ON POLYNOMIAL WARING-GOLDBACH PROBLEM

CHIH-NUNG HSU

1. Introduction

Waring's problem is to prove that every natural number (resp. sufficiently large number) is the sum of a bounded number of d-th powers. Goldbach's problem is to prove that every even number greater than 3 is a sum of two primes and every odd number greater than 5 is a sum of three primes. The Waring-Goldbach problem asks for the possibility of expressing natural numbers as sums of d-th powers of primes ($d \geq 2$), with a bounded number of summands.

For $d = 1$, the first important result for the ternary Goldbach problem, due to Hardy and Littlewood in 1923, is an asymptotic theorem. Using the circle method and a modified form of the Riemann hypothesis, they proved that every sufficiently large odd number is the sum of three primes. In 1937, without appealing to any form of the Riemann's hypothesis and modifying the method of Hardy and Littlewood, Vinogradov also proved the ternary Goldbach problem for sufficiently large odd numbers. The best result for the binary Goldbach's problem is, due to Chen in 1974, that every sufficiently large even number can be written as the sum of an odd prime and a number that is either prime or the product of two primes.

For $d \geq 2$, Hua proved the following theorem (cf. [11], theorems 11 and 12): If positive integer s satisfies

$$s \geq \begin{cases} 2^d + 1 & \text{if } 2 \leq d \leq 10, \\ 2d^2(2\ln d + \ln\ln d + 2.5) & \text{if } 10 < d, \end{cases}$$

then every sufficiently large number N can be written as a sum of s d-th powers of primes provided

$$N \equiv s \pmod{K}, \tag{1}$$

where

$$K = \prod_{(p-1)|d} p^{r_p},$$

$r_2 = \theta_2 + 2, r_p = \theta_p + 1 (p \geq 3)$, and θ_p is the largest integer satisfying $p^{\theta_p} | d$. The condition (1) for N arises from the structure theorem of $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

1991 *Mathematics Subject Classification.* Primary, 11P.

Key words and phrases. circle method; Waring problem; polynomial Waring-Goldbach problem.

Also, Hua obtained an asymptotic formula for the number of ways N may be written as a sum of s d-th powers of primes.

In this paper, I explore the problem of expressing polynomials (over finite fields) as sums of d-th powers of irreducibles ($d \geq 2$). This is a problem of the same kind as classical Waring-Goldbach problem. We call it the polynomial Waring-Goldbach problem. Let $\mathbb{F}_q$ be the finite field with q elements and let prime p be its characteristic. Let $\mathbf{A} = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$ and let $\mathbf{A}_+$ denote the subset of $\mathbf{A}$ consisting of all monic polynomials. Suppose we wish to write $M \in \mathbf{A}$ in the form

$$M = z_1^d + z_2^d + \cdots + z_s^d \tag{2}$$

with irreducible polynomials $z_1, z_2, \cdots, z_s \in \mathbf{A}$. As in the strict analogue in $\mathbf{A}$ of the classical Waring problem, formulated by Carlitz (cf. [4], chapter 1), we say that the polynomial M is the strict sum of s d-th powers of irreducibles if the degrees $\deg z_i$ in (2) satisfy $\deg z_i \leq \lceil \deg M/d \rceil$ for all $1 \leq i \leq s$, where $\lceil x \rceil$ is the least integer which is greater than or equal to x. If we restrict the irreducibles z_i to be such that

$$\deg M/d \leq \deg z_i < \deg M/d + 1,$$

then it is easy to deduce that the coefficient of the $d \cdot \lceil \deg M/d \rceil$-th term of M is equal to

$$(\operatorname{sgn} z_1)^d + (\operatorname{sgn} z_2)^d + \cdots + (\operatorname{sgn} z_s)^d,$$

where $\operatorname{sgn} z_i$ denote the leading coefficient of z_i. Thus our version of the polynomial Waring-Goldbach problem is to counting the number of the solutions of

$$M = r_1 P_1^d + r_2 P_2^d + \cdots + r_s P_s^d$$

with monic irreducibles $P_1, P_2, \cdots, P_s$ satisfying

$$\deg M/d \leq \deg P_i < \deg M/d + 1, \quad (1 \leq i \leq s),$$

and $r_1, r_2, \cdots, r_s \in {\mathbb{F}_q^\times}^d$ satisfying

$$r_1 + r_2 + \cdots + r_s = \text{ coefficient of the } d \cdot \lceil \deg M/d \rceil \text{-th term of } M.$$

The above restriction is the most restrictive degree condition. We denote this number by $G_{z^d,s}(M)$. The main result of this paper is given in theorem 10.2: Suppose $2 \leq d < p$ and

$$s \geq \begin{cases} 2^d + 1 & \text{if } 2 \leq d < 11, \\ 2d^2(2\ln d + \ln\ln d + 2) - 4d + 2 & \text{if } d \geq 11. \end{cases}$$

Then for any given integer $s_1 > s$, we have

$$G_{z^d,s}(M) - \frac{q^{N(s-d)}}{N^s} \cdot \mathfrak{S}(M) \ll \frac{q^{N(s-d)}}{N^{s_1}},$$

where the implied constant depends only on d, s, s_1, and q, and $\mathfrak{S}(M) > 0$ provided

$$M \equiv s \pmod{T^p - T} \quad \text{if } q = p \text{ and } d = p - 1. \tag{3}$$

The condition (3) arises from the Fermat's little theorem. The polynomial Waring-Goldbach singular series $\mathfrak{S}(M)$ is defined in section 9. Moreover, in theorem 10.1, we obtain an asymptotic formula $G_{f,s}(M)$ for general polynomial $f(z) \in \mathbf{A}[z]$.

For polynomial Waring problem and polynomial Goldbach problem (i.e., the case when $d = 1$), we refer to [4], [6], [1], and [18]. The rest of this Introduction, we survey the procedure for solving the polynomial Waring-Goldbach problem.

For each positive integer Q and for each polynomial $f(x) \in \mathbb{Z}[x]$ of degree $d \geq 1$, let the exponential sum

$$S(f, Q) = \sum_{x=1}^{Q} \exp\left(\frac{2\pi f(x)}{Q}\right).$$

In 1940, Hua [10] proved that if the coefficients are relatively prime, then for arbitrary $\epsilon > 0$,

$$|S(f, Q)| \ll Q^{1-\frac{1}{d}+\epsilon}, \tag{4}$$

where the implied constant depends only on d and ϵ. Another Hua's estimate for exponential sums is the well-known Hua's lemma (cf. [11], theorem 4 or [17], lemma 2.5). Let $g(x)$ denote a polynomial of degree $d \geq 1$ with coefficients in $\mathbb{R}$. Then for $1 \leq v \leq d$

$$\int_0^1 \left|\sum_{x=1}^{N} \exp(g(x) \cdot y)\right|^{2^v} dy \ll N^{2^v - v + \epsilon}, \tag{5}$$

where the implied constant depends only on d and ϵ.

The purpose of sections 2, 3 and 4 is to establish the analogous inequalities (4) and (5) for polynomial rings over finite fields. Moreover, we remove the minor term ϵ in our situation. An analogue with ϵ-term of (5) for polynomial ring is established in [4], theorem 8.13.

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the subfield of $\mathbb{F}_q$ with p elements. Let $\psi_p : \mathbb{F}_p \to \mathbb{C}^\times$ be the canonical additive character defined by

$$\psi_p([c]) = \exp\left(\frac{2\pi i \cdot c}{p}\right),$$

where $[c]$ denotes the canonical image of c in $\mathbb{F}_p$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be the additive character defined by $\psi(x) = \psi_p(\mathrm{Tr}(x))$ for all $x \in \mathbb{F}_q$ where Tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Let $\mathbf{A} = \mathbb{F}_q[T]$ (resp. $\mathbf{K} = \mathbb{F}_q(T)$) be the polynomial ring (resp. rational function field) with coefficients in $\mathbb{F}_q$. Let $\mathbf{A}_+$ denote the subset of $\mathbf{A}$ consisting of all monic polynomials. Let $\mathbf{K}_\infty = \mathbb{F}_q(\!(1/T)\!)$ denote the completion of $\mathbf{K}$ at the infinite place, in other words, every $a \in \mathbf{K}_\infty$, if $a \neq 0$, then a can be expressed in the form

$$a = \sum_{i=d}^{-\infty} c_i T^i,$$

where $c_i \in \mathbb{F}_q$ and $c_d \neq 0$. The sign, degree, and absolute value of a are defined by $\operatorname{sgn} a = c_d$, $\deg a = d$, and $|a| = q^d$. The residue of a at the infinite place is denoted by $\operatorname{Res}_\infty a = c_{-1}$. The exponential map $E : \mathbf{K}_\infty \to \mathbb{C}^\times$ is defined by

$$E(a) = \psi(\operatorname{Res}_\infty a).$$

The exponential map E is a non-trivial additive character from $\mathbf{K}_\infty$ to $\mathbb{C}^\times$. Let $Q \in \mathbf{A}_+$ and let

$$f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbf{A}[x]$$

satisfy $1 \leq \deg f = d < p$, and $(a_d, \cdots, a_1, Q) = 1$. Let

$$S(f, Q) = \sum_{a \in \mathbf{A}, \deg a < \deg Q} E\left(\frac{f(a)}{Q}\right),$$

$$W(f, Q) = \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ (a, Q) = 1}} E\left(\frac{f(a)}{Q}\right).$$

In theorem 2.1 and corollary 2.5, we obtain

$$S(f, Q) \ll |Q|^{1 - \frac{1}{d}}, W(f, Q) \ll |Q|^{1 - \frac{1}{d}},$$

where the implied constants depend only on d and q. The first inequality is an analogue of (4).

Let $\mathfrak{M}$ be the subring of $\mathbf{K}_\infty$ consisting of $a \in \mathbf{K}_\infty$ with $\deg a \leq -1$. Let $g(z) \in \mathbf{K}_\infty[z]$ denote a polynomial of degree d with coefficients in $\mathbf{K}_\infty$. The Weyl sum $S(g, N)$ is defined to be

$$S(g, N) = \sum_{b \in \mathbf{A}_+, \deg b = N} E(g(b)).$$

If $g(z) \in \mathbf{A}[z]$ is of degree $d < p$ and such that the coefficients are relatively prime, then in theorem 4.2, we obtain

$$\int_{\mathfrak{M}} |S(\alpha \cdot g, N)|^{2^v} d\alpha \ll q^{N(2^v - v)} N^{C_2}$$

for all $1 \leq v \leq d$. This is an analogue of (5). Moreover, using the Vinogradov's idea (cf. [17]), if $d < p$ and $s = dl$, then in theorem 5.4, we obtain

$$\int_{\mathfrak{M}} |S(\alpha \cdot g, N)|^{2s} d\alpha \ll q^{N(2s - d + \delta)},$$

where $2\delta = d^2(1 - 1/d)^l$.

2. Exponential sums for polynomial rings

Let π_N denote the number of monic irreducible polynomials in $\mathbf{A}$ of degree N. The prime number theorem for $\mathbf{A}$ is given by

$$q^N/N - q^{N/2} < \pi_N < q^N/N. \tag{6}$$

Let f and Q be as in introduction. It is easy to deduce

$$|S(f(x),Q)| = |S(f(x)-a_0,Q)|, |W(f(x),Q)| = |W(f(x)-a_0,Q)|, \tag{7}$$

and if $d=1$, then

$$S(f,Q) = 0. \tag{8}$$

Therefore, if $(Q_1,Q_2)=1$ and $a_0=0$, then we have

$$\begin{aligned} S(f,Q_1Q_2) &= S\left(\frac{f(Q_1x)}{Q_1},Q_2\right) S\left(\frac{f(Q_2x)}{Q_2},Q_1\right), \\ W(f,Q_1Q_2) &= W\left(\frac{f(Q_1x)}{Q_1},Q_2\right) W\left(\frac{f(Q_2x)}{Q_2},Q_1\right). \end{aligned} \tag{9}$$

The object of this section is

Theorem 2.1. *For any monic polynomial $Q \in \mathbf{A}_+$, we have*

$$S(f,Q) \ll |Q|^{1-\frac{1}{d}},$$

where the implied constant depends only on d and q.

Proof. First, we prove this theorem in the case when $Q=P$ is a monic irreducible polynomial in $\mathbf{A}$. Let

$$\begin{aligned} \psi_P : \mathbf{A}/(P) &\to \mathbb{C}^\times, \\ \bar{a} &\mapsto E\left(\frac{a}{P}\right), \end{aligned}$$

where $\bar{a}$ denotes the canonical image of a in $\mathbf{A}/(P)$. Since ψ is a non-trivial additive character, ψ_P is also a nontrivial additive character of the finite field $\mathbf{A}/(P)$. Since $(a_d,\cdots,a_1,P)=1$ and $1 \le d < p$,

$$\bar{f}(x) = \overline{a_d}x^d + \cdots + \overline{a_1}x + \overline{a_0} \in \mathbf{A}/(P)[x]$$

is a non-zero polynomial with $(\deg \bar{f}, p) = 1$. Thus by [16], theorem 2 of Section 1.4, we obtain

$$\sum_{a\in\mathbf{A},\deg a<\deg P} E\left(\frac{f(a)}{P}\right) = \sum_{\bar{a}\in\mathbf{A}/(P)} \psi_P(\bar{f}(\bar{a})) \le (d-1)|P|^{\frac{1}{2}}. \tag{10}$$

Second, we prove this theorem in the case when $Q=P^N (N\ge 2)$ where P is a monic irreducible polynomial in $\mathbf{A}$. Let $f'(x) \equiv (x-r_1)^{m_1}\cdots(x-r_s)^{m_s}g(x) \pmod P$, where $r_i \in \mathbf{A}(\deg r_i < \deg P)$ and $g(x) \pmod P$ has no linear factors. We write

$$S(f,P^N) = \sum_{r\in\mathbf{A},\deg r<\deg P} S_r(f,P^N), \tag{11}$$

where

$$S_r(f,P^N)=\sum_{\substack{a\in\mathbf{A},\deg a<N\deg P\\ a\equiv r \pmod P}} E\left(\frac{f(a)}{P^N}\right).$$

We can write

$$\begin{aligned}S_r(f,P^N)&=\sum_{\substack{b,c\in\mathbf{A},\deg b<(N-1)\deg P,\deg c<\deg P\\ b\equiv r \pmod P}} E\left(\frac{f(b+P^{N-1}c)}{P^N}\right)\\ &=\sum_{\substack{b,c\in\mathbf{A},\deg b<(N-1)\deg P,\deg c<\deg P\\ b\equiv r \pmod P}} E\left(\frac{f(b)+P^{N-1}cf'(b)}{P^N}\right)\\ &=\sum_{\substack{b\in\mathbf{A},\deg b<(N-1)\deg P\\ b\equiv r \pmod P}} E\left(\frac{f(b)}{P^N}\right)\sum_{c\in\mathbf{A},\deg c<\deg P} E\left(\frac{cf'(b)}{P}\right).\end{aligned}$$

If $r\in\mathbf{A}(\deg r<\deg P)$ is not one of the r_i, then by $f'(b)\equiv f'(r)\not\equiv 0 \pmod P$ and (8), we have $S_r(f,P^N)=0$. If $r=r_i$ for some $1\le i\le s$, then

$$S_{r_i}(f,P^N)=E\left(\frac{f(r_i)}{P^N}\right)\sum_{b\in\mathbf{A},\deg b<(N-1)\deg P} E\left(\frac{f(r_i+Pb)-f(r_i)}{P^N}\right).$$

Let σ_i be the greatest integer for which P^{σ_i} divides all the coefficients of the polynomial $f(r_i+Px)-f(r_i)$. Since $1\le\deg f=d<p$ and $(a_d,\cdots,a_1,P)=1$, from lemma 2.3 (2), we have $2\le\sigma_i\le d$. Thus

$$|S_{r_i}(f,P^N)|=\begin{cases}|P|^{\sigma_i-1}|S(g_i,P^{N-\sigma_i})| & \text{if } N>\sigma_i,\\ |P|^{N-1} & \text{if } N\le\sigma_i,\end{cases}\tag{12}$$

where $g_i(x)=P^{-\sigma_i}(f(r_i+Px)-f(r_i))$. Combining these, we obtain

$$|S(f,P^N)|\le\sum_{1\le i\le s,\sigma_i<N}|P|^{\sigma_i-1}|S(g_i,P^{N-\sigma_i})|+\sum_{1\le i\le s,\sigma_i\ge N}|P|^{N-1}.\tag{13}$$

By induction on N. Since $\sigma_i\le d$ and $s\le d$, the first term of the right side of the above inequality is

$$\ll|P|^{\sigma_i(1-1/d)}|P|^{(N-\sigma_i)(1-1/d)}\ll|P|^{N(1-1/d)}.$$

The second term is also

$$\ll|P|^{N(1-1/d)},$$

because $N\le\sigma_i\le d$. Therefore the proof of $Q=P^N$ is completes. In order to deal with the general case, we need

Lemma 2.2. *Let P be a monic irreducible polynomial in $\mathbf{A}$ satisfying*

$$(a_d,\cdots,a_1,P)=1.$$

Then we have

$$|S(f,P^N)| \le \max\left\{1,(d-1)|P|^{1/d-1/2}\right\}|P|^{N(1-1/d)},$$

if $q^{\deg P} \ge 2^d$ *or* $a_d \in \mathbb{F}_q^\times$ *and* $a_i = 0 (1 \le i \le d-1)$.

Proof. We prove this lemma by induction on N. When $N=1$, it follows from (10). Assume this lemma is true for $1, 2, \cdots, N-1$. Let σ_i, g_i, m_i, and s be as above. Then by (12), we have

$$\begin{aligned}
|S(f,P^N)| &\le \sum_{1\le i\le s, \sigma_i<N} |P|^{\sigma_i-1}|S(g_i,P^{N-\sigma_i})| + \sum_{1\le i\le s,\sigma_i\ge N} |P^{N-1}| \\
&\le \max\{1,(d-1)|P|^{1/d-1/2}\}|P|^{(N-1)(1-1/d)} \times \\
&\quad \left(\sum_{1\le i\le s,\sigma_i<N} |P|^{(\sigma_i-1)/d} + \sum_{1\le i\le s,\sigma_i\ge N} |P|^{(N-1)/d}\right) \\
&\le \max\left\{1,(d-1)|P|^{1/d-1/2}\right\}|P|^{(N-1)(1-1/d)} \sum_{i=1}^{s} |P|^{(\sigma_i-1)/d}.
\end{aligned}$$

By lemma 2.3, $1 \le \sigma_i - 1 \le m_i$. Thus

$$\sum_{i=1}^{s}(\sigma_i-1) \le \sum_{i=1}^{s} m_i \le d-1.$$

If $q^{\deg P} \ge 2^d$, then $|P|^{1/d} \ge q^{\deg P/d} \ge 2, \sigma_i - 1 \ge 1$, and we get

$$\sum_{i=1}^{s} |P|^{(\sigma_i-1)/d} \le |P|^{\sum_{i=1}^{s}(\sigma_i-1)/d} \le |P|^{(d-1)/d} = |P|^{1-\frac{1}{d}}.$$

If $a_d \in \mathbb{F}_q^\times$ and $a_i = 0 (1 \le i \le d-1)$, then $s=1, \sigma_1 = d$, and we get

$$|P|^{(d-1)/d} = |P|^{1-1/d}.$$

Combining these, the proof of the lemma is complete. □

Now go back to the proof of theorem 2.1. By (7), we may assume that $a_0 = 0$. Let $Q = P_1^{n_1}P_2^{n_2}\cdots P_l^{n_l}$ be a monic polynomial in $\mathbf{A}$, where $P_1, P_2, \cdots, P_l$

are all the distinct irreducible factors of Q. By (9) , we have

$$S(f,Q)=\prod_{i=1}^{l} S\left(\frac{f(Qx/P_i^{n_i})}{Q/P_i^{n_i}},P_i^{n_i}\right)$$

by lemma 2.2 and (6),

$$\begin{aligned}&\ll\left(\prod_{\deg P_i\geq d}\max\left\{1,(d-1)|P_i|^{1/d-1/2}\right\}\right)\prod_{i=1}^{l}|P_i|^{n_i(1-1/d)}\\&\ll|Q|^{1-1/d},\end{aligned}$$

where the implied constant depends only on d and q. □

Lemma 2.3. *Let $f(x)=a_dx^d+\cdots+a_1x+a_0\in\mathbf{A}[x]$ be a polynomial of degree d with $1\leq d<p$. Then for any monic irreducible polynomial P with $(a_d,\cdots,a_1,P)=1$, we have*

(a) *If $r\in\mathbf{A},r\pmod P$ is a root of multiplicity m of $f(x)\equiv 0\pmod P$ and σ is the greatest integer for which P^σ divides all the coefficients of the polynomial $f(Px+r)$ in x, then $1\leq\sigma\leq m$.*

(b) *If $r\in\mathbf{A},r\pmod P$ is a root of multiplicity m of $f'(x)\equiv 0\pmod P$ and σ is the greatest integer for which P^σ divides all the coefficients of the polynomial $f(Px+r)-f(r)$ in x, then $1\leq\sigma-1\leq m$.*

Proof. To prove (a), we can write

$$f(x)=(x-r)^mf_1(x)+Pf_2(x),$$

where $P\nmid f_1(r)$ and $\deg f_2(x)<m$. Then $f(Px+r)=P^mf_1(Px+r)x^m+Pf_2(Px+r)$. Since $f_1(Px+r)\equiv f_1(r)\pmod P$ and $P\nmid f_1(r)$, we have $1\leq\sigma\leq m$.

