \mathbb{F}_q} \zeta_p^{Tr(a)} = 0$,

$$\begin{aligned} &L(1-s,\overline{\chi}) \\ &= \frac{\tau(\overline{\chi},\lambda)}{q^f} \sum_{X \in \mathbb{A}(F)^+} \chi(X) \left((q-1) \frac{q^{(f-\deg X-1)s} - 1}{q^s - 1} - q^{(f-\deg X-1)s} \right) \\ &= \frac{\tau(\overline{\chi},\lambda)}{q^f} q^{(f-1)s} \left(\frac{q-1}{q^s-1} - 1 \right) \sum_{X \in \mathbb{A}(F)^+} \chi(X) q^{-s \deg X} \\ &= \frac{\tau(\overline{\chi},\lambda)}{q^f} q^{(f-1)s} \frac{q - q^s}{q^s - 1} L(s,\chi). \end{aligned}$$

If we take

$$\Lambda(s,\chi) := \frac{1}{1-q^{-s}} L(s,\chi),$$

we have the following functional equation (cf; [2], Proposition 3.3)

$$\Lambda(1-s,\overline{\chi}) = \frac{\tau(\overline{\chi},\lambda)q^{(f-2)s}}{q^{f-1}}\Lambda(s,\chi).$$

Now assume that χ is odd. Then

$$\begin{aligned} L(1-s,\overline{\chi}) &= \frac{\tau(\overline{\chi},\lambda)}{q^f} \sum_{X\in\mathbb{A}(F)} \chi(X) q^{(f-1)s} q^{-s\deg X} \zeta_p^{Tr(\ell(X))} \\ &= \frac{\tau(\overline{\chi},\lambda)q^{(f-1)s}}{q^f} \sum_{X\in\mathbb{A}(F)^+} \chi(X) q^{-s\deg X} \sum_{a\in\mathbb{F}_p^*} \chi(a)\zeta_p^{Tr(a)} \\ &= \frac{\tau(\overline{\chi},\lambda)\tau_1(\chi,\zeta_p)q^{(f-1)s}}{q^f} L(s,\chi), \end{aligned}$$

where $\tau_1(\chi,\zeta_p) = \sum_{a\in\mathbb{F}_q^*} \chi(a)\zeta_p^{Tr(a)}$. We summarize these results in the following Theorem

THEOREM 2.2. *Let χ be a Dirichlet character of conductor F degree f. Let λ be the additive character modulo F defined by $\lambda_i = 0$ for $0 \le i < f-1$ and $\lambda_{f-1} = 1$.*

i) *If χ is even, then*

$$L(1-s,\overline{\chi}) = \frac{\tau(\overline{\chi},\lambda)}{q^f} q^{(f-1)s} \frac{q-q^s}{q^s-1} L(s,\chi) \tag{2.7}$$

or, equivalently

$$\Lambda(1-s,\overline{\chi}) = \frac{\tau(\overline{\chi},\lambda)q^{(f-2)s}}{q^{f-1}} \Lambda(s,\chi) \tag{2.8}$$

ii) *If χ is odd, then*

$$L(1-s,\overline{\chi}) = \frac{\tau(\overline{\chi},\lambda)\tau_1(\chi,\zeta_p)q^{(f-1)s}}{q^f} L(s,\chi) \tag{2.9}$$

3. Large sieve inequalities

For each $F \in \mathbb{A}_f^+$ we let λ^F to be the primitive additive character modulo F defined by $\lambda_i^F = 0$ for $0 \le i < d-1$ and $\lambda_{f-1}^F = 1$. Let Λ^F be the associated matrix. We are going to derive analogues of large sieve inequalities.

Lemma 3.1. *Let $F, G \in \mathbb{A}_f^+$. Suppose that $n \ge f$, $A \in \mathbb{A}(F)$, $B \in \mathbb{A}(G)$, not both 0, and the pairs $(F, A) \ne (G, B)$. Write $D_A^F = \mathbf{c}_F(A)\Lambda^F$ and $D_B^G = \mathbf{c}_G(B)\Lambda^G$. Then*

$$\sum_{N \in \mathbb{A}_n^+} \lambda^F(AN)\overline{\lambda^G(BN)} = \begin{cases} \zeta_p^{Tr(D_A^F \mathbf{c}_F(T^f)^t - D_B^G \mathbf{c}_G(T^f)^t)} q^f & \text{if } n = f \text{ and } D_A^F = D_B^G \\ 0 & \text{otherwise} \end{cases}$$

