1-1-2020

Topics In Analytic And Combinatorial Number Theory

Zhenchao Ge

TOPICS IN ANALYTIC AND COMBINATORIAL NUMBER THEORY

DISSERTATION

A Dissertation
presented in partial fulfillment of requirements
for the degree of Doctor of Philosophy
in the Department of Mathematics
The University of Mississippi

by

ZHENCHAO GE

May 2020

ABSTRACT

In this dissertation, I introduce some results that I have proved (collaboratively and independently) in analytic number theory and additive combinatorics. In analytic number theory, I study certain continuous and discrete mean value estimates for the Z-function associated to a Dirichlet L-functions. These problems lead naturally to an investigation of certain Gauss type sums which are studied in some depth. This is joint work with Jonathan W. Bober and Micah B. Milinovich. In additive combinatorics, I study two problems on sumsets. This is joint work with Thái Hoàng Lê.

ACKNOWLEDGEMENTS

First I would like thank my supervisors, Proferssors Micah Milinovich and Thái Hoàng Lê for their consistent support and guidance in the past 6 years. Their insight and knowledge steered me through the research.

I am grateful to all faculty members in the Department of Mathematics at the University of Mississippi who have helped and mentored me in graduate studies, research, teaching, and job searching. I would like to thank Prof. James Reid for allowing me to postpone my graduation and funded me for one more year. I would like to thank my Graduate Program Coordinator, Prof. Bing Wei, for his continuous help and encouragement.

A special thank to Professors Jonathan W. Bober and Paul Pollack for their inspiration and support in my research.

Finally, I would like to thank all my committee members: Professors Kevin Beach, Erwin Miña Díaz, Ayla Gafni, and Rizwanur Khan for generously offering their time, support, and guidance.

TABLE OF CONTENTS

1 INTRODUCTION

In this dissertation, I introduce some of the results that I have proved (collaboratively and independently) in analytic number theory and additive combinatorics. The two problems on Z-functions are joint work with Micah B. Milinovich and Jonathan W. Bober. The two problems on essential components are joint work with Thái Hoàng Lê.

1.1 The Hardy Z-function

Let s be a complex variable and following the traditional notation let $s = \sigma + it$. The *Riemann zeta-function* is initially defined as

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \tag{1.1}$$

for $\sigma > 1$. By the unique factorization of $\mathbb{Z}$, one can express $\zeta(s)$ as

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1} \tag{1.2}$$

for $\sigma > 1$, which is known as the *Euler product*. In 1860, Riemann (in his only paper on number theory) showed that the key to the investigation of the distribution of the primes lies in the study of $\zeta(s)$. He proved that $\zeta(s)$ can be continued analytically

to $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$. Moreover, he gave two proofs that $\zeta(s)$ satisfies the *functional equation*

$$\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s) = \pi^{-\frac{1}{2}(1-s)}\Gamma(\tfrac{1}{2}(1-s))\zeta(1-s). \tag{1.3}$$

From the poles of $\Gamma(s)$ at $s = 0, -1, -2, -3, \ldots$, Riemann observed that $\zeta(s)$ has simple zeros at $s = -2, -4, -6, \cdots$. These are called the *trivial zeros* of the zeta function. He further noted that $\zeta(s)$ has infinitely many zeros in the *critical strip*, $0 \leq \sigma \leq 1$, which are known as the *non-trivial zeros* of $\zeta(s)$. Riemann made the following now famous conjecture about these non-trivial zeros.

Riemann Hypothesis. All zeros of $\zeta(s)$ in the critical strip lie on the *critical line* $\sigma = \frac{1}{2}$.

This conjecture is widely considered to be among the most important problems in pure mathematics.