To prove (b), let $f_3(x)=f(Px+r)-f(r)$. Since $d<p$, σ is also the greater integer for which P^σ divides all the coefficients of the polynomial $f_3'(x)=Pf'(Px+r)$ in x. Thus $\sigma-1$ is the greatest integer for which $P^{\sigma-1}$ divides all the coefficients of the polynomial $f'(Px+r)$ in x. By (a), we obtain that $1\leq\sigma-1\leq m$. □

Corollary 2.4. *Let f,Q be as before. If $\deg Q>N$, then we have*

$$\sum_{a\in\mathbf{A}_+,\deg a=N}E\left(\frac{f(a)}{Q}\right)\ll q^{D/d}|Q|^{1-\frac{1}{d}},$$

where the implied constant depends only on d and q.

Proof. Let

$$N(a)=\begin{cases}1 & \text{if } a\in\mathbf{A}_+ \text{ and } \deg a=N,\\ 0 & \text{otherwise.}\end{cases}$$

Then for each $a \in \mathbf{A}_+$ satisfying $\deg a < \deg Q$, we have

$$N(a) = |Q|^{-1} \sum_{r \in \mathbf{A}, \deg r < \deg Q} E\left(\frac{ar}{Q}\right) \sum_{b \in \mathbf{A}_+, \deg b = N} E\left(\frac{-rb}{Q}\right).$$

Thus, we get

$$\begin{aligned}
&\sum_{a \in \mathbf{A}_+, \deg a = N} E\left(\frac{f(a)}{Q}\right) \\
&= \sum_{a \in \mathbf{A}, \deg a < \deg Q} E\left(\frac{f(a)}{Q}\right) N(a) \\
&= |Q|^{-1} \sum_{a \in \mathbf{A}, \deg a < \deg Q} E\left(\frac{f(a)}{Q}\right) \times \\
&\qquad \sum_{r \in \mathbf{A}, \deg r < \deg Q} E\left(\frac{ar}{Q}\right) \sum_{b \in \mathbf{A}_+, \deg b = N} E\left(\frac{-rb}{Q}\right) \\
&= |Q|^{-1} \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ r \in \mathbf{A}, \deg r < \deg Q}} E\left(\frac{f(a) + ar}{Q}\right) \sum_{b \in \mathbf{A}_+, \deg b = N} E\left(\frac{-rb}{Q}\right).
\end{aligned}$$

If $\deg r < \deg Q - N$, then

$$\sum_{b \in \mathbf{A}_+, \deg b = N} E\left(\frac{-rb}{Q}\right) = q^N E\left(\frac{-rT^N}{Q}\right).$$

If $\deg r \geq \deg Q - N$, then

$$\sum_{b \in \mathbf{A}_+, \deg b = N} E\left(\frac{-rb}{Q}\right) = 0.$$

This implies

$$\begin{aligned}
&\sum_{a \in \mathbf{A}_+, \deg a = N} E\left(\frac{f(a)}{Q}\right) \\
&\quad \leq q^{N - \deg Q} \sum_{r \in \mathbf{A}, \deg r < \deg Q - N} \Big| \sum_{a \in \mathbf{A}, \deg a < \deg Q} E\left(\frac{f(a) + ar}{Q}\right) \Big| \\
&\text{let } (a_d, \cdots, a_2, a_1 + r, Q) = Q_r \\
&\quad = q^{N - \deg Q} \sum_{r \in \mathbf{A}, \deg r < \deg Q - N} \Big| \sum_{a \in \mathbf{A}, \deg a < \deg Q} E\left(\frac{(f(a) + ar)/Q_r}{Q/Q_r}\right) \Big|
\end{aligned}$$

by theorem 2.1

$$\ll q^{N-\deg Q} \sum_{r\in\mathbf{A},\deg r<\deg Q-N} |Q_r|\cdot\big|\frac{Q}{Q_r}\big|^{1-1/d}$$

by $\deg Q_r \le D$

$$\ll q^{N-\deg Q} \sum_{r\in\mathbf{A},\deg r<\deg Q-N} q^{D/d}|Q|^{1-1/d}$$
$$\ll q^{D/d}|Q|^{1-1/d}.$$

□

Corollary 2.5. *Let f, Q be as above. Then we have*

$$W(f,Q) \ll |Q|^{1-\frac{1}{d}},$$

where the implied constant depends only on d and q.

Proof. By (7), we may assume that $a_0 = 0$. First, we prove this theorem in the case when $Q = P^N (N \ge 1)$, where P is a monic irreducible polynomial in $\mathbf{A}$. By (11), we have

$$W(f,P^N) = -S_0(f,P^N) + \sum_{r\in\mathbf{A},\deg r<\deg P} S_r(f,P^N).$$

Hence

$$\big|W(f,P^N)\big| \le \sum_{r\in\mathbf{A},\deg r<\deg P} \big|S_r(f,P^N)\big|. \tag{14}$$

If $N = 1$, then by (10), we have

$$W(f,P) \le d|P|^{\frac{1}{2}}. \tag{15}$$

If $N \ge 2$, then by (14) and (12), we have

$$W(f,P^N) \ll |P|^{N(1-1/d)}.$$

With (15) at hand, a slight modified proof of lemma 2.2, we obtain that

$$|W(f,P^N)| \le \max\big\{1, d|P|^{1/d-1/2}\big\}|P|^{N(1-1/d)}, \tag{16}$$

if $q^{\deg P} \ge 2^d$ or $a_d \in \mathbb{F}_q^\times$ and $a_i = 0 (1 \le i \le d-1)$. Now let $Q = P_1^{n_1}P_2^{n_2}\cdots P_l^{n_l}$ be a monic polynomial in $\mathbf{A}$, where $P_1, P_2, \cdots, P_l$ are all the

distinct irreducible factors of Q. By (9), we have

$$W(f,Q)=\prod_{i=1}^{l}W\left(\frac{f(Qx/P_i^{n_i})}{Q/P_i^{n_i}},P_i^{n_i}\right)$$

by (16) and (6),

$$\begin{aligned}&\ll\left(\prod_{\deg P_i\geq d}\max\left\{1,d|P_i|^{1/d-1/2}\right\}\right)|P_1|^{n_1(1-1/d)}\cdots|P_l|^{n_l(1-1/d)}\\&\ll|Q|^{1-\frac{1}{d}},\end{aligned}$$

where the implied constant depends only on d and q. □

3. An estimation for sum involving the divisor function

Let $\tau_l(a)$ denote the number of solutions of $\mathrm{sgn}(a)^{-1}a=a_1a_2\cdots a_{l+1}$ with $a_i\in\mathbf{A}_+$ if $0\neq a\in\mathbf{A}$. For any monic irreducible polynomial P, let $\chi(P,i)\geq 0$ for all integer $i\geq 0$. Let function $G_N:\mathbf{A}\to\mathbb{R}$ satisfy $G_N(a)\geq 0$ for all $a\in\mathbf{A}$ and positive integer N. Let sequences $<R_N>$ and $<X_N>$ satisfy $R_N\geq 0, X_N\geq 0$ for all positive integer N. Then fix functions G_N,χ, and sequences $<R_N>,<X_N>$, we have

Lemma 3.1. *Suppose that there exist positive real numbers r,C, and positive integer l such that*

$$\sum_{a\in\mathbf{A},\deg a\leq X_N}G_N(a)\leq R_N,\qquad\sum_{\substack{a\in\mathbf{A},\deg a\leq X_N\\V|a}}G_N(a)\leq R_N\prod_{P|V}\frac{\chi(P,i_P(V))}{|P|},$$

for all $N\in\mathbb{N}$ and $V\in\mathbf{A}_+$ with $\deg V\leq rX_N$, where $i_P(V)$ denotes the greatest integer for which $P^{i_P(V)}|V$; also such that

$$\sum_{i=1}^{\infty}(i+1)^{(1+2/r)l}\chi(P,i)\leq C,$$

for all monic irreducible polynomials P. Then as N goes to ∞, we have

$$\sum_{a\in\mathbf{A},\deg a\leq X_N}\tau_l(a)G_N(a)\ll R_N\max\{X_N^C,1\},$$

where the implied constant depends only on r,C, and l.

Proof. It is convenient to let $G=G_N,R=R_N$, and $X=X_N$. Given X, write any $a\in\mathbf{A}(\deg a\leq X)$ as $a=P_1P_2\cdots P_mV$ where P_i run through all monic irreducible factors of a of degree $>rX$. Let $V_1\in\mathbf{A}_+$ denote a factor of V such that $\deg V_1\leq rX$ and $\deg V_1\geq\deg D$ for all $D|V$ with $\deg D\leq rX$, let $V_2\in\mathbf{A}_+$ denote a factor of V/V_1 such that $\deg V_2\leq$

rX and $\deg V_2 \geq \deg D$ for all $D|(V/V_1)$ with $\deg D \leq rX$, and so forth. Suppose that this process ends at the n-th step. Then V can be expressed as $\mathrm{sgn}(V)V_1 \cdots V_n$. The n is called the index of a, and $V_1, \cdots, V_n$ will be called the characteristic factors of a. Since $\deg a \leq X$ and $\deg V_{n-1} \geq rX/2$, we have

$$m < 1/r, n - 1 \leq 2/r,$$

and

$$\tau_1(a) \leq 2^m \tau_1(V_1) \cdots \tau_1(V_n) \leq 2^{\frac{1}{r}} \tau_1(V_1) \cdots \tau_1(V_n).$$

This implies that

$$\tau_l(a) \leq \begin{cases} 2^{\frac{l}{r}} & \text{if } n = 0, \\ 2^{\frac{l}{r}} \sum_{j=1}^{n} \tau_1(V_j)^{ln} & \text{if } n \geq 1. \end{cases}$$

Write

$$\sum_{a \in \mathbf{A}, \deg a \leq X} \tau_l(a) G(a) = \sum_{0 \leq n \leq 1+2/r} U_n,$$

where U_n denotes the part of this sum which are taken over a with index n. If $n = 0$, then we have

$$U_0 \leq 2^{\frac{l}{r}} \sum_{a \in \mathbf{A}, \deg a \leq X} G(a) \leq 2^{\frac{l}{r}} R.$$

If $1 \leq n \leq 1 + 2/r$, then

$$U_n \leq 2^{\frac{l}{r}} \sum_{i=1}^{n} U_{n,i},$$

in which

$$U_{n,i} = \sum_{V \in \mathbf{A}_+, 1 \leq \deg V \leq rX} \tau_1(V)^{ln} \sum_{\substack{a \in \mathbf{A}, \deg a \leq X \\ V|a}}^{**} G(a),$$

where the double asterisks means summation over a with index n that have V as their i-th characteristic factor. Therefore, if $V = P_1^{d_1} P_2^{d_2} \cdots P_s^{d_s}$, where P_j are distinct monic irreducible polynomials, then

$$\sum_{\substack{a \in \mathbf{A}, \deg a \leq X \\ V|a}}^{**} G(a) \leq \sum_{\substack{a \in \mathbf{A}, \deg a \leq X \\ V|a}} G(a) \leq R \prod_{j=1}^{s} \frac{\chi(P_j, d_j)}{|P_j|}.$$

Since $\tau_1(V) = (d_1+1)(d_2+1)\cdots(d_s+1)$, we obtain

$$\begin{aligned} U_{n,i} &\le R \sum_{V\in\mathbf{A}_+, 1\le \deg V\le rX} \prod_{j=1}^{s} \frac{(d_j+1)^{ln}\chi(P_j,d_j)}{|P_j|} \\ &\le R \prod_{\substack{P \text{ monic irreducible} \\ \deg P\le rX}} \left(1+\sum_{i=1}^{\infty}\frac{(i+1)^{ln}\chi(P,i)}{|P|}\right) \end{aligned}$$

by $n \le 1+2/r$

$$\le R \prod_{\substack{P \text{ monic irreducible} \\ \deg P\le rX}} \left(1+\frac{C}{|P|}\right)$$

$$\le R\cdot\exp\left(C \sum_{\substack{P \text{ monic irreducible} \\ \deg P\le rX}} |P|^{-1}\right)$$

by (6)

$$\ll R\max\{\exp(C\ln(rX)),1\} \ll R\max\{X^C,1\}.$$

Combining these, we complete the proof. □

Lemma 3.2. *Let $f(x_1,x_2,\cdots,x_n)$ be a polynomial of degree d with coefficients in $\mathbf{A}$. Further, give a monic irreducible polynomial P such that not all the coefficients of f are multiples of P. Then the number of solutions of the congruence*

$$f(x_1,x_2,\cdots,x_n)\equiv 0 \pmod{P^m}$$

with $x_i\in\mathbf{A}, \deg x_i < \deg P^m$ is

$$\ll \min\{|P|^{mn-1}, (m+1)^{n-1}|P|^{mn-m/d}\},$$

where the implied constant depends only on n, d, and q.

Proof. The proofs are slightly modified of the classical cases. The proofs of the classical cases may see [11], lemmas 2.2 and 2.3. □

Theorem 3.3. *Let $f(x_1,x_2,\cdots,x_n)$ be a polynomial of degree d with coefficients in $\mathbf{A}$ such that the coefficients are relatively prime. Then*

$$\sum_{\substack{a_1,\cdots,a_n\in\mathbf{A}_+, \deg a_i=N \\ f(a_1,\cdots,a_n)\neq 0}} \tau_l(f(a_1,\cdots,a_n)) \ll \max\left\{q^{Nn}, q^{\frac{nX_N}{d}}\right\} X_N^{C_1},$$

where the implied constant and C_1 depend only on d,n,l,q, and X_N is the maximum degree of $f(a_1,\cdots,a_n)$ with $a_i\in\mathbf{A}_+, \deg a_i = N$.

Proof. Let $G_N(a)$ be the solutions of $f(x_1, \cdots, x_n) = a$ with $x_i \in \mathbf{A}_+, \deg x_i = N$, and let $R_N = \max\{q^{Nn}, q^{\frac{nX_N}{d}}\}$. Then we have

$$\sum_{\substack{a_1,\cdots,a_n \in \mathbf{A}_+, \deg a_i = N \\ f(a_1,\cdots,a_n)\neq 0}} \tau_l(f(a_1, \cdots, a_n)) = \sum_{a\in\mathbf{A}, \deg a \le X_N} \tau_l(a) G_N(a).$$

Let $r = 1/d$ and for any monic irreducible polynomial P, let

$$\chi(P, i) = \begin{cases} 1 & \text{if } i \le d, \\ (i+1)^{n-1}|P|^{1-\frac{i}{d}} & \text{if } i > d. \end{cases}$$

Then we have

$$\sum_{a\in\mathbf{A}, \deg a \le X_N} G_N(a) = \sum_{a_1,\cdots,a_n\in\mathbf{A}_+, \deg a_i = N} 1 = q^{Nn} \le R_N,$$
$$\sum_{\substack{a\in\mathbf{A}, \deg a \le X_N \\ V|a}} G_N(a) \le \max\{q^{(N-\deg V)n}, 1\} M,$$

where M is the number of solutions of $f(x_1, \cdots, x_n) \equiv 0 \pmod V$ with $x_i \in \mathbf{A}, \deg x_i < \deg V$. By Chinese Remainder theorem for $\mathbf{A}$, M is the product of the number of the solutions of $f(x_1, \cdots, x_n) \equiv 0 \pmod{P^{i_P(V)}}$ with $x_i \in \mathbf{A}, \deg x_i < \deg P^{i_P(V)}$ for all monic irreducible factors P of V. By lemma 3.2, we get

$$M \ll \prod_{P|V} |P|^{n\cdot i_P(V)} \frac{\chi(P, i_P(V))}{|P|}.$$

If $\deg V \le rX_N$, then combining these, we have

$$\sum_{\substack{a\in\mathbf{A}, \deg a \le X_N \\ V|a}} G_N(a) \ll R_N \prod_{P|V} \frac{\chi(P, i_P(V))}{|P|}.$$

Since $r = 1/d$, we get

$$\sum_{i=1}^{\infty} (i+1)^{(1+\frac{2}{r})l} \chi(P, i) = \sum_{i\le d} (i+1)^{(1+2d)l} + \sum_{i>d} (i+1)^{(1+2d)l+n-1} |P|^{1-\frac{i}{d}}$$
$$= O(1).$$

Therefore, by lemma 3.1, our theorem is proved. □

4. Hua's lemma for $\mathbb{F}_q[T]$

Let $\mathfrak{M}$ be the subring of $\mathbf{K}_\infty$ consisting of $a \in \mathbf{K}_\infty$ with $\deg a \leq -1$. The Haar integral for $\mathbf{K}_\infty$ is defined to be

$$\int_{\mathfrak{M}} 1\, da = 1.$$

Throughout this section, let d be a positive integer such that $1 \leq d < p$ (p the characteristic of $\mathbf{A}$), let $g(z) \in \mathbf{K}_\infty[z]$ denote a polynomial of degree d with coefficients in $\mathbf{K}_\infty$ and let D be the maximal degree of the coefficients of g. The Weyl sum $S(g, N)$ is defined to be

$$S(g, N) = \sum_{b \in \mathbf{A}_+, \deg b = N} E(g(b)).$$

If $c \in \mathbf{A}$, we define the difference operator $\Delta_c g(z) \in \mathbf{K}_\infty[z]$ by

$$\Delta_c g(z) = g(z + c) - g(z).$$

If $a_1, a_2, \cdots, a_v \in \mathbf{A}$, we define the iterated difference operator $\Delta_{a_v, a_{v-1}, \cdots, a_1}$ by

$$\Delta_{a_v, a_{v-1}, \cdots, a_1} = \Delta_{a_v} \circ \Delta_{a_{v-1}} \circ \cdots \circ \Delta_{a_1}$$

for the composite operator.

Lemma 4.1. *We have*

$$\left|S(g, N)\right|^{2^v} \leq q^{N(2^v - v - 1)} \sum_{\substack{a_1, a_2, \cdots, a_v \in \mathbf{A} \\ \deg a_i < N}} S(\Delta_{a_v, a_{v-1}, \cdots, a_1} g, N) \tag{17}$$

for all $1 \leq v \leq d$.

Proof. We prove this lemma by induction on v. If $v = 1$, then

$$\begin{aligned} |S(g, N)|^2 &= \sum_{a_1, a_2 \in \mathbf{A}, \deg a_i < N} E(g(T^N + a_1) - g(T^N + a_2)) \\ &= \sum_{\deg a_1 < N} \sum_{\deg a_2 < N} E(g(T^N + a_2 + a_1) - g(T^N + a_2)) \\ &= \sum_{\deg a_1 < N} \sum_{\deg a_2 < N} E(\Delta_{a_1} g(T^N + a_2)) \\ &= \sum_{\deg a_1 < N} S(\Delta_{a_1} g, N) \end{aligned}$$

as desired. Let us assume that (17) holds for some $1 \leq v < d$. We square both sides and apply Cauchy's inequality on the right, using the fact that there are q^N polynomials of degree less than N and also using the result

just proved for $v = 1$. We obtain

$$\begin{aligned}\left|S(g,N)\right|^{2^{v+1}} &\le q^{N(2^{v+1}-2v-2)} \left(\sum_{\substack{a_1,a_2,\cdots,a_v \in \mathbf{A} \\ \deg a_i < N}} S(\Delta_{a_v,a_{v-1},\cdots,a_1} g, N) \right)^2 \\ &\le q^{N(2^{v+1}-2v-2)} q^{Nv} \sum_{\substack{a_1,a_2,\cdots,a_v \in \mathbf{A} \\ \deg a_i < N}} |S(\Delta_{a_v,a_{v-1},\cdots,a_1} g, N)|^2 \\ &= q^{N(2^{v+1}-(v+1)-1)} \sum_{\substack{a_1,a_2,\cdots,a_{v+1} \in \mathbf{A} \\ \deg a_i < N}} S(\Delta_{a_{v+1},a_v,\cdots,a_1} g, N).\end{aligned}$$

This completes the proof. □

Theorem 4.2 (Hua's lemma). *Let $g(z)$ denote a polynomial of degree $d < p$ with coefficients in $\mathbf{A}$ such that the coefficients are relatively prime. Then when $1 \le v \le d$, we have*

$$\int_{\mathfrak{M}} |S(\alpha \cdot g, N)|^{2^v} d\alpha \ll q^{N(2^v - v)} N^{C_2}, \tag{18}$$

where the implied constant depends on D, v, d, and q, C_2 depends on v, d, and q. In other words, the number of solutions of

$$g(x_1) + \cdots + g(x_{2^{v-1}}) = g(y_1) + \cdots + g(y_{2^{v-1}})$$

with $x_i, y_i \in \mathbf{A}_+$ and $\deg x_i = \deg y_i = N$ is $\ll q^{N(2^v - v)} N^{C_2}$.