Proof. Write $\mathbf{x}_i = \mathbf{c}_F(T^i)$ and $\mathbf{y}_i = \mathbf{c}_G(T^i)$. Then, for $n \ge f$, writing $N = T^n + a_{n-1}T^{n-1} + \cdots + a_0$,

$$\begin{aligned} &\sum_{N \in \mathbb{A}_n^+} \lambda^F(AN)\overline{\lambda^G(BN)} \\ &= \zeta_p^{Tr(D_A^F \mathbf{x}_n - D_B^G \mathbf{y}_n)} \Big(\sum_{a_{n-1} \in \mathbb{F}_q} \zeta_p^{Tr(a_{n-1}(D_A^F \mathbf{x}_{n-1} - D_B^G \mathbf{y}_{n-1}))} \Big) \cdots \\ &\quad \cdot \Big(\sum_{a_f \in \mathbb{F}_q} \zeta_p^{Tr(a_f(D_A^F \mathbf{x}_f - D_B^G \mathbf{y}_f))} \Big) \Big(\sum_{M \in \mathbb{A}_{f-1}} \zeta_p^{Tr((D_A^F - D_B^G)\mathbf{c}_F(M))} \Big), \end{aligned}$$

since $\mathbf{c}_F(M) = \mathbf{c}_G(M)$ for $\deg M < f$. Now it is not hard to see that

$$\sum_{M \in \mathbb{A}_{f-1}} \zeta_p^{Tr((D_A^F - D_B^G)\mathbf{c}_F(M))} = \begin{cases} q^f & \text{if } D_A^F = D_B^G \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that $\mathbf{x}_f \ne \mathbf{y}_f$ unless $F = G$, and

$$\sum_{a_f \in \mathbb{F}_q} \zeta_p^{Tr(a_f(D_A^F \mathbf{x}_f - D_B^G \mathbf{y}_f))} = 0,$$

if $D_A^F = D_B^G$ and $\mathbf{x}_f \ne \mathbf{y}_f$. Now the result follows since $(F, A) \ne (G, B)$. $\square$

We first prove the following analogue of additive large sieve inequality ([4] Theorem 7.11).

Theorem 3.2. *Let w_N be a complex number for each $N \in \mathbb{A}$ of degree n. Then we have*

$$\sum_{F\in\mathbb{A}_f^+}\ \sum_{A \bmod {}^*F} \Big|\sum_{N\in\mathbb{A}_n^+} w_N\lambda^F(AN)\Big|^2 \le (q^n+q^{2f})\|w\|^2, \tag{3.1}$$

where $\|w\|^2 = \sum_N |w_N|^2$.

Proof. Let

$$\mathcal{C} := \{(F,A) : F\in\mathbb{A}_f^+,\ A\in\mathbb{A}(F),\ A \text{ is prime to } F\}.$$

From the Duality Principle([4], p170) it suffices to show that

$$\sum_{N\in\mathbb{A}_n^+} \Big|\sum_{(F,A)\in\mathcal{C}} z_{(F,A)}\lambda^F(AN)\Big|^2 \le (q^n+q^{2f})\|z\|^2,$$

where $\|z\|^2 = \sum_{(F,A)\in\mathcal{C}} |z_{(F,A)}|^2$. The inner sum is equal to

$$\begin{aligned}&\sum_{(F,A)\in\mathcal{C}}\ \sum_{(G,B)\in\mathcal{C}} z_{(F,A)}\overline{z}_{(G,B)}\frac{\lambda^F(AN)}{\lambda^G(BN)}\\ &= \|z\|^2 + \sum\ \sum_{(F,A)\neq(G,B)} z_{(F,A)}\overline{z}_{(G,B)}\frac{\lambda^F(AN)}{\lambda^G(BN)}.\end{aligned}$$

Thus

$$\begin{aligned}&\sum_{N\in\mathbb{A}_n^+} \Big|\sum_{(F,A)\in\mathcal{C}} z_{(F,A)}\lambda^F(AN)\Big|^2\\ &= q^n\|z\|^2 + \sum\ \sum_{(F,A)\neq(G,B)} z_{(F,A)}\overline{z}_{(G,B)}\sum_{N\in\mathbb{A}_n^+}\frac{\lambda^F(AN)}{\lambda^G(BN)}.\end{aligned}$$

For $n > f$ the result follows from Lemma 3.1 since we clearly have $q^n < q^n + q^{2f}$. Now assume that $n \le f$. Let $D(F,A,G,B) = (D_A^F - D_B^G)^*$, where $(a_0, a_1, \dots, a_{f-1})^* = (a_0, a_1, \dots, a_{n-1})$. Then it is easy to see that

$$\sum_{N\in\mathbb{A}_n^+}\frac{\lambda^F(AN)}{\lambda^G(BN)} = \begin{cases} \zeta_p^a q^n & \text{for some integer } a \text{ if } D(F,A,G,B)=0\\ 0 & \text{otherwise.}\end{cases}$$

Then

$$
\begin{aligned}
&|\sum \sum_{(F,A)\neq(G,B)} z_{(F,A)}\overline{z}_{(G,B)} \sum_{N\in\mathbb{A}_n^+} \frac{\lambda^F(AN)}{\lambda^G(BN)}| \\
&\leq q^n \sum \sum_{(F,A)\neq(G,B),D(F,A,G,B)=0} |z_{(F,A)}\overline{z}_{(G,B)}| \\
&\leq q^n \sum \sum_{(F,A)\neq(G,B),D(F,A,G,B)=0} \frac{1}{2}(|z_{(F,A)}|^2 + |z_{(G,B)}|^2).
\end{aligned}
$$

For a given (F, A) and G, there exist at most q^{f-n} such $B \in \mathbb{A}(G)$ making $D(F, A, G, B) = 0$. Hence the result follows in this case too. □

Now we are going to prove the following analogue of multiplicative large sieve inequality ([4] Theorem 7.13).