Rewriting the functional equation in an asymmetric form as

$$\zeta(s) = G(s)\zeta(1-s) \qquad \text{where} \qquad G(s) = \pi^{s-1/2}\frac{\Gamma(\frac{1}{2}(1-s))}{\Gamma(\frac{1}{2}s)}, \tag{1.4}$$

we observe that

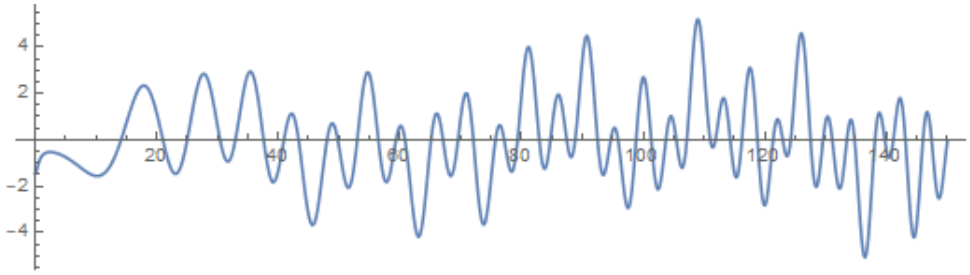
$$G(s) = \frac{1}{G(1-s)} \text{ for } s \in \mathbb{C} \text{ and } |G(\tfrac{1}{2}+it)| = 1 \text{ for } t \in \mathbb{R}.$$

With these observations in mind, Hardy defined the function

$$Z(t) = G(\tfrac{1}{2}-it)^{1/2}\zeta(\tfrac{1}{2}+it) \tag{1.5}$$

now known as Hardy's Z-function (also known as Riemann-Siegel Z-function). From the definition, we deduce that $\overline{Z(t)} = Z(t)$, so that $Z(t)$ is real-valued for real t. It is

also clear that $|\zeta(\frac{1}{2}+it)| = |Z(t)|$. Moreover, sign changes of $Z(t)$ correspond to zeros of $\zeta(s)$ on the critical line of odd multiplicity. It is conjectured that all non-trivial zeros are simple, but this is a well-known open problem.



A plot of $Z(t)$ for $0 \leq t \leq 150$

These and other properties of the Hardy Z-function make it a powerful tool in the study of the zero distribution of $\zeta(s)$, because in contrast to the difficult problem of finding zeros of a complex-valued function, it is much easier to detect sign changes of a continuous real-valued function. By investigating sign changes of $Z(t)$, Hardy [15] proved a partial Riemann Hypothesis.

Theorem. (Hardy, 1914) *There are infinitely many zeros of $\zeta(s)$ on the critical line $\sigma = \frac{1}{2}$.*

The idea of Hardy's proof is simple to explain. He showed that

$$\left| \int_0^T Z(t)dt \right| = o(T) \quad \text{and} \quad \int_0^T |Z(t)|dt \geq C \cdot T$$

for some $C > 0$ as $T \to \infty$. This implies that $Z(t)$ cannot be of constant sign from some point on, so $Z(t)$ has infinitely many sign changes. Developing new tools for studying sign changes of $Z(t)$, Selberg proved the following stronger result.

Theorem. (Selberg, 1942) *The Riemann zeta-function has at least $cT \log T$ zeros on the critical line up to height T, for some positive absolute constant c.*

Since $\zeta(s)$ has roughly $\frac{T}{2\pi}\log T$ non-trivial zeros with imaginary part in the interval $[0,T]$, Selberg's result can be interpreted as saying that a positive proportion of the nontrivial zeros of $\zeta(s)$ are on the critical line. In other words, the Riemann Hypothesis is true a positive percentage of the time.

These results motivate studying the integral

$$\int_0^T Z(t)dt.$$

From the oscillations of $Z(t)$, one might guess that the integral is probably quite small (as a function of T). Note that an estimate of the form $\int_0^T Z(t)dt = O(T^{1-\theta})$ for any $\theta > 0$ implies Hardy's Theorem. A classical estimate of Hardy and Littlewood implies that $\int_0^T Z(t)dt = O(T^{\frac{7}{8}})$ (see [37, Eq. (10.5.1)]). More recently, A. Ivić [16] substantially improved this classical estimate.

Theorem. (Ivić, 2004) *For any $\varepsilon > 0$, we have*

$$\int_0^T Z(t)dt = O_\varepsilon(T^{\frac{1}{4}+\varepsilon}) \tag{1.6}$$

as $T \to \infty$.

In the same paper, Ivić made the following conjecture about the behavior of this integral.