Proof. We prove this lemma by induction on v. If $v = 1$, then the integral

$$\int_{\mathfrak{M}} |S(\alpha \cdot g, N)|^2 d\alpha$$

is the number of (b_1, b_2) with $b_1, b_2 \in \mathbf{A}_+, \deg b_1 = \deg b_2 = N$, and $g(b_1) = g(b_2)$. Fix a b_2. Since $\deg g = d$, the number of solutions of $g(b_1) = g(b_2)$ is less than d. Thus the theorem is obvious when $v = 1$. Let us assume that (18) holds for some $1 \le v < d$. By lemma 4.1

$$\begin{aligned}|S(\alpha \cdot g, N)|^{2^v} &\le q^{N(2^v - v - 1)} \sum_{\substack{a_1,\cdots,a_v \in \mathbf{A} \\ \deg a_i < N}} S(\Delta_{a_v,\cdots,a_1} \alpha \cdot g, N) \\ &= q^{N(2^v - v - 1)} \sum_{\substack{a_1,\cdots,a_v \in \mathbf{A}, z \in \mathbf{A}_+ \\ \deg a_i < N, \deg z = N}} E(\alpha \Delta_{a_v,\cdots,a_1} g(z)).\end{aligned}$$

If $a_1 a_2 \cdots a_v = 0$, then $\Delta_{a_v,\cdots,a_1} g(z)$ is a zero polynomial in z. If $a_1 a_2 \cdots a_v \ne 0$, then since $\Delta_{a_v,\cdots,a_1} g(z)$ is a polynomial of degree $d - v$, the number of solutions of $\Delta_{a_v,\cdots,a_1} g(z) = 0$ is less than $d - v$. Thus if $\alpha \ne 0$, then we have

$$|S(\alpha \cdot g, N)|^{2^v} \ll q^{N(2^v - 1)} + q^{N(2^v - v - 1)} \sum_{\substack{a_1,\cdots,a_v \in \mathbf{A}, z \in \mathbf{A}_+ \\ \deg a_i < N, \deg z = N}}^{*} E(\alpha \Delta_{a_v,\cdots,a_1} g(z)),$$

where the asterisk means that $\Delta_{a_v,\cdots,a_1}g(z) \neq 0$. Multiplying both sides of the above inequality by $|S(\alpha\cdot g,N)|^{2^v}$ and integrating with $\alpha\in\mathfrak{M}$, we obtain

$$\begin{aligned}\int_{\mathfrak{M}}|S(\alpha\cdot g,N)|^{2^{v+1}}d\alpha &\ll q^{N(2^v-1)}\int_{\mathfrak{M}}|S(\alpha\cdot g,N)|^{2^v}d\alpha\\ &+q^{N(2^v-v-1)}\int_{\mathfrak{M}}\sum_{\substack{a_1,\cdots,a_v\in\mathbf{A},z\in\mathbf{A}_+\\ \deg a_i<N,\deg z=N}}^{*}E(\alpha\Delta_{a_v,\cdots,a_1}g(z))|S(\alpha\cdot g,N)|^{2^v}d\alpha.\end{aligned}$$

By the induction hypothesis we know that the first term of the right side of the above inequality is

$$\ll q^{N(2^{v+1}-(v+1))}N^{C_2}.$$

The second term of the right side of the above inequality is equal to

$$\begin{aligned}&q^{N(2^v-v-1)}\int_{\mathfrak{M}}\sum_{\substack{a_1,\cdots,a_v\in\mathbf{A},z\in\mathbf{A}_+\\ \deg a_i<N,\deg z=N}}^{*}\sum_{\substack{z_1,\cdots,z_{2^v}\in\mathbf{A}_+\\ \deg z_i=N}}E\Big(\alpha\big(\Delta_{a_v,\cdots,a_1}g(z)\\ &\qquad\qquad+\sum_{i=1}^{2^{v-1}}-g(z_i)+g(z_{2^{v-1}+i})\big)\Big)d\alpha\\ &=q^{N(2^v-v-1)}Y,\end{aligned}$$

where Y is the number of solution of the system

$$\begin{cases}\Delta_{a_v,\cdots,a_1}g(z)=\displaystyle\sum_{i=1}^{2^{v-1}}g(z_i)-g(z_{2^{v-1}+i}),\\ \Delta_{a_v,\cdots,a_1}g(z)\neq 0,\\ a_i\in\mathbf{A},z,z_j\in\mathbf{A}_+,\deg a_i<N,\deg z=\deg z_j=N.\end{cases}\tag{19}$$

Since $\Delta_{a_v,\cdots,a_1}g(z)$ is a polynomial of degree $d-v\geq 1$ in z and each coefficient of this polynomial is divided by $a_1a_2\cdots a_v$, for given $z_1,\cdots,z_{2^v}$ satisfying

$$\sum_{i=1}^{2^{v-1}}g(z_i)-g(z_{2^{v-1}+i})\neq 0,\tag{20}$$

the number of solutions of (19) is

$$\ll\tau_v\left(\sum_{i=1}^{2^{v-1}}g(z_i)-g(z_{2^{v-1}+i})\right).$$

By theorem 3.3, we obtain

$$\begin{aligned} Y &\ll \sum_{z_i\in\mathbf{A}_+,\deg z_i=N}^{+} \tau_v\left(\sum_{i=1}^{2^{v-1}} g(z_i)-g(z_{2^{v-1}+i})\right)\\ &\ll q^{(N+D/d)2^v}N^{C_1}\\ &\ll q^{N2^v}N^{C_1}, \end{aligned}$$

where the plus means that the z_i satisfy (20). This completes the proof. □

5. VINOGRADOV'S MEAN VALUE THEOREM FOR $\mathbb{F}_q[T]$

For any d-tuple $\alpha=(\alpha_1,\cdots,\alpha_d)$ with $\alpha_i\in\mathfrak{M}$, let

$$C_N(\alpha)=\sum_{z\in\mathbf{A}_+,\deg z=N} E(\alpha_d z^d+\cdots+\alpha_1 z),$$

and let

$$J_s(N)=\int_{\mathfrak{M}}\cdots\int_{\mathfrak{M}}\left|C_N(\alpha)\right|^{2s}d\alpha_1\cdots d\alpha_d. \tag{21}$$

The value of the above integral is equal to the number of solutions of the equations

$$\sum_{i=1}^{s}(z_i^j-z_{s+i}^j)=0 \qquad (1\le j\le d) \tag{22}$$

with $z_1,\cdots,z_{2s}\in\mathbf{A}_+$ and $\deg z_i=N(1\le i\le 2s)$. Given any $a_1,\cdots,a_d\in\mathbf{A}$. Since the integral

$$\int_{\mathfrak{M}}\cdots\int_{\mathfrak{M}}\left|C_N(\alpha)\right|^{2s}E(-(\alpha_d a_d+\cdots+\alpha_1 a_1))d\alpha_1\cdots d\alpha_d$$

is equal to the number of solutions of the equations

$$\sum_{i=1}^{s}(z_i^j-z_{s+i}^j)=a_j \qquad (1\le j\le d) \tag{23}$$

with $z_1,\cdots,z_{2s}\in\mathbf{A}_+$, $\deg z_i=N(1\le i\le 2s)$, and

$$\begin{aligned} &\int_{\mathfrak{M}}\cdots\int_{\mathfrak{M}}\left|C_N(\alpha)\right|^{2s}E(-(\alpha_d a_d+\cdots+\alpha_1 a_1))d\alpha_1\cdots d\alpha_d\\ &\le\int_{\mathfrak{M}}\cdots\int_{\mathfrak{M}}\left|C_N(\alpha)\right|^{2s}d\alpha_1\cdots d\alpha_d, \end{aligned}$$

so the number of solutions of (23) is $\le J_s(N)$.

Let P be a monic irreducible polynomial in $\mathbf{A}$. Given any fixed d-tuple $g = (g_1, \cdots, g_d)$ with $g_i \in \mathbf{A}$. Let $X(P, g)$ denote the number of solutions of the congruences

$$\sum_{i=1}^{d} z_i^j \equiv g_j \pmod{P^d} \qquad (1 \le j \le d) \tag{24}$$

with $z_i \in \mathbf{A}, \deg z_i < d \cdot \deg P$, and $z_1, \cdots, z_d$ distinct modulo P. Then we have

Lemma 5.1. *If $d < p$, then*

$$X(P, g) \le d!.$$

Proof. Let $y_1, \cdots, y_d$ be another solution of (24). We have

$$\sum_{i=1}^{d} y_i^j \equiv \sum_{i=1}^{d} z_i^j \pmod{P^d} \qquad (1 \le j \le d).$$

Let σ_j and σ_j' denote the elementary symmetric functions of j-th degree of $y_1, \cdots, y_d$ and $z_1, \cdots, z_d$ respectively. Let

$$S_j = \sum_{i=1}^{d} y_i^j, \qquad S_j' = \sum_{i=1}^{d} z_i^j.$$

We have

$$S_j - \sigma_1 S_{j-1} + \sigma_2 S_{j-2} + \cdots + (-1)^j \cdot j \cdot \sigma_j = 0,$$
$$S_j' - \sigma_1' S_{j-1}' + \sigma_2' S_{j-2}' + \cdots + (-1)^j \cdot j \cdot \sigma_j' = 0,$$

for all $1 \le j \le d$. Since $j \le d < p$, and $S_j \equiv S_j' \pmod{P^d}$ for all $1 \le j \le d$, we get

$$\sigma_j \equiv \sigma_j' \pmod{P^d},$$

for all $1 \le j \le d$. Therefore

$$(x - y_1) \cdots (x - y_d) \equiv (x - z_1) \cdots (x - z_d) \pmod{P^d}.$$

Since $\deg y_i < d \cdot \deg P$, $\deg z_i < d \cdot \deg P$, and the z_i are distinct modulo P, the $y_1, \cdots y_d$ are a permutation of the $z_1, \cdots z_d$. Hence

$$X(P, g) \le d!.$$

□

Let $X_1(P, g)$ denote the number of solutions of the congruences

$$\sum_{i=1}^{d} z_i^j \equiv g_j \pmod{P^j} \qquad (1 \le j \le d)$$

with $z_i \in \mathbf{A}$, $\deg z_i < d \cdot \deg P$, and z_i distinct modulo P.

Lemma 5.2. *If $d < p$, then we have*

$$X_1(P, g) \le d! \cdot |P|^{\frac{d(d-1)}{2}}.$$

Proof. We have

$$X_1(P,g) = \sum_{\substack{w_1\in\mathbf{A},\deg w_1<d\cdot\deg P\\ w_1\equiv g_1 \pmod{P^1}}} \cdots \sum_{\substack{w_d\in\mathbf{A},\deg w_d<d\cdot\deg P\\ w_d\equiv g_d \pmod{P^d}}} X(P,w),$$

where $w = (w_1,\cdots,w_d)$. Since $X(P,w) \le d!$ and the total number of possible choices for w is equal to

$$|P|^{(d-1)+\cdots+1+0} = |P|^{\frac{d(d-1)}{2}},$$

we have

$$X_1(P,g) \le d!\cdot|P|^{\frac{d(d-1)}{2}}.$$

□

The main result of this section is

Theorem 5.3. *Let $d < p$, l be positive integers and let $s = d\cdot l$. Then*

$$J_s(N) \ll (q^N)^{2s-\frac{d(d+1)}{2}+\delta},$$

where $2\delta = d^2(1-1/d)^l$ and the implied constant depends only on d, l, and q.

Proof. The case when $d = 1$ is obvious. Thus assume $d \ge 2$ and we prove this theorem by induction on l. When $l = 1$, i.e., $s = d$. Let $z_1,\cdots,z_{2d}$ be a solution of (22). Let P be any monic irreducible polynomial in $\mathbf{A}$ with $\deg P > N$. As in the proof of lemma 5.1, we have

$$(x-z_{d+1})\cdots(x-z_{2d}) \equiv (x-z_1)\cdots(x-z_d) \pmod{P}.$$

Since $\deg z_i < \deg P$, the $z_{d+1},\cdots,z_{2d}$ are a permutation of the $z_1,\cdots,z_d$. Thus

$$J_d(N) \le d!q^{N\cdot d}.$$

This gives the case $l = 1$ at once.

Now suppose this theorem holds for $l-1$. For any d-tuple $g = (g_1,\cdots,g_d)$ with $g_j \in \mathbf{A}$, $\deg g_j \le j\cdot N$, let $R_1(g)$ denote the number of solutions of the equations

$$\sum_{i=1}^{s} z_i^j = g_j \qquad (1 \le j \le d)$$

with $z_i \in \mathbf{A}_+$, $\deg z_i = N (1 \le i \le s)$, and $z_1,\cdots,z_d$ distinct. Let $R_2(g)$ denote the corresponding number with at most $d-1$ of the $z_1,\cdots,z_d$ distinct. Then we have

$$\begin{aligned} J_s(N) &= \sum_{g_1\in\mathbf{A},\deg g_1\le 1\cdot N} \cdots \sum_{g_d\in\mathbf{A},\deg g_d\le d\cdot N} (R_1(g)+R_2(g))^2 \\ &\le 2 \sum_{g_1\in\mathbf{A},\deg g_1\le 1\cdot N} \cdots \sum_{g_d\in\mathbf{A},\deg g_d\le d\cdot N} \left(R_1(g)^2+R_2(g)^2\right). \end{aligned}$$

Hence

$$J_s(N) \le 2I_1 + 2I_2,$$

where

$$I_i = \sum_{g_1 \in \mathbf{A}, \deg g_1 \le 1\cdot N} \cdots \sum_{g_d \in \mathbf{A}, \deg g_d \le d\cdot N} R_i(g)^2.$$

To estimate I_2, let $f(z) = \alpha_d z^d + \cdots + \alpha_1 z$, $\alpha = (\alpha_1, \cdots, \alpha_d)$, and $\beta = (2\alpha_1, \cdots, 2\alpha_d)$. We have

$$\begin{aligned} I_2 &\le \binom{d}{2}^2 \int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \sum_{\substack{z_1, \cdots, z_{2s} \in \mathbf{A}_+, \deg z_1 = \cdots = \deg z_{2S} = N \\ z_1 = z_2, z_{s+1} = z_{s+2}}} \\ &\qquad E\left(\sum_{i=1}^{s} f(z_i) - f(z_{s+i})\right) d\alpha_1 \cdots d\alpha_d \\ &= \binom{d}{2}^2 \int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \left|C_N(\beta)\right|^2 \cdot \left|C_N(\alpha)\right|^{2s-4} d\alpha_1 \cdots d\alpha_d \end{aligned}$$

by Hölder's inequality

$$\begin{aligned} &\le \binom{d}{2}^2 \left(\int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} d\alpha_1 \cdots d\alpha_d\right)^{\frac{1}{s}} \left(\int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \left|C_N(\beta)\right|^{2s} d\alpha_1 \cdots d\alpha_d\right)^{\frac{1}{s}} \\ &\qquad \times \left(\int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \left|C_N(\alpha)\right|^{2s} d\alpha_1 \cdots d\alpha_d\right)^{1-\frac{2}{s}} \\ &\le \binom{d}{2}^2 J_s(N)^{1-\frac{1}{s}}. \end{aligned}$$

Thus if $I_1 \le I_2$, then we get

$$J_s(N) \le 2I_1 + 2I_2 \le 4I_2 \le 4\binom{d}{2}^2 J_s(N)^{1-\frac{1}{s}}.$$

This implies

$$J_s(N) \le 4^s \binom{d}{2}^{2s}.$$

Therefore in any case, we have

$$J_s(N) \le 4^s \binom{d}{2}^{2s} + 4I_1 \ll I_1.$$

It remains to treat I_1. Since $d \ge 2$, by (6), for large N, there exists a set Λ consisting of $d^2(d-1)$ monic irreducible polynomials P with $N/d + 1 \ge \deg P > N/d$. Let $\omega_d(z)$ denote the number of distinct monic irreducible polynomials P which divide z and $\deg P > N/d$. Given $z_1, \cdots, z_d \in \mathbf{A}_+$ of degree N and all distinct, put

$$z = \prod_{1 \le i < j \le d} (z_i - z_j).$$

Then we have

$$\omega_d(z) < \frac{\deg z}{N/d} < \frac{d^2(d-1)}{2}.$$

Now I_1 is the number of solutions of (22) with $z_1, \cdots, z_d$ distinct and $z_{s+1}, \cdots, z_{s+d}$ distinct. Thus, for any solution $z_1, \cdots, z_{2s}$ counted by I_1, by the above inequality, there is a $P \in \Lambda$ such that $z_1, \cdots, z_d$ are distinct modulo P and $z_{s+1}, \cdots, z_{s+d}$ are distinct modulo P. Thus

$$I_1 \le \sum_{P \in \Lambda} I_1(P),$$

where $I_1(P)$ denotes the number of solutions of (22) with $z_1, \cdots, z_d$ distinct modulo P, and $z_{s+1}, \cdots, z_{s+d}$ distinct modulo P.

Let $\alpha = (\alpha_1, \cdots, \alpha_d), a \in \mathbf{A}$, and $P \in \Lambda$, we define

$$C_N(\alpha, a, P) = \sum_{\substack{z \in \mathbf{A}_+, \deg z = N \\ z \equiv a \pmod P}} E(\alpha_d z^d + \cdots + \alpha_1 z).$$

We have

$$I_1(P) = \int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \Big| \sum_{\substack{a_1, \cdots, a_d \in \mathbf{A} \\ \deg a_1, \cdots, \deg a_d < \deg P \\ a_1, \cdots, a_d \text{ distinct}}} C_N(\alpha, a_1, P) \cdots C_N(\alpha, a_d, P) \Big|^2 \times \Big| \sum_{c \in \mathbf{A}, \deg c < \deg P} C_N(\alpha, c, P) \Big|^{2s-2d} d\alpha_1 \cdots d\alpha_d.$$

By Hölder's inequality, we have

$$\Big| \sum_{\substack{c \in \mathbf{A} \\ \deg c < \deg P}} C_N(\alpha, c, P) \Big|^{2s-2d} \le |P|^{2s-2d-1} \sum_{c \in \mathbf{A}, \deg c < \deg P} \Big| C_N(\alpha, c, P) \Big|^{2s-2d}.$$

Thus

$$I_1(P) \le |P|^{2s-2d} \max_{c \in \mathbf{A}, \deg c < \deg P} I_3(c),$$

where $I_3(c)$ is the number of solutions of the simultaneous equations

$$\sum_{i=1}^{d} (z_i^j - z_{s+i}^j) = \sum_{i=d+1}^{s} \left((Pz_{s+i} + c)^j - (Pz_i + c)^j \right) \qquad (1 \le j \le d)$$

with $z_i \in \mathbf{A}_+, \deg z_i = \deg z_{s+i} = N (1 \le i \le d), \deg z_i = \deg z_{s+i} = N - \deg P (d+1 \le i \le s)$, $z_1, \cdots, z_d$ distinct modulo P, and $z_{s+1}, \cdots, z_{s+d}$ distinct modulo P. A simple application of the binomial theorem shows (cf. [17], p. 61) that $I_3(c)$ is also the number of solutions of the simultaneous equations

$$\sum_{i=1}^{d} \left(z_i^j - z_{s+i}^j \right) = \sum_{i=d+1}^{s} P^j \left(z_{s+i}^j - z_i^j \right) \qquad (1 \le j \le d)$$

with the variables satisfying the same conditions as before. Since $\deg z_{s+i} = N < d\cdot\deg P (1\le i\le d)$, $\deg z_i = \deg z_{s+i} = N - \deg P (d+1\le i\le s)$, and the number of solutions of (23) is $\le J_s(N)$, by lemma 5.2 , we have

$$I_3(c) \le q^{N\cdot d}\cdot d!|P|^{\frac{d(d-1)}{2}}\cdot J_{s-d}(N-\deg P).$$

Thus

$$I_1(P) \le d!q^{N\cdot d}\cdot |P|^{2s+\frac{d(d-5)}{2}}\cdot J_{s-d}(N-\deg P).$$

This implies

$$I_1 \le d^2(d-1)d!q^{N\cdot d}\max_{P\in\Lambda}|P|^{2s+\frac{d(d-5)}{2}}\cdot J_{s-d}(N-\deg P).$$

Since $s-d = d(l-1)$, by induction and $N/d+1\ge \deg P$, we obtain

$$\begin{aligned} J_s(N) &\ll q^{N\cdot d}\max_{P\in\Lambda}|P|^{2s+\frac{d(d-5)}{2}}(q^{N-\deg P})^{2(s-d)-\frac{d(d+1)}{2}+\frac{1}{2}d^2(1-1/d)^{l-1}} \\ &\ll (q^N)^{2s-d-\frac{d(d+1)}{2}+\frac{1}{2}d^2(1-1/d)^{l-1}}\max_{P\in\Lambda}|P|^{d^2-\frac{1}{2}d^2(1-1/d)^{l-1}} \\ &\ll (q^N)^{2s-\frac{d(d+1)}{2}+\delta-\frac{1}{d}\left(d^2-\frac{1}{2}d^2(1-1/d)^{l-1}\right)}\left(q^{N/d}\right)^{d^2-\frac{1}{2}d^2(1-1/d)^{l-1}} \\ &\ll (q^N)^{2s-\frac{d(d+1)}{2}+\delta}. \end{aligned}$$

This completes this proof. □

Let $f(z)$ denote a polynomial of degree d with coefficients in $\mathbf{A}$.