THEOREM 3.3. *With the same notations as in Theorem 3.2, we have*

$$
\sum_{F\in\mathbb{A}_f^+} \frac{q^f}{\phi(F)} \sum_{\chi \mod {}^*F} |\sum_{N\in\mathbb{A}_n^+} w_N\chi(N)|^2 \leq (q^f + q^n)q^f\|w\|^2,
$$

where $\sum_{\chi \mod {}^*F}$ *means summing over primitive multiplicative characters modulo* F.

Proof. Before starting the proof we introduce some notations. For an additive character ψ modulo Q,

$$
c_Q(\psi, N) := \sum_{B \mod {}^*Q} \psi(BN).
$$

For a positive integer n and $A \in \mathbb{A}$,

$$
S_n(A, \psi) := \sum_{N\in\mathbb{A}_n^+} w_N\psi(AN).
$$

Suppose that χ is induced by a primitive character χ_S modulo S with $F = RS$ and $(R, S) = 1$. Then

$$
\begin{aligned}
&\sum_{A \mod F} \chi(A)\lambda^F(AN) \\
&= \sum_{B \mod {}^*R} \sum_{C \mod {}^*S} \chi(BS + CR)\lambda^F((BS + CR)N) \\
&= \sum_{B \mod {}^*R} \sum_{C \mod {}^*S} \chi_S(CR)\lambda_S^F((BN)\lambda_R^F(CN)
\end{aligned}
$$

$$
\begin{aligned}
&= \chi_S(R) \sum_{B \mod {}^*R} \lambda_S^F(BN) \sum_{C \mod {}^*S} \chi_S(C)\lambda_R^F(CN) \\
&= \chi_S(R) c_R(\lambda_S^F, N)\overline{\chi}(N)\tau(\chi_S, \lambda_R^F) \qquad \text{by Lemma 1.3.}
\end{aligned}
$$

Thus

$$
\begin{aligned}
\sum_{N \in \mathbb{A}_n^+} w_N \overline{\chi}(N) c_R(\lambda_S^F, N) &= \sum_{N \in \mathbb{A}_n^+} w_N \frac{\sum_{a \mod F} \chi(A)\lambda^F(AN)}{\chi_S(R)\tau(\chi_S, \lambda_R^F)} \\
&= \frac{\overline{\chi}_S(R)}{\tau(\chi_S, \lambda_R^F)} \sum_{A \mod F} \chi(A) S_n(A, \lambda^F).
\end{aligned}
$$

Then

$$
\begin{aligned}
&\sum_{F \in \mathbb{A}_f^+} \sum_{\substack{RS=F \\ (R,S)=1 \\ R,S \text{ monic}}} \frac{|S|}{\phi(RS)} \sum_{\chi \mod {}^*S} |\sum_{N \in \mathbb{A}_n^+} w_N \overline{\chi}(N) c_R(\lambda_S^F, N)|^2 \\
&\leq \sum_{F \in \mathbb{A}_f^+} \frac{|S|}{\phi(F)} \sum_{\chi \mod F} |\sum_{A \mod F} \chi(A) S_n(A, \lambda^F)|^2 \frac{1}{|\tau(\chi_S, \lambda_R^F)|^2} \\
&= \sum_{F \in \mathbb{A}_f^+} \frac{1}{\phi(F)} \sum_{\chi \mod F} |\sum_{A \mod F} \chi(A) S_n(A, \lambda^F)|^2 \quad \text{by Theorem 1.5} \\
&= \sum_{F \in \mathbb{A}_f^+} \sum_{A \mod {}^*F} |\sum_{N \in \mathbb{A}_n^+} w_N \lambda^F(AN)|^2 \quad \text{by the orthogonality of characters} \\
&\leq (q^n + q^{2f})\|w\|^2 \qquad \text{by Theorem 3.2.}
\end{aligned}
$$

Hence we get the result by ignoring all terms with $R \neq 1$. □

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York Heidelberg Berlin, 1976.

[2] B. Gross and M. Rosen, *Fourier series and the special values of L-functions*, Advances in Math. **69** (1988), 1-31.

[3] D. Hayes, *A polynomial generalized Gauss sum*, J. reine angew. Math. **222** (1966) 113-119.

[4] H. Iwaniec and E. Kowalski, *Analytic Number Theory. In: Colloquium Publications* **53**, Amer. Math. Soc. 2004.

[5] S. Lang, *Cyclotomic fields I and II*, Springer-Verlag, New York Heidelberg Berlin, 1990.

[6] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York Heidelberg Berlin, 1982.

*
Department of Mathematics
KAIST
Daejeon 305-701, Republic of Korea
E-mail: shbae@kaist.ac.kr

**
Department of Mathematics
Chungnam National University
Daejeon 305-764, Republic of Korea
E-mail: plkang@cnu.ac.kr