Conjecture. (Ivić [16]) *As $T \to \infty$, we have*

$$\int_0^T Z(t)dt = \Omega_\pm(T^{1/4}) \quad \textit{and} \quad \int_0^T Z(t)dt = O(T^{1/4}). \tag{1.7}$$

Here $f(x) = \Omega_+(g(x))$ if $\limsup \frac{f(x)}{g(x)} > 0$ and $f(x) = \Omega_-(g(x))$ if $\liminf \frac{f(x)}{g(x)} < 0$. Recently, this conjecture was established independently by M. A. Korolev [23] and M. Jutila [20, 21] using different methods.

Theorem. (Korolev, 2007 & Jutila, 2009) Ivić's conjecture is true.

There are many functions in number theory that generalize the Riemann zeta-function, for instance Dirichlet L-functions and the L-functions associated to an elliptic curve over $\mathbb{Q}$. A main result of this thesis is to prove that the analogue of Ivić's conjecture is **not** true for all L-functions.

1.2 The Z-function associated to a primitive Dirichlet L-function

All results in this section are joint work with Jonathan W. Bober and Micah B. Milinovich.

Let χ be a primitive character modulo q and $\mathfrak{a} \in \{0, 1\}$ such that $\chi(-1) = (-1)^{\mathfrak{a}}$. The *Dirichlet L-function* is defined as

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

for $\mathrm{Re}(s) > 1$. Similar to the Riemann zeta-function, $L(s, \chi)$ also satisfies a functional equation

$$L(s, \chi) = G_\chi(s) L(1 - s, \overline{\chi})$$

for

$$G_\chi(s) = \epsilon_\chi q^{1/2-s} \pi^{-1/2+s} \frac{\Gamma(\frac{1}{2}(1 - s + \mathfrak{a}))}{\Gamma(\frac{1}{2}(s + \mathfrak{a}))}.$$

Here, $\epsilon_\chi = \frac{\tau(\chi)}{i^{\mathfrak{a}} q^{1/2}}$ is the *root number* and $\tau(\chi) = \sum_{n=1}^{q} \chi(n) e(n/q)$ for $e(x) = e^{2\pi i x}$ is the *Gauss sum* of χ.

The Z-function associated to χ is defined as

$$Z_\chi(t) = G_\chi(\tfrac{1}{2}+it)^{-1/2}L(\tfrac{1}{2}+it,\chi).$$

Similarly, from the definition, we can deduce that $\overline{Z_\chi(t)} = Z_\chi(t)$ for all real t, $|L(\frac{1}{2}+it,\chi)| = |Z_\chi(t)|$, and the sign changes of $Z_\chi(t)$ correspond to zeros of $L(s,\chi)$ on the critical line of odd multiplicity.

Given Ivić's conjecture, one expects that

$$\int_0^T Z_\chi(t)\mathrm{d}t = O(T^{\frac{1}{4}}) \qquad \text{and} \qquad \int_0^T Z_\chi(t)\mathrm{d}t = \Omega_\pm(T^{\frac{1}{4}}),$$

where the implied constant depends on q. We have proved that there are infinitely many primitive characters for which this fails.

Theorem 1.2.1. *Let χ be a primitive Dirichlet character modulo q. For large T we have*

$$\int_0^T Z_\chi(t)\mathrm{d}t = C_\chi T^{\frac{3}{4}} + O_q(T^{\frac{1}{4}}\log T),$$

where

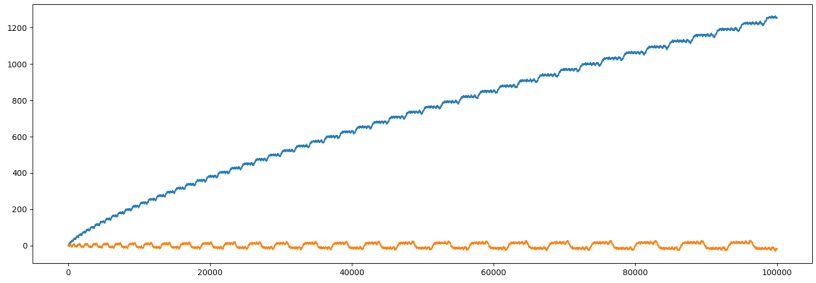
$$C_\chi = \frac{2^{\frac{3}{4}}\pi^{\frac{1}{4}}e(\frac{1}{16})}{3\,q^{\frac{1}{2}}\tau(\chi)^{\frac{1}{2}}}S_1(\chi), \qquad \textit{and} \qquad S_1(\chi) = \sum_{n=1}^{2q}\chi(n)e\left(\frac{-n^2}{2q}\right).$$