Theorem 5.4. *Let $d<p$ and l be positive integers, and let $s=dl$. Then we have*

$$\int_{\mathfrak{M}}|S(\alpha\cdot f,N)|^{2s}d\alpha \ll q^{N(2s-d+\delta)},$$

where $2\delta = d^2(1-1/d)^l$, and the implied constant depends only on d,l , and q.

Proof. Write

$$f(z) = a_dz^d+\cdots+a_1z+a_0\in\mathbf{A}[z].$$

The number of solutions of the equation

$$f(z_1)+\cdots+f(z_s) = f(z_{s+1})+\cdots+f(z_{2s})$$

with $z_i\in\mathbf{A}_+$ and $\deg z_i = N$, is obviously equal to the number of solutions of the equations

$$\sum_{i=1}^{s}\left(z_i^j - z_{s+i}^j\right) = g_j \qquad (1\le j\le d), \tag{25}$$

where $g_1,\cdots,g_d$ satisfy

$$a_dg_d+\cdots+a_1g_1 = 0 \tag{26}$$

with $g_j\in\mathbf{A}$ and $\deg g_j < j\cdot N$. Since $\deg g_j < j\cdot N$, the number of d-tuple $(g_1,\cdots,g_d)$ satisfying (26) is

$$\ll (q^N)^{1+2+\cdots+(d-1)} = q^{N\cdot\frac{1}{2}d(d-1)}.$$

Fix a d-tuple $(g_1, \cdots, g_d)$, the number of solutions of (25) is equal to

$$\int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \Big| \sum_{z \in \mathbf{A}_+, \deg z = N} E(\alpha_d z^d + \cdots + \alpha_1 z) \Big|^{2s} \times E(-(\alpha_d g_d + \cdots + \alpha_1 g_1)) d\alpha_1 \cdots d\alpha_d$$
$$\leq \int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \Big| \sum_{z \in \mathbf{A}_+, \deg z = N} E(\alpha_d z^d + \cdots + \alpha_1 z) \Big|^{2s} d\alpha_1 \cdots d\alpha_d.$$

By theorem 5.3, this integral is

$$\ll (q^N)^{2s - \frac{1}{2}d(d+1) + \delta}.$$

Then we have

$$\int_{\mathfrak{M}} |S(\alpha \cdot f, N)|^{2s} d\alpha \ll q^{N(2s - d + \delta)}.$$

□

6. Weyl's inequality for polynimial Waring problem

Let

$$g(z) = \alpha_d z^d + \cdots + \alpha_1 z \in \mathfrak{M}[z].$$

The purpose of this section is to estimate the Polynomial Weyl sum $S(g, N)$ via the result of section 5. The main result of this section is corollary 6.2. It sharp a result of Effinger and Hayes [4], theorem 8.11.

Theorem 6.1. *Suppose $3 \leq d = \deg g < p$. If there exists $Q \in \mathbf{A}_+, h \in \mathbf{A}$ satisfying $(h, Q) = 1, N < \deg Q \leq (d-1)N$, and*

$$\deg(\alpha_d - h/Q) < -(\deg Q + (d-1)N),$$

then we have

$$S(g, N) = \sum_{z \in \mathbf{A}_+, \deg z = N} E(g(z)) \ll q^{N(1 - 1/\sigma_d)},$$

where $\sigma_d = 2d^2(2 \ln d + \ln \ln d + 3)$, and the implied constant depends only on d and q.

Proof. When $c \in \mathbf{A}, \deg c < N$, let

$$S(c) = \sum_{z \in \mathbf{A}_+, \deg z = N} E(g(z + c) - g(c))$$
$$= \sum_{z \in \mathbf{A}_+, \deg z = N} E(Y_d z^d + \cdots + Y_1 z),$$

where

$$Y_j = Y_j(c) = \binom{d}{j} \alpha_d c^{d-j} + \cdots + \binom{j+1}{j} \alpha_{j+1} c + \alpha_j, \quad (1 \leq j \leq d). \tag{27}$$

Obviously we have

$$\big|S(g,N)\big| = \big|S(c)\big|.$$

Hence

$$\big|S(g,N)\big| = q^{-N} \sum_{c\in\mathbf{A},\deg c<N} |S(c)|.$$

By Hölder's inequality, we have

$$|S(g,N)|^{2s} \le q^{-N} \sum_{c\in\mathbf{A},\deg c<N} |S(c)|^{2s}. \tag{28}$$

For any $z \in \mathbf{K}_\infty$,

$$z = \sum_{i=d}^{-\infty} a_i T^i.$$

Define

$$\{z\} = \sum_{i=-1}^{-\infty} c_i T^i.$$

For a fixed c, $Y_1, \cdots, Y_d$ are also fixed. Now let $U(c)$ be the set of $(d-1)$-tuple $(\beta_1, \cdots, \beta_{d-1}) \in \mathfrak{M}^{d-1}$ satisfying

$$\deg\{\beta_j - Y_j\} < -jN, \qquad (1 \le j \le d-1).$$

Let

$$S_1 = \sum_{z\in\mathbf{A}_+,\deg z=N} E(\alpha_d z^d + \beta_{d-1} z^{d-1} + \cdots + \beta_1 z).$$

Then we have

$$\big|S(c)\big| = \big|S_1\big|,$$

and we obtain

$$\big|S(c)\big|^{2s} = \big|S_1\big|^{2s}.$$

Integrating both sides of the above equation, where the integration is taken over $U(c)$, we obtain

$$|S(c)|^{2s} = (q^N)^{\frac{1}{2}d(d-1)} \int\cdots\int |S_1|^{2s} d\beta_1 \cdots d\beta_{d-1}. \tag{29}$$

Combining (28) and (29), we get

$$|S(g,N)|^{2s} \le (q^N)^{\frac{1}{2}d(d-1)-1} \sum_{c\in\mathbf{A},\deg c<N} \int\cdots\int \big|S_1\big|^{2s} d\beta_1 \cdots d\beta_{d-1}.$$

By (27), we know that for any $c_1 \ne c_2$,

$$Y_{d-1}(c_1) - Y_{d-1}(c_2) = d\alpha_d(c_1 - c_2).$$

Let $r_d = \alpha_d - h/Q$. Since $\deg r_d < -(\deg Q + (d-1)N)$, $p > d \ge 2$, $N < \deg Q$, and $(Q,h) = 1$, we have $Q \nmid (c_1 - c_2)$,

$$\deg\{d(c_1 - c_2)r_d\} < -\deg Q,$$

and

$$\deg\left\{\frac{d(c_1 - c_2)h}{Q}\right\} \ge -\deg Q.$$

Thus by $\deg Q \le (d-1)N$

$$\deg\{Y_{d-1}(c_1) - Y_{d-1}(c_2)\} \ge -\deg Q \ge -(d-1)N.$$

This implies that $U(c_1)$ and $U(c_2)$ have no common point. Hence we know that

$$|S(g,N)|^{2s} \le (q^N)^{\frac{1}{2}d(d-1)-1} \int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} |S_1|^{2s} d\beta_1 \cdots d\beta_{d-1}.$$

Using

$$\begin{aligned}
&\int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} |S_1|^{2s} d\beta_1 \cdots d\beta_{d-1} \\
&\quad \le \int_{\mathfrak{M}} \cdots \int_{\mathfrak{M}} \Big| \sum_{z \in \mathbf{A}_+, \deg z = N} E(\beta_{d-1} z^{d-1} + \cdots + \beta_1 z) \Big|^{2s} d\beta_1 \cdots d\beta_{d-1},
\end{aligned}$$

and theorem 5.3 with $s = l(d-1)$ and $d \ge 2$, we obtain

$$\begin{aligned}
|S(g,N)|^{2s} &\ll (q^N)^{\frac{1}{2}d(d-1)-1} (q^N)^{2s - \frac{1}{2}d(d-1)+\delta} \\
&= q^{N(2s-1+\delta)}.
\end{aligned}$$

Thus we have

$$S(g,N) \ll q^{N(1-\frac{1-\delta}{2s})},$$

where $2\delta = (d-1)^2(1-\frac{1}{d-1})^l$. If we take positive integer l satisfying

$$\frac{\ln(d^2 \ln d)}{-\ln(1-1/d)} < l \le \frac{\ln(d^2 \ln d)}{-\ln(1-1/d)} + 1,$$

then we have

$$\delta < \frac{1}{2} d^2 (1 - \frac{1}{d})^l < \frac{1}{2 \ln d},$$

Since

$$\frac{1}{-\ln(1-1/d)} < d,$$

we have

$$l < d \ln(d^2 \ln d) + 1.$$

It follows that

$$\begin{aligned}
\frac{2s}{1-\delta} &< \frac{2ld}{1-\delta} \\
&< 2d(d \ln(d^2 \ln d) + 1)(1 + \frac{1}{2 \ln d - 1}) \\
&= 2d^2 \left(2 \ln d + \ln \ln d + \frac{1}{d} + \frac{2 \ln d}{2 \ln d - 1} + \frac{\ln \ln d}{2 \ln d - 1} + \frac{1}{2d \ln d - d} \right)
\end{aligned}$$

by $d \ge 3$

$$\le 2d^2 (2 \ln d + \ln \ln d + 3).$$

Hence we obtain the theorem. □

In [4], theorem 8.11, we know that if $d \geq 2$, then

$$S(g,N) \ll q^{N(1-1/(2^{d-1}+1))}.$$

Combining this with theorem 6.1, we have

Corollary 6.2. *Suppose that* $2 \leq d = \deg g < p$. *If there exists* $Q \in \mathbf{A}_+, h \in \mathbf{A}$ *satisfying* $(h,Q)=1, N < \deg Q \leq (d-1)N$, *and*

$$\deg(\alpha_d - h/Q) < -(\deg Q + (d-1)N),$$

then we have

$$S(g,N) = \sum_{z\in\mathbf{A}_+,\deg z=N} E(g(z)) \ll q^{N(1-1/\sigma_d)},$$

where

$$\sigma_d = \begin{cases} 2^{d-1}+1 & \text{if } 2 \leq d < 13, \\ 2d^2(2\ln d + \ln\ln d + 3) & \text{if } 13 \leq d, \end{cases}$$

and the implied constant depends only on d *and* q.

7. Hua's inequality for polynomial Waring problem

Throughout this section, let d be a positive integer satisfying $2 \leq d < p$, p the characteristic of $\mathbf{A}$. Let $f(z) = a_d z^d + \cdots + a_1 z + a_0$ be a fixed polynomial of degree d with coefficients in $\mathbf{A}$ such that $(a_d, a_{d-1}, \cdots, a_1) = 1$. Let D be the maximal degree of the coefficients of f. Let N denote a positive integer satisfying $N \geq D$. For any $Q \in \mathbf{A}_+, h \in \mathbf{A}$ with $\deg h < \deg Q \leq N + \deg a_d$ and $(h,Q)=1$, let $\mathfrak{M}_{\mathrm{maj}}(h/Q)$ be the set of $\alpha \in \mathbf{K}_\infty$ satisfying

$$\deg(\alpha - h/Q) < -(\deg Q + \deg a_d + (d-1)N),$$

and write $\mathfrak{M}_{\mathrm{maj}}$ for the union of the $\mathfrak{M}_{\mathrm{maj}}(h/Q)$ with $\deg h < \deg Q \leq N + \deg a_d$ and $(h,Q) = 1$. We know that $\mathfrak{M}_{\mathrm{maj}}(h/Q) \subseteq \mathfrak{M}$ and any two $\mathfrak{M}_{\mathrm{maj}}(h/Q)$ have no common point. Let $\mathfrak{M}_{\mathrm{min}}$ denote the elements in $\mathfrak{M}$ which are not in any of the sets $\mathfrak{M}_{\mathrm{maj}}(h/Q)$. Then we have $\mathfrak{M} = \mathfrak{M}_{\mathrm{maj}} \bigcup \mathfrak{M}_{\mathrm{min}}$. As defined in section 4, let

$$S(f,N) = \sum_{b\in\mathbf{A}_+,\deg b=N} E(f(b)).$$

Lemma 7.1. *Suppose*

$$s \geq \begin{cases} d^2(d-2)+6 & \text{if } 2 \leq d < 9, \\ d^2(2\ln d + \ln\ln d + 2) - 2d & \text{if } 9 \leq d. \end{cases}$$

We have

$$\int_{\mathfrak{M}_{\mathrm{min}}} \left|S(\alpha f, N)\right|^{2s} d\alpha \ll q^{N(2s-d)},$$

where the implied constant depends only on d *and* q.

Proof. By theorem 11.1, there are unique $Q \in \mathbf{A}_+, h \in \mathbf{A}$ such that $\deg Q \leq (d-1)N, (Q,h) = 1$, and $\deg(\alpha \cdot a_d - h/Q) < -(\deg Q + (d-1)N)$. This implies

$$\deg(\alpha - h/(a_d Q)) < -(\deg Q + \deg a_d + (d-1)N).$$

Since $\alpha \in \mathfrak{M}_{\min}$ and the uniqueness, $\deg a_d Q > N + \deg a_d$, i.e., $(d-1)N \geq \deg Q > N$.

When $d \geq 9$, by corollary 6.2, we get

$$S(\alpha f, N) \ll \left(q^N\right)^{1-1/\sigma_d},$$

where $\sigma_d = 2d^2(2\ln d + \ln\ln d + 3)$. Let $s = s_1 + s_2$. We obtain

$$\int_{\mathfrak{M}_{\min}} \left|S(\alpha f, N)\right|^{2s} d\alpha \ll \left(q^N\right)^{2s_1(1-1/\sigma_d)} \int_{\mathfrak{M}} \left|S(\alpha f, N)\right|^{2s_2} d\alpha$$

by theorem 5.4, if $s_2 \geq dl$, then

$$\begin{aligned} &\ll \left(q^N\right)^{2s_1(1-1/\sigma_d)} \cdot \left(q^N\right)^{2s_2 - d + \delta} \\ &\ll \left(q^N\right)^{2s - d - 2s_1/\sigma_d + \delta}, \end{aligned}$$

where $2\delta = d^2(1-1/d)^l$. If we take $s_1 = 2d^2$ and positive integer l satisfies

$$\frac{\ln(d^2 \ln d)}{-\ln(1-1/d)} < l \leq \frac{\ln(d^2 \ln d)}{-\ln(1-1/d)} + 1,$$

then we have

$$\delta < \frac{1}{2} d^2 \cdot \frac{1}{d^2 \ln d} = \frac{1}{2\ln d}.$$

Since $d \geq 9$, we have

$$\frac{2s_1}{\sigma_d} = \frac{4d^2}{2d^2(2\ln d + \ln\ln d + 3)} > \frac{1}{2\ln d}.$$

Thus we obtain

$$\int_{\mathfrak{M}_{\min}} \left|S(\alpha f, N)\right|^{2s} d\alpha \ll q^{N(2s-d)}.$$

Now since $d \geq 9$ and

$$\frac{1}{-\ln(1-1/d)} < d - 1/2,$$

we have

$$\begin{aligned} l &< (d - \frac{1}{2})(\ln(d^2 \ln d)) + 1 \\ &= d\ln(d^2 \ln d) - \ln d - \frac{1}{2}\ln\ln d + 1 \\ &< 2d\ln d + d\ln\ln d - 2. \end{aligned}$$

Thus

$$s_1 + dl < d^2(2\ln d + \ln\ln d + 2) - 2d.$$

Therefore if $d \geq 9$ and $s \geq d^2(2\ln d + \ln\ln d + 2) - 2d$, then $s_2 \geq dl$ and we obtain

$$\int_{\mathfrak{M}_{\min}} \left|S(\alpha f, N)\right|^{2s} d\alpha \ll q^{N(2s-d)}.$$

When $2 \leq d < 9$, by the same way, if $s \geq d^2(d-2) + 6$, then we have

$$\int_{\mathfrak{M}_{\min}} \left|S(\alpha f, N)\right|^{2s} d\alpha \ll q^{N(2s-d)}.$$

□

Lemma 7.2. *Suppose $\alpha = h/Q + \beta \in \mathfrak{M}_{\mathrm{maj}}(h/Q)$ and $\deg Q \leq N$. Then we have*

$$S(\alpha f, N) \ll \frac{q^N}{|Q|^{\frac{1}{d}}},$$

where the implied constant depends only on d and q.

Proof. We have

$$\begin{aligned} S(\alpha f, N) &= \sum_{a \in \mathbf{A}_+, \deg a = N} E(\alpha f(a)) \\ &= \sum_{b \in \mathbf{A}, \deg b < \deg Q} \sum_{\substack{a \in \mathbf{A}_+, \deg a = N \\ a \equiv b \pmod Q}} E(\frac{h \cdot f(a)}{Q}) \cdot E(\beta f(a)) \\ &= \sum_{b \in \mathbf{A}, \deg b < \deg Q} E(\frac{h \cdot f(b)}{Q}) \sum_{\substack{a \in \mathbf{A}_+, \deg a = N \\ Q \mid a}} E(\beta f(a+b)). \end{aligned}$$

Since $\deg a_i \leq D \leq N$ and $\deg b < \deg Q \leq N$,

$$\deg(a_i a^{i-1} b) \leq \deg a_d + (d-1)N + \deg Q - 1 \qquad (1 \leq i \leq d).$$

By $\deg \beta < -(\deg Q + \deg a_d + (d-1)N)$, we get

$$\deg(\beta a_i a^{i-1} b) < -1 \qquad (1 \leq i \leq d).$$

Since

$$f(a+b) = a_d(a^d + da^{d-1}b + \cdots) + a_{d-1}(a^{d-1} + (d-1)a^{d-2}b + \cdots) + \cdots,$$

so $E(\beta f(a+b)) = E(\beta f(a))$. By theorem 2.1 and $(a_d, a_{d-1}, \cdots, a_1) = 1$, we obtain

$$\begin{aligned} S(\alpha f, N) &= S(hf, Q) \sum_{c \in \mathbf{A}_+, \deg c = N - \deg Q} E(\beta f(Qc)) \\ &\ll |Q|^{1-1/d} \cdot q^{N - \deg Q} \qquad (30) \\ &\ll \frac{q^N}{|Q|^{1/d}}. \end{aligned}$$

□

Lemma 7.3. *Suppose* $2s > 2d+1$. *We have*

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le N\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)}\left|S(\alpha f,N)\right|^{2s}d\alpha \ll q^{N(2s-d)},$$

where the implied constant depends only on d *and* q.