Moreover, there are infinitely many primitive Dirichlet characters χ for which $S_1(\chi) \neq 0$.

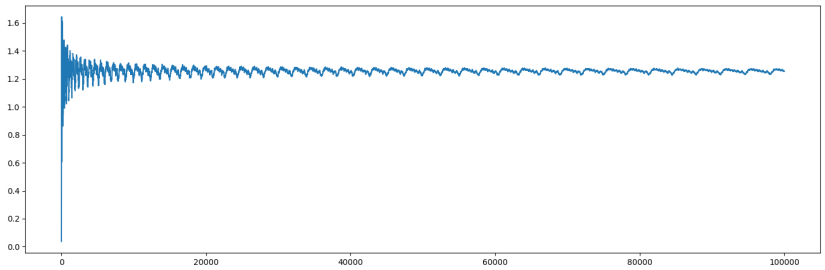
Example 1. *Let χ_1 and χ_2 be the odd and even primitive characters* (mod 8)*, respectively. Then we have*

$$I_1(T) = \int_0^T Z_{\chi_1}(t)\mathrm{d}t = O(T^{\frac{1}{4}}\log T) \quad \textit{and,}$$
$$I_2(T) = \int_0^T Z_{\chi_2}(t)\mathrm{d}t = \frac{2^{\frac{3}{2}}\pi^{\frac{1}{4}}}{3}T^{\frac{3}{4}} + O(T^{\frac{1}{4}}\log T),$$

where $\frac{2^{\frac{3}{2}}\pi^{\frac{1}{4}}}{3} = 1.255195\ldots$



Plot of $I_1(T)$ in orange and $I_2(T)$ in blue for T up to 100,000 (courtesy of J. W. Bober).



Plot of $I_2(T)/T^{3/4}$ for T up to 100,000 (courtesy of J. W. Bober).

Example 2. *Below is the table of the four primitive characters modulo* 16.

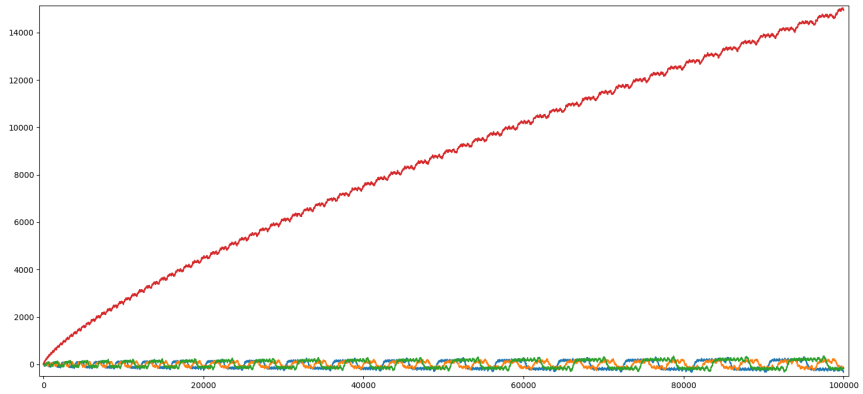
	$\chi(n) \pmod{16}$							
n	1	3	5	7	9	11	13	15
$\chi_1(n)$	1	i	$-i$	-1	-1	$-i$	i	1
$\chi_2(n)$	1	$-i$	i	-1	-1	i	$-i$	1
$\chi_3(n)$	1	i	i	1	-1	$-i$	$-i$	-1
$\chi_4(n)$	1	$-i$	$-i$	1	-1	i	i	-1