Proof. Let $\alpha\in\mathfrak{M}_{\mathrm{maj}}(h/Q)$ and let $\alpha = h/Q+\beta$. Since $D\le N$, if c is a polynomial of degree $N-\deg Q$ in $\mathbf{A}_+$, then

$$\beta f(Qc) = \beta Q^{d-1}(a_d c^d Q + a_{d-1}c^{d-1}) + y_c$$

for some $y_c\in\mathbf{K}_\infty$ with $\deg y_c < \deg(\beta\cdot a_d)+dN-(N-\deg Q)$. Since $d<p$, if c runs through over all polynomials of degree $N-\deg Q$ in $\mathbf{A}_+$ and assume $N>D$, then $\beta f(Qc)$ runs through over all $\mathrm{sgn}(\beta\cdot a_d)T^{\deg(\beta\cdot a_d)+dN}+c_1T^{\deg(\beta\cdot a_d)+dN-1}+\cdots+c_{N-\deg Q}T^{\deg(\beta\cdot a_d)+dN-(N-\deg Q)}+y(c_1,\cdots,c_{N-\deg Q})$, where $c_i\in\mathbb{F}_q\,(1\le i\le N-\deg Q)$ and $y(c_1,\cdots,c_{N-\deg Q})$ uniquely depends on c with $\deg y(c_1,\cdots,c_{N-\deg Q}) < \deg(\beta\cdot a_d)+dN-(N-\deg Q)$. If $\deg(\alpha-h/Q) = \deg\beta \ge -\deg a_d - dN$, then $\deg(\beta\cdot a_d)+dN\ge 0$ and $\deg(\beta\cdot a_d)+dN-(N-\deg Q)\le -1$ because $\deg\beta < -(\deg Q+\deg a_d+(d-1)N)$. By (30), we get $S(\alpha f,N)=0$. Thus, the sum mentioned in this lemma is equal to

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le N\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\int_{\deg(\alpha-h/Q)<-\deg a_d-dN}\left|S(\alpha f,N)\right|^{2s}d\alpha$$

by lemma 7.2

$$\ll \sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le N\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\int_{\deg(\alpha-h/Q)<-\deg a_d-dN}\left(\frac{q^N}{|Q|^{1/d}}\right)^{2s}d\alpha$$

$$\ll \sum_{Q\in\mathbf{A}_+,\deg Q\le N}\ \sum_{\substack{h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} q^{2sN}\int_{\deg(\alpha-h/Q)<-\deg a_d-dN}|Q|^{-2s/d}d\alpha$$

$$\ll q^{N(2s-d)}\sum_{Q\in\mathbf{A}_+,\deg Q\le N}|Q|^{1-2s/d}$$

by $2s>2d+1$

$$\ll q^{N(2s-d)}.$$

□

Lemma 7.4. *Suppose* $2s > 2d+1$. *We have*

$$\sum_{\substack{Q\in\mathbf{A}_+,N+1\le\deg Q\le N+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)}\left|S(\alpha f,N)\right|^{2s}d\alpha \ll q^{N(2s-d)}q^{2sD-N/d},$$

where the implied constant depends only on $d, s,$ *and* q.

Proof. Let $\beta=\alpha-h/Q$. Since $\deg\beta<-(\deg Q+\deg a_d+(d-1)N)\le -\deg a_d-dN-1$ and $D\le N$,

$$S(\alpha f,N)=\sum_{a\in\mathbf{A}_+,\deg a=N}E((h/Q)f(a))$$

by corollary 2.4 with $(h,Q)=1$ and $N<\deg Q$

$$\ll q^{D/d}|Q|^{1-1/d}.$$

Thus we have

$$\begin{aligned}
&\sum_{\substack{Q\in\mathbf{A}_+,N+1\le\deg Q\le N+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)}\left|S(\alpha f,N)\right|^{2s}d\alpha\\
&\ll \sum_{\substack{Q\in\mathbf{A}_+\\ N+1\le\deg Q\le N+\deg a_d}}\ \sum_{\substack{h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} q^{2sD/d}\times\\
&\qquad\int_{\deg(\alpha-h/Q)<-(\deg Q+\deg a_d+(d-1)N)}|Q|^{2s(1-1/d)}d\alpha\\
&\ll q^{-\deg a_d-(d-1)N+(2sD/d)}\sum_{\substack{Q\in\mathbf{A}_+\\ N+1\le\deg Q\le N+\deg a_d}}|Q|^{2s(1-1/d)}\\
&\ll q^{-\deg a_d-(d-1)N+(2sD/d)}\cdot(q^{N+\deg a_d})^{2s(1-1/d)+1}\\
&\ll (q^N)^{2s-d-(2s/d)+2}\cdot(q^{\deg a_d})^{2s-(2s/d)}q^{2sD/d}
\end{aligned}$$

by $2s>2d+1$ and $\deg a_d\le D$

$$\ll q^{N(2s-d)}q^{2sD-N/d}.$$

□

Combining lemma 7.1, lemma 7.3, lemma 7.4, and

$$\int_{\mathfrak{M}} |S(\alpha f, N)|^{2s} d\alpha$$
$$= \int_{\mathfrak{M}_{\min}} |S(\alpha f, N)|^{2s} d\alpha + \sum_{\substack{Q \in \mathbf{A}_+, \deg Q \le N + \deg a_d \\ h \in \mathbf{A}, \deg h < \deg Q \\ (h,Q)=1}} \int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)} |S(\alpha f, N)|^{2s} d\alpha,$$

we obtain

Theorem 7.5. *Suppose $d \ge 2$ and*

$$s \ge \begin{cases} d^2(d-2)+6 & \text{if } 2 \le d < 9, \\ d^2(2\ln d + \ln\ln d + 2) - 2d & \text{if } 9 \le d. \end{cases}$$

Then we have

$$\int_{\mathfrak{M}} |S(\alpha f, N)|^{2s} d\alpha \ll q^{N(2s-d)},$$

where the implied constant depends only on d, s, D, and q.

8. the minor and major arcs in polynomial Waring-Goldbach problem

Let f, d, a_d, and D be defined as in section 7. Let $Q \in \mathbf{A}_+, a \in \mathbf{A}$ satisfy $(a, Q) = 1$. Let $\pi_N(a, Q)$ denote the number of monic irreducible polynomials P of degree N with $P \equiv a \pmod{Q}$. The polynomial Euler phi function $\Phi(Q)$ is defined to be the order of $(\mathbf{A}/Q)^\times$. In [7], theorem 2.4, we have

$$\frac{q^N}{N \cdot \phi(Q)} - \frac{3 + \deg Q}{N} \cdot q^{N/2} < \pi_N(a, Q) \le \frac{q^N}{N \cdot \Phi(Q)} + \frac{\deg Q}{N} \cdot q^{N/2}. \tag{31}$$

Let $\alpha \in \mathfrak{M}$ and $r \in \mathbb{F}_q^\times$. We define $I(\alpha r f, N)$ to be

$$I(\alpha r f, N) = \sum_{\deg P = N}^{*} E(\alpha r f(P)),$$

where the asterisk denotes the sum over monic irreducible polynomials in $\mathbf{A}$. Fix $\sigma > 0$ and let $L = \sigma \ln N$. In this section, we assume that $N > \max\{D, L\}$. For any $Q \in \mathbf{A}_+, h \in \mathbf{A}$ with $\deg h < \deg Q \le L + \deg a_d$ and $(h, Q) = 1$, let $\mathfrak{M}_{\mathrm{maj}}(h/Q)$ be the set of $\alpha \in \mathfrak{M}$ satisfying

$$\deg(\alpha - h/Q) < -(\deg Q + \deg a_d + dN - L),$$

and write $\mathfrak{M}_{\mathrm{maj}}$ for the union of the $\mathfrak{M}_{\mathrm{maj}}(h/Q)$ with $\deg h < \deg Q \le L + \deg a_d$ and $(h, Q) = 1$. Let $\mathfrak{M}_{\min}$ denote the elements in $\mathfrak{M}$ which are not in any of the sets $\mathfrak{M}_{\mathrm{maj}}(h/Q)$.

Lemma 8.1. *Suppose* $\alpha = h/Q + \beta \in \mathfrak{M}_{\mathrm{maj}}(h/Q)$ *and* $\deg(\alpha - h/Q) < -\deg a_d - dN$. *Then we have*

$$I(\alpha rf, N) = \frac{q^N}{N} \cdot \frac{W(hrf, Q)}{\Phi(Q)} \cdot E(\beta a_d r T^{dN}) + O(N^\sigma \cdot q^{N/2}),$$

where the constant implied by the O-notation depends only on σ, D, *and* q.

Proof. Since $\deg \beta < -\deg a_d - dN$ and $D < N$, $\deg(\beta r a_d P^d) \le -1$, and $\deg(\beta r a_{d-i} P^{d-i}) < -1$ for $1 \le i \le d$. This implies

$$\begin{aligned}
I(\alpha rf, N) &= \sideset{}{^*}\sum_{\deg P = N} E((h/Q) \cdot rf(P)) \cdot E(\beta rf(P)) \\
&= E(\beta a_d r T^{dN}) \sideset{}{^*}\sum_{\deg P = N} E((h/Q) \cdot rf(P)) \\
&= E(\beta a_d r T^{dN}) \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ (a,Q)=1}} \sideset{}{^*}\sum_{\substack{\deg P = N \\ P \equiv a \pmod Q}} E((h/Q) \cdot rf(P)) \\
&= E(\beta a_d r T^{dN}) \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ (a,Q)=1}} E((h/Q) \cdot rf(a)) \sideset{}{^*}\sum_{\substack{\deg P = N \\ P \equiv a \pmod Q}} 1
\end{aligned}$$

by (31) and $\deg Q \le \sigma \ln N + \deg a_d$

$$\begin{aligned}
&= E(\beta a_d r T^{dN}) \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ (a,Q)=1}} E((h/Q) \cdot rf(a)) \times \\
&\qquad \left(\frac{q^N}{N \cdot \Phi(Q)} + O(q^{N/2}) \right)
\end{aligned}$$

again by $\deg Q \le \sigma \ln N + \deg a_d$

$$= \frac{q^N}{N} \cdot \frac{W(hrf, Q)}{\Phi(Q)} \cdot E(\beta a_d \cdot r T^{dN}) + O(N^\sigma \cdot q^{N/2}).$$

□

Lemma 8.2. *Suppose* $\alpha = h/Q + \beta \in \mathfrak{M}_{\mathrm{maj}}(h/Q)$ *and* $\deg(\alpha - h/Q) \ge -\deg a_d - dN$. *Then we have*

$$I(\alpha rf, N) \ll N^\sigma \cdot q^{N/2},$$

where the implied constant depends only on σ *and* q.

Proof. We write

$$\deg \beta = -\deg a_d - dN + l - 1,$$

where l is a positive integer such that $l \le \sigma \ln N - \deg Q$ because $\alpha \in \mathfrak{M}_{\mathrm{maj}}(h/Q)$. Thus we have

$$I(\alpha rf, N) = \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ (a,Q)=1}} E((h/Q) \cdot rf(a)) \sum_{\substack{\deg P = N \\ P \equiv a \pmod{Q}}}^{*} E(\beta rf(P)).$$

Given any $c \in \mathbf{A}$ with $\deg c < N - l$, since $\deg a_i \le D < N$,

$$\deg(a_i P^{i-1} c) \le \deg(a_d P^{d-1} c) \le \deg a_d + dN - l - 1 \quad (1 \le i \le d).$$

By $\deg \beta = -\deg a_d - dN + l - 1$, we get

$$\deg(\beta a_i P^{i-1} c) < -1 \qquad (1 \le i \le d).$$

Combining this and

$$f(P+c) = a_d(P^d + dP^{d-1}c + \cdots) + a_{d-1}(P^{d-1} + (d-1)P^{d-2}c + \cdots) + \cdots,$$

we have $E(\beta f(P+c)) = E(\beta f(P))$. Therefore, for any $y \in \mathbf{A}_+$ with $\deg(P - y) < N - l$, we have

$$E(\beta rf(y)) = E(\beta rf(P)). \tag{32}$$

Since $D < N$, if b is a polynomial in $\mathbf{A}_+$ of degree l, then $\beta f(bT^{N-l}) = \beta T^{(d-1)(N-l)}(a_d b^d T^{N-l} + a_{d-1} b^{d-1}) + y_b$ for some $y_b \in \mathbf{K}_\infty$ with $\deg y_b < \deg(\beta \cdot a_d) + dN - l$. Since $d < p$, if b runs through over all polynomials of degree l in $\mathbf{A}_+$, then $\beta f(bT^{N-l})$ runs through over all $\mathrm{sgn}(\beta \cdot a_d) T^{\deg(\beta \cdot a_d) + dN} + b_1 T^{\deg(\beta \cdot a_d) + dN - 1} + \cdots + b_l T^{\deg(\beta \cdot a_d) + dN - l} + y(b_1, \cdots, b_l)$, where $b_i \in \mathbb{F}_q (1 \le i \le l)$ and $y(b_1, \cdots, b_l)$ is uniquely depending on b (or b_i) with $\deg y(b_1, \cdots, b_l) < \deg(\beta \cdot a_d) + dN - l$. Since $\deg(\beta \cdot a_d) + dN - l = -1$, given any $u \in \mathbb{F}_q$, the number of polynomials $bT^{N-l} \in \mathbf{A}_+$ such that $\deg b = l$ and $\mathrm{Res}_\infty\left(\beta rf(bT^{N-l})\right) = u$ is equal to q^{l-1}. Combining (32) and [7], theorem 2.4, the number of monic irreducible polynomials P such that $\deg P = N$, $P \equiv a \pmod{Q}$, and $\mathrm{Res}_\infty(\beta rf(P)) = u$ is equal to

$$q^{l-1}\left(\frac{q^{N-l}}{N \cdot \Phi(Q)} + O(q^{N/2})\right) = \frac{q^{N-1}}{N \cdot \Phi(Q)} + O(q^{(N/2)+l}).$$

Thus we have

$$\begin{aligned} \sum_{\substack{\deg P = N \\ P \equiv a \pmod{Q}}}^{*} E(\beta rf(P)) &= \sum_{u \in \mathbb{F}_q} \psi(u) \left(\frac{q^{N-1}}{N \cdot \Phi(Q)} + O(q^{(N/2)+l})\right) \\ &= O(q^{(N/2)+l}). \end{aligned}$$

Since $l \le L - \deg Q$, we have

$$\begin{aligned} I(\alpha rf, N) &= \sum_{\substack{a \in \mathbf{A}, \deg a < \deg Q \\ (a,Q)=1}} E((h/Q) \cdot rf(a)) \cdot O(q^{(N/2)+l}) \\ &= O(q^{(N/2)+l+\deg Q}) \\ &= O(N^\sigma \cdot q^{N/2}). \end{aligned}$$

□

Lemma 8.3. *Suppose $\sigma_0 \geq 0$ and $\sigma \geq 2^{6d}(\sigma_0+1)d$. If $\alpha \in \mathfrak{M}_{\min}$, then we have*

$$I(\alpha r f, N) \ll \frac{q^N}{N^{\sigma_0}},$$

where the implied constant depends only on d, σ_0, and q.

Proof. By theorem 11.1, there are unique $Q \in \mathbf{A}_+, h \in \mathbf{A}$ such that $\deg Q \leq dN - L, (Q,h) = 1$, and $\deg(\alpha \cdot a_d - h/Q) < -(\deg Q + dN - L)$. This implies

$$\deg(\alpha - h/a_d Q) < -(\deg Q + \deg a_d + dN - L).$$

Since $\alpha \in \mathfrak{M}_{\min}$ and the uniqueness, $\deg a_d Q > L + \deg a_d$, i.e., $dN - L \geq \deg Q > L$. Since $\deg Q > L$ and $N > D$, we have

$$\begin{aligned} E(\alpha r f(P)) &= E((rh/a_d Q) f(P)) E((\alpha - h/a_d Q) r f(P)) \\ &= E((rh/a_d Q) f(P)). \end{aligned}$$

Therefore, by theorem 11.8, $\sigma \geq 2^{6d}(\sigma_0+1)d$, and $dN - L \geq \deg Q > L$, we obtain

$$\sum_{\deg P = N}^{*} E((rh/a_d Q) f(P)) \ll \frac{q^N}{N^{\sigma_0}}.$$

Combining these, we have

$$I(\alpha r f, N) \ll \frac{q^N}{N^{\sigma_0}}.$$

□

9. THE POLYNOMIAL WARING-GOLDBACH SINGULAR SERIES

Let $f(z)$ be a polynomial over $\mathbf{A}$ of degree $2 \leq d = \deg f < p$ such that the coefficients are relatively prime and $f(0) = 0$. Fix a positive integer s. Let $r_1, r_2, \cdots, r_s \in {\mathbb{F}_q^{\times}}^d$, and let M be a polynomial in $\mathbf{A}$. The polynomial Waring-Goldbach singular series $\mathfrak{S}(M)$ is defined to be

$$\mathfrak{S}(M) = \sum_{Q \in \mathbf{A}_+} \sum_{\substack{h \in \mathbf{A}, (h,Q)=1 \\ \deg h < \deg Q}} \frac{\prod_{i=1}^{s} W(h r_i f, Q)}{\Phi^s(Q)} \cdot E\left(-\frac{hM}{Q}\right). \tag{33}$$

By (9) and $f(0) = 0$, it is easy to deduce

$$\mathfrak{S}(M) = \prod_P \mathfrak{S}_P(M),$$

where the product runs through all monic irreducible polynomials P in $\mathbf{A}_+$ and

$$\mathfrak{S}_P(M) = 1 + \sum_{N=1}^{\infty} \sum_{\substack{h \in \mathbf{A}, P \nmid h \\ \deg h < N \deg P}} \frac{\prod_{i=1}^{s} W(hr_i f, P^N)}{\Phi^s(P^N)} \cdot E\left(-\frac{hM}{P^N}\right).$$

In this section, we study the properties of the polynomial Waring-Goldbach singular series when $f(z) = z^d$.

Lemma 9.1. *If $N \geq 2, P \nmid h$, and $f(z) = z^d$, then*

$$W(hf, P^N) = 0.$$

Proof. Let $a = a_1 + a_2 P^{N-1}$, where $a_1, a_2 \in \mathbf{A}, \deg a_1 < (N-1)\deg P, \deg a_2 < \deg P$, and $(a_1, P) = 1$. Then we have

$$a^d \equiv a_1^d + d a_1^{d-1} a_2 P^{N-1} \pmod{P^N}.$$

Hence we deduce

$$\begin{aligned} W(hf, P^N) &= \sum_{\substack{a_1 \in \mathbf{A}, (a_1, P) = 1 \\ \deg a_1 < (N-1)\deg P}} \sum_{\substack{a_2 \in \mathbf{A} \\ \deg a_2 < \deg P}} E\left(\frac{h a_1^d + h d a_1^{d-1} P^{N-1} a_2}{P^N}\right) \\ &= \sum_{\substack{a_1 \in \mathbf{A}, (a_1, P) = 1 \\ \deg a_1 < (N-1)\deg P}} E\left(\frac{h a_1^d}{P^N}\right) \sum_{\substack{a_2 \in \mathbf{A} \\ \deg a_2 < \deg P}} E\left(\frac{h d a_1^{d-1} a_2}{P}\right) \end{aligned}$$

by $(h d a_1^{d-1}, P) = 1$ and (8)

$$= 0.$$

□

Let $X_s(M, P)$ denote the number of solutions of the congruence

$$r_1 z_1^d + \cdots + r_s z_s^d \equiv M \pmod{P}$$

in $z_1, z_2, \cdots, z_s \in \mathbf{A}$ with $z_i \neq 0$ and $\deg z_i < \deg P$.

Lemma 9.2. *We have*

$$X_s(P, M) = \frac{\Phi^s(P)}{|P|} \cdot \mathfrak{S}_P(M).$$

Proof. We have

$$X_s(M,P) = \frac{1}{|P|} \sum_{\substack{a_1,\cdots,a_s \in \mathbf{A} \\ a_i \neq 0, \deg a_i < \deg P}} \sum_{\substack{h \in \mathbf{A} \\ \deg h < \deg P}} E\left(\frac{h(r_1 a_1^d + \cdots + r_s a_s^d - M)}{P}\right)$$

$$= \frac{1}{|P|} \sum_{\substack{h \in \mathbf{A} \\ \deg h < \deg P}} \prod_{i=1}^{s} W(hr_i f, P) E\left(-\frac{hM}{P}\right)$$

by lemma 9.1 and the definition of $\mathfrak{S}_P(M)$

$$= \frac{\Phi^s(P)}{|P|} \mathfrak{S}_P(M).$$

Hence we obtain the lemma. □

Now suppose that ${\mathbb{F}_p^{\times}}^d \neq \{1\}$, in other words, $2 \leq d \leq (p-1)/2$. Let δ be the cardinality of ${\mathbb{F}_p^{\times}}^d$. Then we have

$$\delta = \frac{p-1}{(d, p-1)} \geq \frac{p-1}{d} \geq 2.$$

It follows from Cauchy-Davenport theorem (cf. [14], theorems 2.2, 2.3) that the number of $z_1^d + z_2^d + \cdots + z_s^d \in \mathbb{F}_p^{\times}$ for all $z_i \in \mathbb{F}_p^{\times}$ is $\geq \min\{p, s(\delta-1)+1\}$. Since $d\delta \geq p-1$ and $p-1 \geq 2d$, if $s \geq 2d$, then we have $s(\delta-1)+1 \geq p$. Thus if ${\mathbb{F}_p^{\times}}^d \neq \{1\}$ and $s \geq 2d$, then there exist $z_1, z_2, \cdots, z_s \in \mathbb{F}_p^{\times}$ satisfying

$$z_1^d + z_2^d + \cdots + z_s^d = 0 \in \mathbb{F}_p. \tag{34}$$

In [15], Schwarz showed (the Waring problem for finite fields) that if $s \geq d$, then the equation

$$z_1^d + z_2^d + \cdots + z_s^d \equiv M \pmod{P} \tag{35}$$

have a solution with $z_i \in \mathbf{A}$ for each $M \in \mathbf{A}$. Combining this with (34) and $r_i \in {\mathbb{F}_q^{\times}}^d$, we obtain

Lemma 9.3. *Suppose that* ${\mathbb{F}_p^{\times}}^d \neq \{1\}$, *in other words,* $2 \leq d < p-1$. *If* $s \geq 3d$, *then* $X_s(M,P) > 0$ *for all monic irreducible polynomial* $P \in \mathbf{A}_+$ *and* $M \in \mathbf{A}$.

Lemma 9.4. *Suppose that* ${\mathbb{F}_p^{\times}}^d = \{1\}$, *in other words,* $2 \leq d = p-1$. *Then we have*

(a) *If* $q \geq p^4$ *and* $s \geq d+1$, *then* $X_s(M,P) > 0$ *for all monic irreducible polynomial* $P \in \mathbf{A}_+$ *and* $M \in \mathbf{A}$.
(b) *If* $q = p^2$ *and* $s \geq 2d+1$, *then* $X_s(M,P) > 0$ *for all monic irreducible polynomial* $P \in \mathbf{A}_+$ *and* $M \in \mathbf{A}$.
(c) *If* $q = p^3, p \geq 5$, *and* $s \geq (d+1)(d+2)/2$, *then* $X_s(M,P) > 0$ *for all monic irreducible polynomial* $P \in \mathbf{A}_+$ *and* $M \in \mathbf{A}$.

(d) *If* $q = p^3, p = 3$, *and* $s \geq 3$, *then* $X_s(M, P) > 0$ *for all monic irreducible polynomial* $P \in \mathbf{A}_+$ *and* $M \in \mathbf{A}$.

(e) *If* $q = p$, *and*

$$s \geq \begin{cases} (d+1)(d+2)/2 & \text{if } p \geq 5, \\ 3 & \text{if } p = 3, \end{cases}$$

then $X_s(M, P) > 0$ *for all monic irreducible polynomial* $P \in \mathbf{A}_+$ *and* $M \in \mathbf{A}$ *with*

$$M \equiv s \pmod{T^p - T}.$$

Proof. To prove (a), it follows from [12], Example 6.38 that if $q \geq p^4$, then there exist $a_1, a_2 \in \mathbb{F}_q^\times$ satisfying

$$a_1^d + a_2^d = 1. \tag{36}$$

Since $p \cdot 1^d = 0$, again by (35), for any $M \in \mathbf{A}$, there exist $z_1, z_2, \cdots, z_l \in \mathbf{A}$ satisfying $1 \leq l \leq d + 1 = p$, $P \nmid z_i$, and

$$z_1^d + z_2^d + \cdots + z_l^d \equiv M \pmod{P}.$$

Using (36), we have

$$z_1^d + z_2^d + \cdots + (a_1 z_l)^d + (a_2 z_l)^d \equiv M \pmod{P}.$$

Thus if $s \geq d + 1$, then $X_s(M, P) > 0$ for all monic irreducible polynomial $P \in \mathbf{A}_+$ and $M \in \mathbf{A}$.

To prove (b), since $2 \leq d = p - 1$, p is an odd prime number. Let g be a generator of $\mathbb{F}_q^\times$. Then $(g^{(p+1)/2})^d = -1$, i.e.,

$$(g^{(p+1)/2})^d + 1^d = 0.$$

Combining this with $p \cdot 1^d = 0$ and (35), we obtain that if $s \geq 2d + 1$, then $X_s(M, P) > 0$ for all monic irreducible polynomial $P \in \mathbf{A}_+$ and $M \in \mathbf{A}$.

To prove (c), by [3], corollary to theorem 1, there exist $z_1, z_2, \cdots, z_l \in \mathbb{F}_q^\times$ satisfying $1 \leq l \leq (p+1)/2$ and $-1 = z_1^d + z_2^d + \cdots + z_l^d$. Thus we have

$$z_1^d + z_2^d + \cdots + z_l^d + 1^d = 0, (1 \leq l \leq (p+1)/2),$$
$$p \cdot 1^d = 0.$$

Since $p \geq 5$, $(p, l + 1) = 1$. By elementary number theory, we know that if $s \geq p(l+1) - p - (l+1) + 1 = dl$, then there exist integers $x, y \geq 0$ satisfying $s = px + (l + 1)y$. Thus there exist $z_1, z_2, \cdots, z_s \in \mathbb{F}_q^\times$ satisfying

$$z_1^d + z_2^d + \cdots + z_s^d = 0.$$

Combining this with again [3], corollary to theorem 1, we obtain that if $s \geq (d + 1)(d + 2)/2 \geq dl + (p + 1)/2$, then $X_s(M, P) > 0$ for all monic irreducible polynomial $P \in \mathbf{A}_+$ and $M \in \mathbf{A}$.

To prove (d), it is easy to check that there exist $a_1, a_2 \in \mathbb{F}_q^\times$ satisfying $a_1^2 + a_2^2 = 1$. For example, in $\mathbb{F}_{27} = \mathbb{F}_3[T]/(T^3 - T - 1)$, taking $a_1 = T^2$ and

$a_2 = T^2 + 2T$. Combining this with $1^2 + 1^2 + 1^2 = 0$, we obtain that if $s \geq 3$, then there exist $z_1, z_2, \cdots, z_s \in \mathbb{F}_q^\times$ satisfying

$$z_1^2 + z_2^2 + \cdots + z_s^2 = 0.$$

Combining this with [3], corollary to theorem 1, if $s \geq 3$, then $X_s(M, P) > 0$ for all monic irreducible polynomial $P \in \mathbf{A}_+$ and $M \in \mathbf{A}$.

To prove (e), it follows from (a), (b), (c), (d), and the assumption of (e). □

Lemma 9.5. *Suppose that $f(z) = z^d$ and $2 \leq d < p$. Then if $s \geq 5$, then $\mathfrak{S}(M)$ converges for all $M \in \mathbf{A}$.*

Proof. It follows from lemma 9.1, (15), and $|P|/\Phi(P) \ll |P|^{\epsilon/s}$ (cf. [4], lemma 8.9) that we have

$$|\mathfrak{S}_P(M) - 1| \leq |P| \cdot \frac{d^s |P|^{s/2}}{\Phi^s(P)} \ll d^s |P|^{1-s/2+\epsilon}.$$

By (6) and $s \geq 5$, we obtain

$$\begin{aligned} \sum_P d^s |P|^{1-s/2+\epsilon} &\ll \sum_{i=1}^{\infty} \frac{q^i}{i} \cdot d^s q^{i(1-s/2+\epsilon)} \\ &\ll \sum_{i=1}^{\infty} d^s q^{i(\epsilon-1/2)}. \end{aligned}$$

Thus

$$\mathfrak{S}(M) = \prod_P \mathfrak{S}_P(M)$$

converges. □

The main result of this section is

Theorem 9.6. *Suppose that $f(z) = z^d$ and $2 \leq d < p$. Then if*

$$s \geq \begin{cases} 3d & \text{if } 2 \leq d < p-1, \\ \frac{(d+1)(d+2)}{2} & \text{if } d = p-1 \text{ and } p \geq 5, \\ 3 & \text{if } d = p-1 \text{ and } p = 3, \end{cases}$$

then $\mathfrak{S}(M) > 0$ for all $M \in \mathbf{A}$ with $M \equiv s \pmod{T^p - T}$ if $q = p$.

Proof. It follows from lemmas 9.2, 9.3, and 9.4 that $\mathfrak{S}_P(M) > 0$. By lemma 9.5 and

$$\mathfrak{S}(M) = \prod_P \mathfrak{S}_P(M),$$

we have $\mathfrak{S}(M) \geq 0$. By lemma 9.1, we have

$$\mathfrak{S}_P(M) = 1 + \sum_{\substack{h \in \mathbf{A}, P \nmid h \\ \deg h < \deg P}} \frac{\prod_{i=1}^{s} W(hr_i f, P)}{\Phi^s(P)} \cdot E\left(-\frac{hM}{P}\right)$$

by (15)

$$\geq 1 - |P| \cdot \left(\frac{d\sqrt{|P|}}{|P|-1}\right)^s$$
$$\geq 1 - d^s |P|^{1-s/2}$$

if $|P| \geq d^{4s}$, then we have

$$\geq 1 - |P|^{1-s/2+1/4}.$$

Since $s \geq 5$, by (6), we obtain

$$\mathfrak{S}(M) = \prod_{|P| < d^{4s}} \mathfrak{S}_P(M) \prod_{i \geq \ln_q d^{4s}} \left(1 - \frac{q^{-i/4}}{i}\right) > 0.$$

□

10. THE POLYNOMIAL WARING-GOLDBACH PROBLEM

Let d be a positive integer satisfying $2 \leq d < p$, p the characteristic of $\mathbf{A}$. Let $f(z) = a_d z^d + \cdots + a_1 z + a_0$ be a fixed polynomial of degree d with coefficients in $\mathbf{A}$ such that the coefficients are relatively prime and let D be the maximal degree of the coefficients of f. Let M be a polynomial in $\mathbf{A}$ with $\deg M \geq D$ and let $r_1, \cdots, r_s \in \mathbb{F}_q^{\times\, d}$ satisfy

$$\operatorname{sgn}(a_d) \cdot (r_1 + r_2 + \cdots + r_s) = \text{coefficient of the } dN\text{-th term of } M,$$

where the integer N satisfies $(\deg M - \deg a_d)/d \leq N < (\deg M - \deg a_d)/d + 1$. We observe that if $\deg M < dN$, then $r_1 + r_2 + \cdots + r_s = 0$. Further, let $G_{f,s}(M)$ be the number of monic irreducible polynomials $P_1, \cdots, P_s \in \mathbf{A}_+$, each of degree N, such that

$$M = r_1 f(P_1) + \cdots + r_s f(P_s).$$

For fixed $f, s, r_1, \cdots, r_s$, and M, the polynomial Waring-Goldbach singular series $\mathfrak{S}(M)$ is defined in (33). With $\mathfrak{S}(M)$ at hand, the asymptotic formula for the polynomial Waring-Goldbach problem is given in

Theorem 10.1. *Suppose*

$$s \geq \begin{cases} 2^d + 1 & \text{if } 2 \leq d < 11, \\ 2d^2(2\ln d + \ln\ln d + 2) - 4d + 2 & \text{if } d \geq 11. \end{cases}$$

Then for any given integer $s_1 > s$, we always have

$$G_{f,s}(M) - \frac{q^{N(s-d)}}{|a_d| \cdot N^s} \cdot \mathfrak{S}(M) \ll \frac{q^{N(s-d)}}{N^{s_1}},$$

where the implied constant depends only on d, D, s, s_1, and q.

Proof. Let $L = \sigma \ln N$, $\mathfrak{M}_{\mathrm{maj}}(h/Q)$, and $\mathfrak{M}_{\mathrm{min}}$ be defined in section 8. Then we have

$$\begin{aligned} G_{f,s}(M) &= \int_{\mathfrak{M}} \left(\prod_{i=1}^{s} I(\alpha r_i f, N) \right) E(-\alpha M) d\alpha \\ &= \int_{\mathfrak{M}_{\mathrm{min}}} \left(\prod_{i=1}^{s} I(\alpha r_i f, N) \right) E(-\alpha M) d\alpha + \\ &\qquad \sum_{\substack{Q \in \mathbf{A}_+, \deg Q \leq L + \deg a_d \\ h \in \mathbf{A}, \deg h < \deg Q \\ (h,Q)=1}} \int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)} \left(\prod_{i=1}^{s} I(\alpha r_i f, N) \right) E(-\alpha M) d\alpha. \end{aligned}$$

For $d \geq 11$, since $s \geq 2d^2(2\ln d + \ln\ln d + 2) - 4d + 2$, the integer $t = \lceil d^2(2\ln d + \ln\ln d + 2) - 2d \rceil$ satisfies $s - 2t \geq 0$. In lemma 8.3, let $\sigma_0 \geq s_1$,

if $\sigma \geq 2^{6d}(\sigma_0+1)d$, then we have

$$\int_{\mathfrak{M}_{\min}} \left(\prod_{i=1}^{s} I(\alpha r_i f, N)\right) E(-\alpha M)d\alpha$$
$$\ll \left(\frac{q^N}{N^{\sigma_0}}\right)^{s-2t} \int_{\mathfrak{M}} \prod_{i=1}^{2t} \left|I(\alpha r_i f, N)\right| d\alpha$$

by Cauchy's inequality

$$\leq \frac{q^{N(s-2t)}}{N^{\sigma_0}} \left(\prod_{i=1}^{2t} \int_{\mathfrak{M}} \left|I(\alpha r_i f, N)\right|^{2t} d\alpha\right)^{1/2t}$$
$$\leq \frac{q^{N(s-2t)}}{N^{\sigma_0}} \left(\prod_{i=1}^{2t} \int_{\mathfrak{M}} \left|S(\alpha r_i f, N)\right|^{2t} d\alpha\right)^{1/2t}$$

by theorem 7.5 and $t \geq d^2(2\ln d + \ln\ln d + 2) - 2d$

$$\ll \frac{q^{N(s-2t)}}{N^{\sigma_0}} \cdot q^{N(2t-d)}$$
$$\ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

For $2 \leq d < 11$, since $s \geq 2^d + 1$, if $\sigma \geq 2^{6d}(\sigma_0+1)d$, then by lemma 8.3, we have

$$\int_{\mathfrak{M}_{\min}} \left(\prod_{i=1}^{s} I(\alpha r_i f, N)\right) E(-\alpha M)d\alpha$$
$$\ll \left(\frac{q^N}{N^{\sigma_0}}\right)^{s-2^d} \int_{\mathfrak{M}} \prod_{i=1}^{2^d} \left|I(\alpha r_i f, N)\right| d\alpha$$

by Cauchy's inequality

$$\leq \frac{q^{N(s-2^d)}}{N^{\sigma_0}} \left(\prod_{i=1}^{2^d} \int_{\mathfrak{M}} \left|I(\alpha r_i f, N)\right|^{2^d} d\alpha\right)^{1/2^d}$$
$$\leq \frac{q^{N(s-2^d)}}{N^{\sigma_0}} \left(\prod_{i=1}^{2^d} \int_{\mathfrak{M}} \left|S(\alpha r_i f, N)\right|^{2^d} d\alpha\right)^{1/2^d}$$

by theorem 4.2 and $2 \le d < p$

$$\ll \frac{q^{N(s-2^d)}}{N^{\sigma_0}} \cdot q^{N(2^d-d)} N^{C_2}$$

let $\sigma_0 \ge s_1 + C_2$

$$\ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

To estimate the integral over $\mathfrak{M}_{\mathrm{maj}}(h/Q)$, by lemma 8.2, we have

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} \int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)} \left(\prod_{i=1}^{s} I(\alpha r_i f,N)\right) E(-\alpha M)d\alpha -$$

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} \int_{\deg(\alpha-h/Q)<-\deg a_d-dN} \left(\prod_{i=1}^{s} I(\alpha r_i f,N)\right) E(-\alpha M)d\alpha$$

$$\ll \sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} \int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)} \left(N^{\sigma} q^{N/2}\right)^s d\alpha$$

by $\deg(\alpha - h/Q) < -(\deg Q + \deg a_d + dN - L)$ and $L = \sigma \ln N$

$$\ll \sum_{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d} N^{s\sigma} \cdot q^{N(s/2-d)} \cdot q^{L-\deg a_d}$$

$$\ll N^{s\sigma+2\sigma} \cdot q^{N(s/2-d)} \ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

Suppose $\alpha = h/Q + \beta \in \mathfrak{M}_{\mathrm{maj}}(h/Q)$. We define

$$I^*(\alpha r_i f,N) = \frac{q^N}{N} \cdot \frac{W(hr_i f,Q)}{\Phi(Q)} \cdot E(\beta a_d r_i T^{dN}).$$

For any $0 < \epsilon < 1$, by [4], lemma 8.9, we have

$$\frac{1}{\Phi(Q)} \le C_\epsilon |Q|^{-1+\epsilon}. \tag{37}$$

Thus by corollary 2.5, we have

$$I^*(\alpha r_i f,N) \ll |Q|^{-(1/d)+\epsilon} \cdot \frac{q^N}{N}. \tag{38}$$

If $\deg(\alpha - h/Q) < -\deg a_d - dN$, then by lemma 8.1, we get

$$I(\alpha r_i f,N) - I^*(\alpha r_i f,N) \ll N^{\sigma} q^{N/2}. \tag{39}$$

Combining (38) and (39), we obtain

$$\prod_{i=1}^{s} I(\alpha r_i f, N) - \prod_{i=1}^{s} I^*(\alpha r_i f, N) \ll N^{\sigma} q^{N/2} \left(|Q|^{-(1/d)+\epsilon} \cdot \frac{q^N}{N} \right)^{s-1}.$$

Thus, we obtain

$$\sum_{\substack{Q \in \mathbf{A}_+, \deg Q \leq L + \deg a_d \\ h \in \mathbf{A}, \deg h < \deg Q \\ (h,Q)=1}} \int_{\deg(\alpha - h/Q) < -\deg a_d - dN} \left(\prod_{i=1}^{s} I(\alpha r_i f, N) - \prod_{i=1}^{s} I^*(\alpha r_i f, N) \right) E(-\alpha M) d\alpha$$

$$\ll \sum_{\substack{Q \in \mathbf{A}_+, \deg Q \leq L + \deg a_d \\ h \in \mathbf{A}, \deg h < \deg Q \\ (h,Q)=1}} \int_{\deg(\alpha - h/Q) < -\deg a_d - dN} N^{\sigma} q^{N/2} \left(|Q|^{-(1/d)+\epsilon} \frac{q^N}{N} \right)^{s-1} d\alpha$$

$$\ll N^{\sigma+1-s} q^{N(s-d-1/2)} \cdot q^{-\deg a_d} \sum_{Q \in \mathbf{A}_+, \deg Q \leq L + \deg a_d} |Q|^{1 - \frac{s-1}{d} + (s-1)\epsilon}$$

since $(s-1)/d \geq 2$, may choose $0 < \epsilon < 1$ such that the summation above converges

$$\ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

Combining these, we obtain

$$\sum_{\substack{Q \in \mathbf{A}_+, \deg Q \leq L + \deg a_d \\ h \in \mathbf{A}, \deg h < \deg Q \\ (h,Q)=1}} \int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)} \left(\prod_{i=1}^{s} I(\alpha r_i f, N) \right) E(-\alpha M) d\alpha -$$

$$\sum_{\substack{Q \in \mathbf{A}_+, \deg Q \leq L + \deg a_d \\ h \in \mathbf{A}, \deg h < \deg Q \\ (h,Q)=1}} \int_{\deg(\alpha - h/Q) < -\deg a_d - dN} \left(\prod_{i=1}^{s} I^*(\alpha r_i f, N) \right) E(-\alpha M) d\alpha$$

$$\ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

By the definition of $I^*(\alpha r_i f, N)$, we have

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\int_{\deg(\alpha-h/Q)<-\deg a_d-dN}\left(\prod_{i=1}^{s}I^*(\alpha r_i f,N)\right)E(-\alpha M)d\alpha$$

$$=\frac{q^{Ns}}{N^s}\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\frac{\prod_{i=1}^{s}W(hr_i f,Q)}{\Phi^s(Q)}\cdot E\left(-\frac{hM}{Q}\right)\times$$

$$\int_{\deg\beta<-\deg a_d-dN}E(\beta a_d(r_1+\cdots+r_s)T^{dN})E(-\beta M)d\beta$$

by $\operatorname{sgn}(a_d)\cdot(r_1+r_2+\cdots+r_s)=$ coefficient of the dN-th term of M

$$=\frac{q^{N(s-d)}}{|a_d|\cdot N^s}\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\le L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\frac{\prod_{i=1}^{s}W(hr_i f,Q)}{\Phi^s(Q)}\cdot E(-\frac{hM}{Q}).$$

Since

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q>L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}\frac{\prod_{i=1}^{s}W(hr_i f,Q)}{\Phi^s(Q)}\cdot E(-\frac{hM}{Q})$$

$$\ll\sum_{\substack{Q\in\mathbf{A}_+,\deg Q>L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}}(|Q|^{-(1/d)+\epsilon})^s\quad\text{(by corollary 2.5 and (37))}$$

$$\le\sum_{Q\in\mathbf{A}_+,\deg Q>L+\deg a_d}|Q|^{1-s/d+s\epsilon}$$

$$=\sum_{i=1}^{\infty}q^{(L+\deg a_d+i)(2-s/d+s\epsilon)}$$

may choose suitable $0 < \epsilon < 1$ such that $2 - s/d + s\epsilon < -1/(2^{6d}d)$

$$\ll q^{-\frac{L+\deg a_d}{2^{6d}d}}$$

by $L = \sigma \ln N$

$$\ll N^{-\frac{\sigma}{2^{6d}d}}$$

let $\sigma \geq 2^{6d}(\sigma_0 + 1)d$ and let $\sigma_0 \geq s_1$

$$\ll N^{-s_1},$$

we have

$$\mathfrak{S}(M) - \sum_{\substack{Q\in\mathbf{A}_+,\deg Q\leq L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} \left(\frac{\prod_{i=1}^{s} W(hr_i f, Q)}{\Phi^s(Q)}\right) \cdot E\left(-\frac{hM}{Q}\right) \ll N^{-s_1}.$$

This implies

$$\sum_{\substack{Q\in\mathbf{A}_+,\deg Q\leq L+\deg a_d\\ h\in\mathbf{A},\deg h<\deg Q\\ (h,Q)=1}} \int_{\mathfrak{M}_{\mathrm{maj}}(h/Q)} \left(\prod_{i=1}^{s} I(\alpha r_i f, N)\right) E(-\alpha M)d\alpha$$

$$- \frac{q^{N(s-d)}}{|a_d| \cdot N^s} \cdot \mathfrak{S}(M) \ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

Therefore, we obtain

$$G_{f,s}(M) - \frac{q^{N(s-d)}}{|a_d| \cdot N^s} \cdot \mathfrak{S}(M) \ll \frac{q^{N(s-d)}}{N^{s_1}}.$$

□

The main result of this paper is

Theorem 10.2. *Suppose* $2 \leq d < p$ *and*

$$s \geq \begin{cases} 2^d + 1 & \text{if } 2 \leq d < 11, \\ 2d^2(2\ln d + \ln\ln d + 2) - 4d + 2 & \text{if } d \geq 11. \end{cases}$$

Then for any given integer $s_1 > s$, *we have*

$$G_{z^d,s}(M) - \frac{q^{N(s-d)}}{N^s} \cdot \mathfrak{S}(M) \ll \frac{q^{N(s-d)}}{N^{s_1}},$$

where the implied constant depends only on d, s, s_1, *and* q, *and* $\mathfrak{S}(M) > 0$ *provided* $M \equiv s \pmod{T^p - T}$ *if* $q = p$ *and* $d = p - 1$.