Since $S_1(\chi_1) = -16e^{\frac{15}{16}\pi i}$ *and* $S_1(\chi_2) = S_1(\chi_3) = S_1(\chi_4) = 0$, *we have*

$$I_1(T) = \int_0^T Z_{\chi_1}(t)\mathrm{d}t = \frac{2^{\frac{7}{4}}\pi^{\frac{1}{4}}}{3}T^{\frac{3}{4}} + O(T^{\frac{1}{4}}\log T)$$

and

$$I_j(T) = \int_0^T Z_{\chi_j}(t)\mathrm{d}t = O(T^{\frac{1}{4}}\log T), \text{ for } j = 2, 3, 4.$$



Plots of $I_j(T)$ for the four primitive characters (mod 16), $I_1(T)$ in red, for T up to $100,000$ (courtesy of J. Bober).

In Chapter 3, we give a characterization of the primitive Dirichlet characters for which $S_1(\chi) \neq 0$ and our method allows to count the number of such characters. For instance, we prove that if $S_1(\chi) \neq 0$, then the modulus q must be divisible by 8 and χ has to be a square of another character. If we let $\mathcal{S}_Q = \{\chi \pmod q : q \leq Q \text{ and } S_1(\chi) \neq 0\}$, then we show in Theorem 1.4.4 that $|\mathcal{S}_Q| \sim c\frac{Q^2}{\sqrt{\log Q}}$ for some constant $c > 0$ as $Q \to \infty$. Note that there are $\asymp Q^2$ primitive characters $\chi \pmod q$ with $q \leq Q$. Theorem 1.4.4 implies that $S_1(\chi) = 0$ for 100% of primitive characters. Therefore we expect that an analogue of Ivić's conjecture holds 100% of the time, but we have proved that there is an infinite set of primitive characters for which the analogue of Ivić's conjecture does not hold. We propose the following modification of Ivić's conjecture which we expect to hold for every Dirichlet L-function.

Conjecture 1. *For T sufficiently large, we conjecture that*

$$\int_0^T Z_\chi(t)\mathrm{d}t - C_\chi T^{\frac{3}{4}} = O_q(T^{\frac{1}{4}}) \qquad \text{and} \qquad \int_0^T Z_\chi(t)\mathrm{d}t - C_\chi T^{\frac{3}{4}} = \Omega_\pm(T^{\frac{1}{4}}),$$

where C_χ is the constant in Theorem 1.2.1.

I hope to prove Conjecture 1 in the near future using tools of Jutila.

Assuming the generalized Riemann hypothesis (GRH), we denote the nontrivial zeros ρ of $L(s,\chi)$ as $\rho = \frac{1}{2} + i\gamma$. For simplicity, we are suppressing the dependence on χ in the notation. Note that since $|Z_\chi(t)| = |L(\frac{1}{2}+it,\chi)|$, trivially $Z_\chi(\gamma) = 0$ for all zeros ρ. It is a natural question to study the behavior of $Z'_\chi(\gamma)$ averaged over the zeros ρ. Defining the sum

$$S_2(\chi) = \sum_{n=1}^{q} \chi(n)\, e\Big(\frac{-2n^2}{q}\Big)$$

and using similar methods to the proof of Theorem 1.2.1, we have proved the following result.

Theorem 1.2.2. *Assume GRH and let T be large. Then the following formulas hold:*

(i) *When q is odd, we have*

$$\sum_{0<\gamma<T} Z'_\chi(\gamma) = A_\chi \left(\frac{qT}{2\pi}\right)^{\frac{3}{4}} \left(\log\left(\frac{qT}{2\pi}\right) + C_q\right) + O_q(T^{\frac{1}{2}}(\log T)^{\frac{7}{2}}), \tag{1.8}$$

where

$$A_\chi = \mathrm{Re}\Big[ie(\tfrac{1}{16})\tau(\chi)^{-\frac{1}{2}}\chi(2)S_2(\chi)\Big]\,\frac{2^{\frac{3}{2}}\log(2)}{3\,q^{\frac{5}{4}}},\quad C_q = 2C_0 - 5\log(2) - \frac{4}{3} - 2\sum_{p|q}\frac{p\log p}{p-1},$$

and C_0 is Euler's constant. Moreover, there are infinitely many primitive characters χ for which $A_\chi \neq 0$.