Proof. It follows from theorem 9.6 and theorem 10.1. □

11. A THEOREM IN ADDITIVE THEORY OF IRREDUCIBLE POLYNOMIALS

The purpose of this section is to prove theorem 11.8. This theorem is an analogue of [11], theorem 10, due to Vinogradov. The classical Vinogradov's theorem plays a very important role in the additive theory of prime numbers. Throughout this section, let d be a positive integer satisfying $2 \leq d < p$ and let $f(z) \in \mathbf{K}_\infty[z]$ denote a polynomial of degree d with leading coefficient $\frac{a}{Q}$ satisfying $a \in \mathbf{A}, Q \in \mathbf{A}_+$, and $(a, Q) = 1$. Let $h \in \mathbf{A}_+$, the Weyl sum $S_h(f, N)$ is defined to be

$$S_h(f, N) = \sum_{b \in \mathbf{A}_+, \deg b = N, h|b} E(f(b)).$$

We recall the Dirichlet's theorem for $\mathbf{A}$ in

Theorem 11.1. *Given any $\alpha \in \mathbf{K}_\infty$ and positive integer N. There exist unique monic polynomial Q and polynomial a in $\mathbf{A}$ satisfying $(Q, a) = 1, \deg Q \leq N$, and $\deg(\alpha - a/Q) \leq -(\deg Q + N + 1)$.*

Proof. See [6]. □

If $\alpha = a_n T^n + \cdots + a_1 T + a_0 + \cdots \in \mathbf{K}_\infty, a_i \in \mathbb{F}_q$, then we define $[\alpha]$ to be the polynomial $[\alpha] = a_n T^n + \cdots + a_1 T + a_0 \in \mathbf{A}$. Let $z \in \mathbf{A}_+$ of degree N, let $\alpha \in \mathbf{K}_\infty$, and set

$$z = T^N + a_{N-1} T^{N-1} + \cdots + a_1 T + a_0,$$
$$\alpha - [\alpha] = b_{-l} T^{-l} + b_{-(l+1)} T^{-(l+1)} + \cdots,$$

where $a_i, b_j \in \mathbb{F}_q, l \geq 1$ satisfying $a_N = 1, b_{-l} \neq 0$ and $b_j = 0$ for $0 > j > -l$. Then we have

$$\begin{aligned}
&\mathrm{Res}_\infty(\alpha \cdot z) \\
&\quad = \mathrm{Res}_\infty((\alpha - [\alpha]) \cdot z) \\
&\quad = \begin{cases} 0 & \text{if } l > N + 1, \\ b_{-l} & \text{if } l = N + 1, \\ b_{-l} a_{l-1} + b_{-l-1} a_l + \cdots + b_{-N} a_{N-1} + b_{-N-1} & \text{if } 1 \leq l \leq N. \end{cases}
\end{aligned}$$

Since $b_{-l} \neq 0$, we get

Lemma 11.2. *We have*

$$\left| \sum_{z \in \mathbf{A}_+, \deg z = N} E(\alpha \cdot z) \right| = \begin{cases} q^N & \text{if } -\deg(\alpha - [\alpha]) \geq N + 1, \\ 0 & \text{if } 1 \leq -\deg(\alpha - [\alpha]) \leq N. \end{cases}$$

Let $z \in \mathbf{A}_+$ and let $\tau_m(z)$ denote the number of solutions of

$$z = z_1 z_2 \cdots z_{m+1}$$

with $z_1, z_2, \cdots, z_{m+1} \in \mathbf{A}_+$. Then we have (cf. [2], p. 43)

$$\sum_{z \in \mathbf{A}_+, \deg z = N} \tau_m(z) = \binom{N + m}{m} q^N. \tag{40}$$

From this, we have

Lemma 11.3. *We have*

$$\sum_{z\in\mathbf{A}_+,\deg z=N}\tau_1(z)^n \ll N^{2^n-1}q^N,$$

where the implied constant depends only on n and q.

Proof. We prove this lemma by induction on n. If $n=1$, then it follows from (40). Let us assume that

$$\sum_{z\in\mathbf{A}_+,\deg z=N}\tau_1(z)^{n-1} \ll N^{2^{n-1}-1}q^N. \tag{41}$$

Then

$$\begin{aligned}\sum_{z\in\mathbf{A}_+,\deg z=N}\tau_1(z)^n &= \sum_{y\in\mathbf{A}_+,\deg y\le N}\ \sum_{z\in\mathbf{A}_+,\deg z=N,y|z}\tau_1(z)^{n-1}\\ &= \sum_{y\in\mathbf{A}_+,\deg y\le N}\ \sum_{z\in\mathbf{A}_+,\deg z=N-\deg y}\tau_1(yz)^{n-1}\\ &\le \sum_{y\in\mathbf{A}_+,\deg y\le N}\tau_1(y)^{n-1}\sum_{z\in\mathbf{A}_+,\deg z=N-\deg y}\tau_1(z)^{n-1}\end{aligned}$$

by (41)

$$\ll \sum_{y\in\mathbf{A}_+,\deg y\le N}\tau_1(y)^{n-1}(N-\deg y)^{2^{n-1}-1}q^{N-\deg y}$$

again by (41)

$$\begin{aligned}&\ll \sum_{i=0}^{N} i^{2^{n-1}-1}q^i\cdot(N-i)^{2^{n-1}-1}q^{N-i}\\ &\ll N^{2^n-1}q^N.\end{aligned}$$

This completes the proof. □

Lemma 11.4. *Suppose that $\sigma_2\ge 2^{3d}-1$. Then*

$$\sum_{\substack{z\in\mathbf{A}_+,\deg z\le N\\ N^{\sigma_2}\le\tau_d(z)}}\tau_d(z)\ll\frac{q^N}{N^{\sigma_2}},$$

where the implied constant depends only on d and q.

Proof. By lemma 11.3, we have

$$\begin{aligned} N^{2\sigma_2} \sum_{\substack{z\in\mathbf{A}_+,\deg z\le N\\ N^{\sigma_2}\le \tau_d(z)}} \tau_d(z) &\le \sum_{z\in\mathbf{A}_+,\deg z\le N} \tau_d(z)^3 \\ &\le \sum_{i=1}^{N} \sum_{z\in\mathbf{A}_+,\deg z=i} \tau_1(z)^{3d} \\ &\ll \sum_{i=1}^{N} i^{2^{3d}-1} q^i \\ &\ll N^{\sigma_2} q^N. \end{aligned}$$

This completes the proof. □

Let the iterated difference operator $\Delta_{a_v,a_{v-1},\cdots,a_1}$ be as defined in section 4. Then we have

Lemma 11.5. *If $h\in\mathbf{A}_+, \deg h\le N$, then*

$$\left|S_h(f,N)\right|^{2^v} \le q^{(N-\deg h)(2^v-v-1)} \sum_{\substack{a_1,\cdots,a_v\in\mathbf{A},h|a_i\\ \deg a_i<N}} S_h(\Delta_{a_v,\cdots,a_1}f,N) \tag{42}$$

for all $1\le v\le d$.

Proof. We prove this lemma by induction on v. If $v=1$, then

$$\begin{aligned} \left|S_h(f,N)\right|^2 &= \sum_{\substack{a_1,a_2\in\mathbf{A},h|(T^N+a_i)\\ \deg a_i<N}} E(f(T^N+a_1)-f(T^N+a_2)) \\ &= \sum_{\substack{\deg a_2<N\\ h|(T^N+a_2)}} \sum_{\substack{\deg a_1<N\\ h|a_1}} E(f(T^N+a_1+a_2)-f(T^N+a_2)) \\ &= \sum_{\deg a_1<N,h|a_1} \sum_{\deg a_2<N,h|(T^N+a_2)} E(\Delta_{a_1}f(T^N+a_2)) \\ &= \sum_{\deg a_1<N,h|a_1} S_h(\Delta_{a_1}f,N) \end{aligned}$$

as desired. Let us assume that (42) holds for some $1\le v<d$. We square both sides and apply Cauchy's inequality on the right, using the fact that there are q^N polynomials of degree less than N and also using the result

just proved for $v = 1$. We obtain

$$\begin{aligned}
&\big|S_h(f,N)\big|^{2^{v+1}} \\
&\le q^{(N-\deg h)(2^{v+1}-2v-2)} \left(\sum_{\substack{a_1,a_2,\cdots,a_v \in \mathbf{A} \\ h|a_i, \deg a_i < N}} S_h(\Delta_{a_v,a_{v-1},\cdots,a_1} f, N) \right)^2 \\
&\le q^{(N-\deg h)(2^{v+1}-2v-2)} q^{(N-\deg h)v} \sum_{\substack{a_1,a_2,\cdots,a_v \in \mathbf{A} \\ h|a_i, \deg a_i < N}} |S_h(\Delta_{a_v,a_{v-1},\cdots,a_1} f, N)|^2 \\
&= q^{(N-\deg h)(2^{v+1}-(v+1)-1)} \sum_{\substack{a_1,a_2,\cdots,a_{v+1} \in \mathbf{A} \\ h|a_i, \deg a_i < N}} S_h(\Delta_{a_{v+1},a_v,\cdots,a_1} f, N).
\end{aligned}$$

This completes the proof. □

Lemma 11.6. *Let $\sigma_0, \sigma_3 \ge 0$ be real numbers and let $h \in \mathbf{A}_+$ satisfy $\deg h \le \min\{N, \sigma_3 \ln N\}$. Suppose that $\sigma \ln N \le \deg Q \le dN - \sigma \ln N$. Then, when*

$$\sigma \ge 2^d(\sigma_0 + \sigma_3) + 2^{3(d-2)},$$

we have

$$|\ S_h(f,N)\ | \ll \frac{q^{N-\deg h}}{N^{\sigma_0}},$$

where the implied constant depends only on d, σ_0, σ_3, and q.

Proof. Taking $v = d-1$ in lemma 11.5. Since f is a polynomial of degree d, we get

$$\Delta_{a_{d-1},\cdots,a_1} f(z) = d! \cdot a_1 a_2 \cdots a_{d-1} \cdot \frac{a}{Q} \cdot z + c(a_1, a_2, \cdots, a_{d-1}),$$

where $c(a_1, a_2, \cdots, a_{d-1})$ is a polynomial in $a_1, a_2, \cdots, a_{d-1}$. Therefore

$$|S_h(\Delta_{a_{d-1},\cdots,a_1} f, N)| = \Big| \sum_{b \in \mathbf{A}_+, \deg b = N, h|b} E\left(\frac{d! \cdot a_1 \cdots a_{d-1} \cdot a \cdot b}{Q}\right) \Big|.$$

There are clearly less than $d \cdot q^{(N-\deg h)(d-2)}$ $(d-1)$-tuples $(a_1, a_2, \cdots, a_{d-1})$ with at least one zero entry. For each of these, the sum on the right above is $q^{N-\deg h}$. Since $2 \le d < p$, by (42) with $v = d-1$ and lemma 11.2

$$\big|S_h(f,N)\big|^{2^{d-1}} \le dq^{(N-\deg h)(2^{d-1}-1)} + q^{(N-\deg h)(2^{d-1}-d)} X, \tag{43}$$

where

$$X = \sum_{\substack{a_1,a_2,\cdots,a_{d-1}\in\mathbf{A}\\ a_i\neq 0, h|a_i, \deg a_i<N}} \Big| \sum_{b\in\mathbf{A}_+,\deg b=N,h|b} E\left(\frac{a_1\cdots a_{d-1}\cdot a\cdot b}{Q}\right)\Big|$$

$$= \sum_{\substack{a_1,a_2,\cdots,a_{d-1}\in\mathbf{A}\\ a_i\neq 0, \deg a_i<N-\deg h}} \Big| \sum_{b\in\mathbf{A}_+,\deg b=N-\deg h} E\left(\frac{h^d a_1\cdots a_{d-1}\cdot a\cdot b}{Q}\right)\Big|$$

$$\ll \sum_{\substack{0\neq z\in\mathbf{A}\\ \deg z\le \deg h+(d-1)N}} \tau_{d-2}\big(\mathrm{sgn}(z)^{-1}z\big)\Big| \sum_{b\in\mathbf{A}_+,\deg b=N-\deg h} E\left(\frac{z\cdot a\cdot b}{Q}\right)\Big|$$

It follows from lemma 11.4 and lemma 11.2 that if $\sigma_2 \ge 2^{3(d-2)}-1$, then we have

$$X \ll \frac{q^{\deg h+(d-1)N}}{N^{\sigma_2}}\cdot q^{N-\deg h} +$$
$$N^{\sigma_2} \sum_{\substack{z\in\mathbf{A}\\ \deg z\le \deg h+(d-1)N}} \Big| \sum_{b\in\mathbf{A}_+,\deg b=N-\deg h} E\left(\frac{z\cdot a\cdot b}{Q}\right)\Big|$$

by $(Q,a)=1$

$$\ll \frac{q^{dN}}{N^{\sigma_2}} + N^{\sigma_2}\max\left\{1,\frac{q^{\deg h+(d-1)N}}{q^{\deg Q}}\right\} \sum_{\substack{z\in\mathbf{A}\\ \deg z<\deg Q}} \Big| \sum_{\substack{b\in\mathbf{A}_+\\ \deg b=N-\deg h}} E\left(\frac{z\cdot b}{Q}\right)\Big|$$

again by lemma 11.2 (taking $\alpha = z/Q$) and $\deg h \le N$

$$\ll \frac{q^{dN}}{N^{\sigma_2}} + N^{\sigma_2}\max\left\{1,\frac{q^{\deg h+(d-1)N}}{q^{\deg Q}}\right\}\cdot\max\left\{1,\frac{q^{\deg Q}}{q^{N-\deg h}}\right\}\cdot q^{N-\deg h}$$

by $\deg h \le \sigma_3 \ln N$ and $\sigma \ln N \le \deg Q \le dN - \sigma\ln N$

$$\ll q^{d(N-\deg h)}(N^{d\sigma_3-\sigma_2} + N^{\sigma_2+d\sigma_3-\sigma}).$$

If we take $\sigma_2 = 2^{d-1}(\sigma_0+\sigma_3) + 2^{3(d-2)} - 1 \ge 2^{3(d-2)}-1$, then since $\sigma \ge 2^d(\sigma_0+\sigma_3)+2^{3(d-2)}$, we have

$$X \ll q^{d(N-\deg h)}\cdot N^{-2^{d-1}\sigma_0-(2^{d-1}-d)\sigma_3}.$$

Therefore from (43) and $\sigma_3 \ge 0$, we obtain

$$|\, S_h(f,N)\,|^{2^{d-1}} \ll q^{2^{d-1}(N-\deg h)}\cdot N^{-2^{d-1}\sigma_0-(2^{d-1}-d)\sigma_3}$$
$$\ll q^{2^{d-1}(N-\deg h)}\cdot N^{-2^{d-1}\sigma_0}.$$

This implies that

$$| S_h(f,N) | \ll \frac{q^{N-\deg h}}{N^{\sigma_0}},$$

where the implied constant depends only on d, σ_0, σ_3, and q. □

Let $1 \le i \le N - \deg h$, let X_i be a set of monic polynomials of degree i, and let X_i' be a set of monic polynomials of degree $N - \deg h - i$. Then we set

$$\Omega_{h,X_i} = \sum_{x \in X_i} \sum_{z \in X_i'} E(f(hxz))$$

Lemma 11.7. *Suppose that $2 \le d < p, \sigma_0, \sigma_3, \sigma_5 \ge 0$, $h \in \mathbf{A}_+$ satisfies $\deg h \le \min\{N, \sigma_3 \ln N\}$, $\sigma \ln N \le \deg Q \le dN - \sigma \ln N$ and $\sigma_5 \ln N \le i \le N - \sigma_6 \ln N$, where $\sigma_5 \ge 2^{2d}\sigma_0, \sigma_6 \ge (2d+1)\sigma_3 + 2^{2d+1}\sigma_0 + 2^{3(2d-1)}$. Then when $\sigma \ge 2d\sigma_3 + 2^{2d+1}\sigma_0 + 2^{3(2d-1)}$, we have*

$$\Omega_{h,X_i} \ll \frac{q^{N-\deg h}}{N^{\sigma_0}},$$

where the implied constant depends only on $d, \sigma_0, \sigma_3, \sigma_5, \sigma_6$, and q.