(ii) *When q is even, there is no main term and we have*

$$\sum_{0<\gamma<T} Z'_\chi(\gamma) = O_q(T^{\frac{1}{2}}(\log T)^{\frac{7}{2}}). \tag{1.9}$$

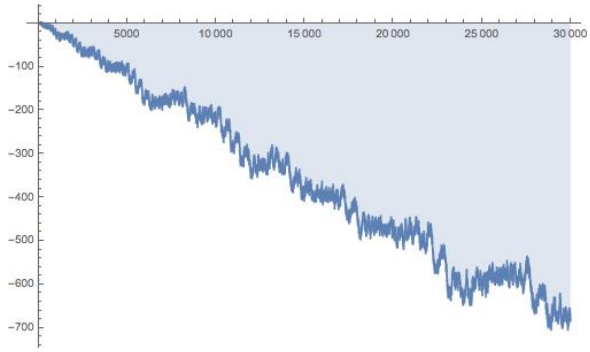
It is interesting to compare and contrast the results in Theorem 1.2.1 and Theorem 1.2.2. If the constant $C_\chi \neq 0$ (in Theorem 1.2.1), then q must be even but if the constant $A_\chi \neq 0$ (in Theorem 1.2.2), then q must be odd! On the other hand, the

sums $S_1(\chi)$ and $S_2(\chi)$ share the following property: if they are nonzero then the character has to be a square.

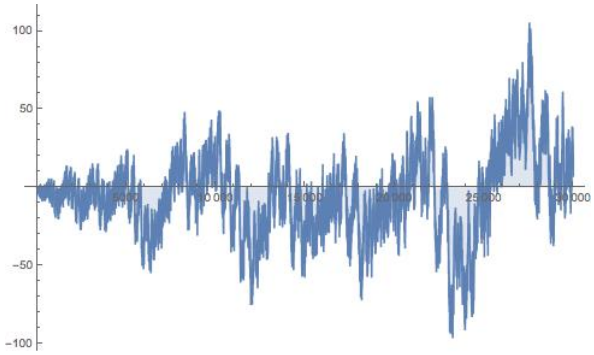
Example 3. *In particular, for Hardy's Z-function, we can use formula* (1.8) *to deduce that*

$$\sum_{0<\gamma<T} Z'(\gamma)$$
$$= -\frac{2^{\frac{3}{2}}\log(2)\sin(\frac{\pi}{8})}{3}\left(\frac{T}{2\pi}\right)^{\frac{3}{4}}\left(\log\left(\frac{T}{2\pi}\right)-\frac{4}{3}+2C_0-5\log(2)\right)+O(T^{\frac{1}{2}}(\log T)^{\frac{7}{2}}),$$

where C_0 is Euler's constant.



Plot of $\sum_{0<\gamma\leq T} Z'(\gamma)$ for T up to 30,000.



Plot of ($\sum_{0<\gamma\leq T} Z'(\gamma) - \textit{Main Terms}$) for T up to 30,000.

1.3 The Z-function associated to a primitive $GL(2)$ L-function

The Riemann zeta-function and Dirichlet L-functions are degree one L-functions, the simplest examples of L-functions. It is natural to ask if there are analogues of the

above theorems for higher degree L-functions. We give some evidence that this is not the case for degree two L-functions (associated to holomorphic modular forms and Maass forms). Using the functional equation for an L-function, $L(s,\pi)$, associated to a cuspidal automorphic representation of $GL_n(\mathbb{A}_{\mathbb{Q}})$, we can define the Z-function, $Z_\pi(t)$, in a usual way.

Theorem 1.3.1. *Let T be large and let π be a cuspidal automorphic representation of $GL_2(\mathbb{A}_{\mathbb{Q}})$. If π is a form for which the Ramanujan-Peterson Conjecture is established, then we have*

$$\int_0^T Z_\pi(t)dt \ll \sqrt{T}\log T.$$

Otherwise, we have

$$\int_0^T Z_\pi(t)dt \ll T^{\frac{11}{20}}\log T.$$

Here, the implied constants depend on the representation.