Proof. By Cauchy inequality, we know that

$$\begin{aligned}
|\Omega_{h,X_i}|^2 &\le q^i \sum_{x \in X_i} \Big| \sum_{z \in X_i'} E(f(hxz)) \Big|^2 \\
&\le q^i \sum_{\substack{x \in \mathbf{A}_+ \\ \deg x = i}} \Big| \sum_{z \in X_i'} E(f(hxz)) \Big|^2 \\
&= q^i \sum_{\substack{x \in \mathbf{A}_+ \\ \deg x = i}} \sum_{z_1, z_2 \in X_i'} E\left(\frac{a}{Q} h^d x^d (z_1^d - z_2^d) + \cdots \right) \qquad (44) \\
&\le q^i \sum_{\substack{z_1, z_2 \in \mathbf{A}_+ \\ \deg z_j = N - \deg h - i}} |S_{z_1,z_2}|,
\end{aligned}$$

where

$$S_{z_1,z_2} = \sum_{\substack{x \in \mathbf{A}_+ \\ \deg x = i}} E(f_1(x)),$$
$$f_1(x) = f(hxz_1) - f(hxz_2).$$

Applying lemma 11.5 for $f_1(x)$ with $v = d$, since

$$\Delta_{a_1,\cdots,a_d} f_1(x) = \frac{a}{Q} h^d (z_1^d - z_2^d) d! a_1 \cdots a_d,$$

we obtain

$$|S_{z_1,z_2}|^{2^d} \le q^{i(2^d-d-1)} \sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}} \sum_{\substack{x\in\mathbf{A}_+\\ \deg x=i}} E\left(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\right)$$
$$= q^{i(2^d-d)} \sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}} E\left(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\right).$$

Therefore

$$\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} |S_{z_1,z_2}|^{2^d}$$
$$\le q^{i(2^d-d)} \sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}} \Big| \sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} E\left(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\right)\Big|. \tag{45}$$

By Hölder inequality ($d\ge 2$), we have

$$\left(\sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}} \Big| \sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} E\big(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\big)\Big|\right)^{2^{d-1}}$$
$$\le q^{id(2^{d-1}-1)} \sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}} \Big| \sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} E\left(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\right)\Big|^{2^{d-1}}. \tag{46}$$

Again applying lemma 11.5 for $v=d-1$ and

$$f_2(z_1)=\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d,$$

as in the proof of lemma 11.6, we obtain

$$\Big| \sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} E\left(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\right)\Big|^{2^{d-1}} \le q^{(N-\deg h-i)(2^{d-1}-d)}\times$$
$$\sum_{\substack{w_1,\cdots,w_{d-1}\in\mathbf{A}\\ \deg w_j<N-\deg h-i}} \Big| \sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} E\left(\frac{a}{Q}h^d(d!)^2a_1\cdots a_dw_1\cdots w_{d-1}z_1\right)\Big|.$$

Combining this inequality with (46), we obtain

(47)
$$\Bigg(\sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}}\Big|\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}}E\big(\frac{a}{Q}h^d(z_1^d-z_2^d)d!a_1\cdots a_d\big)\Big|\Bigg)^{2^{d-1}}$$
$$\le q^{id(2^{d-1}-1)}q^{(N-\deg h-i)(2^{d-1}-d)}\sum_{\substack{a_1,\cdots,a_d\in\mathbf{A}\\ \deg a_j<i}}$$
$$\sum_{\substack{w_1,\cdots,w_{d-1}\in\mathbf{A}\\ \deg w_j<N-\deg h-i}}\Big|\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}}E\left(\frac{a}{Q}h^d(d!)^2a_1\cdots a_dw_1\cdots w_{d-1}z_1\right)\Big|.$$

The sum of the terms in this sum satisfying $a_1\cdots a_dw_1\cdots w_{d-1}=0$ is

(48)
$$\begin{aligned}&\ll q^{id(2^{d-1}-1)}q^{(N-\deg h-i)(2^{d-1}-d)}\cdot q^{id}\cdot q^{(N-\deg h-i)(d-1)}\times\\ &\quad\left(\frac{1}{q^i}+\frac{1}{q^{N-\deg h-i}}\right)\cdot q^{N-\deg h-i}\\ &\ll q^{id2^{d-1}}q^{(N-\deg h-i)2^{d-1}}(N^{-\sigma_5}+N^{\sigma_3-\sigma_6}).\end{aligned}$$

Since

$$\deg(h^da_1\cdots a_dw_1\cdots w_{d-1})<i+\deg h+(d-1)N\overset{\text{def}}{=}d_0,$$

we have

$$\begin{aligned}X&\overset{\text{def}}{=}\sum_{\substack{a_1,\cdots,a_d\in\mathbf{A},a_j\ne0\\ \deg a_j<i}}\sum_{\substack{w_1,\cdots,w_{d-1}\in\mathbf{A},w_j\ne0\\ \deg w_j<N-\deg h-i}}\\ &\quad\Big|\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}}E\left(\frac{a}{Q}h^d(d!)^2a_1\cdots a_dw_1\cdots w_{d-1}z_1\right)\Big|\\ &\ll\sum_{z\in\mathbf{A}_+,\deg z\le d_0}\tau_{2d-1}(z)\Big|\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}}E\big(\frac{a\cdot z\cdot z_1}{Q}\big)\Big|\end{aligned}$$

By lemma 11.4 and lemma 11.2 (removing $(d!)^2$), if $\sigma_2 \geq 2^{3(2d-1)} - 1$, then we have

$$X \ll \frac{q^{d_0}}{N^{\sigma_2}} \cdot q^{N-\deg h-i} + N^{\sigma_2} \sum_{\deg z \leq d_0} \Big| \sum_{z_1 \in \mathbf{A}_+, \deg z_1 = N-\deg h-i} E\big(\frac{a \cdot z \cdot z_1}{Q}\big)\Big|$$

by $(Q, a) = 1$

$$\ll \frac{q^{dN}}{N^{\sigma_2}} + N^{\sigma_2} \max\big\{1, \frac{q^{d_0}}{q^{\deg Q}}\big\} \sum_{\deg z < \deg Q} \Big| \sum_{\substack{z_1 \in \mathbf{A}_+ \\ \deg z_1 = N-\deg h-i}} E\big(\frac{z \cdot z_1}{Q}\big)\Big|$$

again by lemma 11.2

$$\ll \frac{q^{dN}}{N^{\sigma_2}} + N^{\sigma_2} \max\big\{1, \frac{q^{d_0}}{q^{\deg Q}}\big\} \cdot \max\big\{1, \frac{q^{\deg Q}}{q^{N-\deg h-i}}\big\} \cdot q^{N-\deg h-i}$$

by $\deg h \leq \sigma_3 \ln N, \sigma \ln N \leq \deg Q \leq dN - \sigma \ln N$, and $i \leq N - \sigma_6 \ln N$

$$\ll q^{d(N-\deg h)}(N^{d\sigma_3-\sigma_2} + N^{\sigma_2+d\sigma_3-\sigma} + N^{\sigma_2+(d+1)\sigma_3-\sigma_6}).$$

Combining this with (47) and (48), we get

$$\Bigg(\sum_{\substack{a_1,\cdots,a_d \in \mathbf{A} \\ \deg a_j < i}} \Big| \sum_{\substack{z_1 \in \mathbf{A}_+ \\ \deg z_1 = N-\deg h-i}} E\big(\frac{a}{Q} h^d (z_1^d - z_2^d) d! a_1 \cdots a_d\big)\Big|\Bigg)^{2^{d-1}}$$
$$\ll q^{id2^{d-1}} q^{(N-\deg h-i)2^{d-1}} (N^{-\sigma_5} + N^{\sigma_3-\sigma_6} + N^{d\sigma_3-\sigma_2} + N^{\sigma_2+d\sigma_3-\sigma} + N^{\sigma_2+(d+1)\sigma_3-\sigma_6}).$$

Taking

$$\sigma_2 = d\sigma_3 + 2^{2d}\sigma_0 + 2^{3(2d-1)} - 1.$$

Since

$$\sigma_5 \geq 2^{2d}\sigma_0, \sigma_6 \geq (2d+1)\sigma_3 + 2^{2d+1}\sigma_0 + 2^{3(2d-1)}$$

and

$$\sigma \geq 2d\sigma_3 + 2^{2d+1}\sigma_0 + 2^{3(2d-1)},$$

we obtain

$$\sum_{\substack{a_1,\cdots,a_d \in \mathbf{A} \\ \deg a_j < i}} \Big| \sum_{\substack{z_1 \in \mathbf{A}_+ \\ \deg z_1 = N-\deg h-i}} E\big(\frac{a}{Q} h^d (z_1^d - z_2^d) d! a_1 \cdots a_d\big)\Big| \ll \frac{q^{id+(N-\deg h-i)}}{N^{2^{d+1}\sigma_0}}.$$

By (45), we obtain

$$\sum_{\substack{z_1 \in \mathbf{A}_+ \\ \deg z_1 = N-\deg h-i}} |S_{z_1,z_2}|^{2^d} \ll \frac{q^{i2^d+(N-\deg h-i)}}{N^{2^{d+1}\sigma_0}}.$$

Using Hölder inequality, we obtain

$$\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} |S_{z_1,z_2}| \le q^{(N-\deg h-i)(1-\frac{1}{2^d})}\Big(\sum_{\substack{z_1\in\mathbf{A}_+\\ \deg z_1=N-\deg h-i}} |S_{z_1,z_2}|^{2^d}\Big)^{2^{-d}} \ll \frac{q^{N-\deg h}}{N^{2\sigma_0}}.$$

By (44), we obtain

$$|\Omega_{h,X_i}|^2 \ll q^i\cdot q^{N-\deg h-i}\cdot\frac{q^{N-\deg h}}{N^{2\sigma_0}} \ll \frac{q^{2(N-\deg h)}}{N^{2\sigma_0}}.$$

This completes the proof. □

We define

$$S'(f,N)=\sum_{\deg P=N}{}' E(f(P)),$$

where $\sum'$ denotes the sum over monic irreducible polynomials in $\mathbf{A}$. Then we have

Theorem 11.8. *Let $2\le d<p$ and let $\sigma_0\ge 0$ be a real number. Suppose that $\sigma\ln N\le\deg Q\le dN-\sigma\ln N$. Then, when $\sigma\ge d2^{6d}(\sigma_0+1)$, we have*

$$|\ S'(f,N)\ |\ll\frac{q^N}{N^{\sigma_0}},$$

where the implied constant depends only on d,σ_0, and q.

Proof. Let D be the product of all monic irreducible polynomials P in $\mathbf{A}$ satisfying $\deg P\le N/2$, let H be the set of monic divisors of D, and let H_0 (resp. H_1) the subset of H consisting of $h\in H$ satisfying $\mu(h)=1$ (resp. $\mu(h)=-1$), where μ is the polynomial möbius function. Let S_i be the set of $h\in H_0$ satisfying $\deg h=i$.

We note that

$$S'(f,N)=\sum_{h\in H,\deg h\le N}\mu(h)S_h(f,N).$$

Let us first estimate the value of

$$X_0=\sum_{h\in H,\deg h\le\lambda_1\ln N} S_h(f,N),$$

where $\lambda_1=2^{2d}(\sigma_0+1)$. Taking $\sigma_3=\lambda_1$ in lemma 11.6 and substituting σ_0+1 for σ_0, we obtain

$$|S_h(f,N)|\ll\frac{q^{N-\deg h}}{N^{\sigma_0+1}}.$$

Therefore

$$X_0\ll\sum_{h\in H,\deg h\le\lambda_1\ln N}\frac{q^{N-\deg h}}{N^{\sigma_0+1}}\ll\frac{q^N}{N^{\sigma_0}}. \tag{49}$$

Let

$$Y = \sum_{\substack{h\in H\\ \lambda_1 \ln N<\deg h\le N}} \mu(h)S_h(f,N) = Y_0 - Y_1,$$

where

$$Y_0 = \sum_{\substack{h\in H_0\\ \lambda_1 \ln N<\deg h\le N}} S_h(f,N), \quad Y_1 = \sum_{\substack{h\in H_1\\ \lambda_1 \ln N<\deg h\le N}} S_h(f,N).$$

Now we shall confine ourselves to the study of Y_0, since the same method can be applied to Y_1. Let

$$\begin{aligned} Y_0' &= \sum_{\substack{h\in H_0\\ \lambda_1 \ln N<\deg h\le N-\lambda_2 \ln N}} S_h(f,N) \\ &= \sum_{\lambda_1 \ln N<i\le N-\lambda_2 \ln N} \Omega_{1,S_i}, \end{aligned}$$

where $\lambda_2 = 2^{2d+1}(\sigma_0+1) + 2^{3(2d-1)}$ and Ω_{1,S_i} is defined in lemma 11.7 by taking $S_i' = \{x \in \mathbf{A}_+ \mid \deg x = N-i\}$. If $\lambda_1 \ln N < i \le N - \lambda_2 \ln N$, then taking $\sigma_3 = 0, \sigma_5 = \lambda_1, \sigma_6 = \lambda_2$ in lemma 11.7 and substituting $\sigma_0 + 1$ for σ_0, we obtain

$$\Omega_{1,S_i} \ll \frac{q^N}{N^{\sigma_0+1}}.$$

Therefore

$$Y_0' \ll \frac{q^N}{N^{\sigma_0}}. \tag{50}$$

The part of the sum which remains to be considered is

$$Y_0'' = \sum_{\substack{h\in H_0\\ N-\lambda_2 \ln N<\deg h\le N}} S_h(f,N) = \sum_{0\le i<\lambda_2 \ln N} Y_0(i), \tag{51}$$

where

$$Y_0(i) = \sum_{y\in\mathbf{A}_+,\deg y=i} \sum_{h\in S_{N-i}} E(f(hy)).$$

Let S_{N-i}' denote the subset of S_{N-i} consisting of the polynomials which have irreducible factors P satisfying $\deg P \ge \lambda_3 \ln N$, where $\lambda_3 = \sigma_0 + \lambda_2$. Let S_{N-i}'' be the set of $h \in S_{N-i}$, but $h \notin S_{N-i}'$. Then

$$Y_0(i) = Y_0'(i) + Y_0''(i), \tag{52}$$

where

$$\begin{aligned} Y_0'(i) &= \sum_{y\in\mathbf{A}_+,\deg y=i} \sum_{h\in S_{N-i}'} E(f(hy)), \\ Y_0''(i) &= \sum_{y\in\mathbf{A}_+,\deg y=i} \sum_{h\in S_{N-i}''} E(f(hy)). \end{aligned}$$

Estimating $Y_0''(i)$, let $0 \le i < \lambda_2 \ln N$. If $h \in S''_{N-i}$, then $\deg h = N - i \ge N/2$ for large N (depending on d and σ_0), h is square free, and $\deg P < \lambda_3 \ln N$ for any irreducible factor P of h. Suppose $\tau_1(h) = 2^s$, i.e., s is the number of monic irreducible factors of h. Then we have $N/2 \le \deg h \le s\lambda_3 \ln N$. Hence $s \ge N/(2\lambda_3 \ln N)$. This implies that

$$\tau_1(h) = 2^s \ge 2^{\frac{N}{2\lambda_3 \ln N}} \gg N^{\lambda_3+1}.$$

By lemma 11.3, we obtain

$$|S''_{N-i}| N^{\lambda_3+1} \ll \sum_{h \in \mathbf{A}_+, \deg h = N-i} \tau_1(h) \ll N q^{N-i},$$

where $|S''_{N-i}|$ denotes the cardinality of $|S''_{N-i}|$. Therefore, by $\lambda_3 \ge \sigma_0 + 1$ and trivial estimate, we obtain

$$\sum_{0 \le i < \lambda_2 \ln N} Y_0''(i) \ll \sum_{0 \le i < \lambda_2 \ln N} q^i \cdot \frac{N \cdot q^{N-i}}{N^{\lambda_3+1}} \ll \frac{q^N}{N^{\sigma_0}}. \tag{53}$$

Let $S'_{N-i}(s)$ denote the subset of S'_{N-i} whose elements contain exactly s monic irreducible factors with degree $\ge \lambda_3 \ln N$. If $h \in S'_{N-i}(s)$ and $N \ge 3$, then since $s\lambda_3 \ln N \le N - i$, $s < N$. Hence

$$Y_0'(i) = \sum_{s < N} Y'_{0,s}(i), \tag{54}$$

where

$$Y'_{0,s}(i) = \sum_{y \in \mathbf{A}_+, \deg y = i} \sum_{h \in S'_{N-i}(s)} E(f(hy)).$$

In order to estimate $Y'_{0,s}(i)$, we define

$$Z_s(i) = \sum_{y \in \mathbf{A}_+, \deg y = i} {\sum_{\substack{P \in H \\ \deg P \ge \lambda_3 \ln N}}}' \sum_{v \in S'_{N-i-\deg P}(s-1)} E(f(Pvy)),$$

where $\sum'$ denotes the sum over monic irreducible polynomials in $\mathbf{A}$. Since $0 \le i < \lambda_2 \ln N < \lambda_3 \ln N$, we obtain that for each Pvy in the above

equation, $P \nmid y$ and $P^2 \nmid v$ because v is square free. Thus we obtain

$$Z_s(i) = sY'_{0,s}(i) + \sum_{y\in\mathbf{A}_+,\deg y=i} \sideset{}{'}\sum_{\substack{P\in H\\ \deg P\geq\lambda_3\ln N}} \sum_{Pv\in S'_{N-i-\deg P}(s-1)} E(f(P^2vy))$$

Since each element in $S'_{N-i-\deg P}(s-1)$ is square free and $i < \lambda_3 \ln N$, we get

$$\begin{aligned} &= sY'_{0,s}(i) + O\left(q^i \sum_{\lambda_3\ln N\leq j} \frac{q^j}{j}\cdot q^{N-i-2j}\right) \\ &= sY'_{0,s}(i) + O\big(\frac{q^N}{i\cdot N^{\lambda_3}}\big). \end{aligned}$$

Therefore

$$Y'_{0,s}(i) = \frac{Z_s(i)}{s} + O\big(\frac{q^N}{s\cdot N^{\lambda_3}}\big). \tag{55}$$

We apply lemma 11.7 to estimate $Z_s(i)$. Let X_j denote the set of monic irreducible polynomials $P \in H$ with $\deg P = j$, and let $X'_j = S'_{N-i-j}(s-1)$. Since each irreducible polynomial P in H have $\deg P \leq N/2$, we obtain

$$Z_s(i) = \sum_{\lambda_3\ln N\leq j\leq N/2} \sum_{y\in\mathbf{A}_+,\deg y=i} \Omega_{y,X_j}.$$

Now in lemma 11.7 take $h = y, \sigma_3 = \lambda_2, \sigma_5 = \lambda_3$, and take σ_6 to be an arbitrarily large integer (depending on d and σ_0). Also, substitute $\sigma_0 + 2$ for σ_0. Then from

$$\begin{aligned} \deg h = \deg y = i < \lambda_2\ln N = \sigma_3\ln N,\\ \lambda_3\ln N \leq j \leq N/2 \leq N - \sigma_6\ln N(\text{ for large } N),\\ \sigma_5 = \lambda_3 = \sigma_0 + \lambda_2 = \sigma_0 + 2^{2d+1}(\sigma_0+1) + 2^{3(2d-1)} \geq 2^{2d}(\sigma_0+2),\\ \sigma \geq d2^{6d}(\sigma_0+1), \end{aligned}$$

we obtain

$$Z_s(i) = \sum_{\lambda_3\ln N\leq j\leq N/2} \sum_{y\in\mathbf{A}_+,\deg y=i} \Omega_{y,X_j} \ll \frac{N}{2}\cdot q^i\cdot\frac{q^{N-i}}{N^{\sigma_0+2}} \ll \frac{q^N}{N^{\sigma_0+1}}.$$

Combining this with (55), (54), and $\lambda_3 \geq \sigma_0 + 1$, we obtain

$$Y'_0(i) = \sum_{s<N} \frac{Z_s(i)}{s} + O\big(\frac{q^N}{s\cdot N^{\sigma_3}}\big) \ll \frac{q^N}{N^{\sigma_0+1}}\cdot\ln N.$$

Therefore

$$\sum_{0\leq i<\lambda_2\ln N} Y'_0(i) \ll \frac{q^N}{N^{\sigma_0+1}}\cdot\ln N\cdot\lambda_2\ln N \ll \frac{q^N}{N^{\sigma_0}}. \tag{56}$$

Combining (51), (52), (53), and (56), we obtain

$$Y_0'' \ll \frac{q^N}{N^{\sigma_0}}.$$

This completes the proof. □

References

[1] M. Car, Arithmétique additive dans l'anneau des polynômes à une indéterminée sur un corps fini, Thèse soutenue à l'Université de Provence, (1972).

[2] L. Carlitz, The arithmetic of polynomials in a Galois field, *Am. J. Math.*, 54 (1932), 39–50.

[3] G. T. Diderrich and H. B. Mann, Representations by k-th powers in $GF(q)$, Journal of Number Theory, 4 (1972), 269–273.

[4] G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field*, Oxford, Clarendon Press (1991).

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, Clarendon Press (1945).

[6] D. R. Hayes, The expression of a polynomial as the sum of three irreducibles, *Acta Arith.* 11 (1966), 461–488.

[7] C. N. Hsu, The Distribution of Irreducible Polynomials in $\mathbb{F}_q[t]$, Journal of Number Theory, 61 (1996), 85–96.

[8] C. N. Hsu, Diophantine Inequalities for Polynomial Rings, to appear in *Journal of Number Theory*.

[9] C. N. Hsu, On Hardy-Littlewood method for non-Archimedean line, preprint.

[10] L. K. Hua, On exponential sums, *J. Chinese Math. Soc.*, 2(1940), 301–312.

[11] L. K. Hua, *Additive Theory of Prime Numbers*, American Mathematical Society (1965).

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press (1997).

[13] M. B. Nathanson, *Additive Number Theory (the classical bases)*, GTM 164 (1996).

[14] M. B. Nathanson, *Additive Number Theory (inverse problems and the geometry of sumsets)*, GTM 165 (1996).

[15] S. Schwarz, On Waring's problem for finite fields, *Quart. Joun. Math.*, 19(1948), 123–128.

[16] S. A. Stepanow, *Arithmetic of Algebraic Curves*, Translated from Russian by Irene Aleksanova, Consultants Bureau, New York (1994).

[17] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press (1997) .

[18] W. A. Webb, Waring Problem in $GF[q, x]$, *Acta Arithmetica*, 22 (1973), 207–220.

Chih-Nung Hsu

Department of Mathematics, National Taiwan Normal University, 88 Sec. 4 Ting-Chou Road, Taipei, **Taiwan**

E-mail address: maco@math.ntnu.edu.tw