Note that both integrals are $o(T^{3/4})$, unlike the analogous integrals for $Z_\chi(t)$ where $S_1(\chi)\neq 0$. This indicates the "special" Dirichlet L-functions we have discovered are distinguished among all primitive degree one and degree two L-functions.

1.4 Results on the sums $S_1(\chi)$ and $S_2(\chi)$

Recall that

$$S_1(\chi)=\sum_{n=1}^{2q}\chi(n)\,e\left(\frac{-n^2}{2q}\right), \qquad \text{and} \qquad S_2(\chi)=\sum_{n=1}^{q}\chi(n)\,e\left(\frac{-2n^2}{q}\right),$$

where χ is a primitive character (mod q). In this section, we state the complete criteria of the primitive characters χ for which $S_1(\chi)\neq 0$ and $S_2(\chi)\neq 0$. Furthermore, for a fixed modulus q, we give an exact formula for the number of primitive characters for which $S_1(\chi)\neq 0$, and using this formula, we prove an asymptotic estimate for

the number of primitive characters with modulus less than or equal to Q for which $S_1(\chi)$ does not vanish.

Theorem 1.4.1. *Let χ be a primitive character modulo q, where $q = \prod_p p^{e_p}$ is the factorization of q into prime powers and $\chi = \prod_p \chi_p$ is the factorization of χ into characters of prime-power modulus. Set α_2 to be an integer such that $\chi_2(5) = e(\alpha_2/2^{e_2-2})$, and for each other prime p set α_p to be an integer such that $\chi_p(p+1) = e(\alpha_p/p^{e_p-1})$. Then $S_1(\chi) \neq 0$ if and only if all of the following hold:*

(i) *χ_p is even for each p;*

(ii) *For each odd p with $e_p > 1$, the residue $\alpha_p q/p^{e_p}$ is a square modulo p;*

(iii) *We have $e_2 \geq 3$ (so $8|q$). If $3 \leq e_2 \leq 5$, then $\alpha_2 \equiv 3q/2^{e_2} \pmod{2^{e_2-2}}$ and if $e_2 \geq 6$, then $\alpha_2 \equiv -q/2^{e_2} \pmod 8$.*

In particular, when $q = 8d$ where d is an odd square free number and $3 \nmid d$, we can deduce the following corollary.

Corollary 1.4.2. *Let $q = 8d$ where $d \in \mathbb{N}$ with $\mu^2(6d) = 1$, and let χ be a primitive character* (mod q). *Then $S_1(\chi) \neq 0$ if and only if χ can be expressed as the even primitive character* (mod 8) *times the product of even primitive characters modulo each prime dividing d.*

Using ideas from the proof of Theorem 1.4.1 along with local information modulo prime powers, we can count the number of primitive characters (mod q) such that $S_1(\chi) \neq 0$.
Let

$$N_1(q) := \#\big\{\chi \,(\text{mod } q) : \chi \text{ primitive and } S_1(\chi) \neq 0\big\}. \tag{1.10}$$

Then the following estimate holds.

Theorem 1.4.3. *Let $q \in \mathbb{N}$ be a positive integer such that $8|q$, and either $(q,3)=1$ or $9|q$. Writing $q = 2^m\Big(\prod_i p_i\Big)\Big(\prod_j p_j^{a_j}\Big)$, where p_i, p_j are distinct odd primes, $p_i \geq 5$, $m \geq 3$, and $a_j \geq 2$, we have*

$$N_1(q) = \left\lceil 2^{m-5} \right\rceil \prod_i \left(\frac{p_i - 3}{2}\right) \prod_j \left(\frac{1}{4} p_j^{a_j - 2} \left(p_j - 1\right)^2\right).$$

Note that $\left\lceil 2^{m-5} \right\rceil = 1$ when $m = 3, 4$ and that $\left\lceil 2^{m-5} \right\rceil = 2^{m-5}$ when $m \geq 5$. This formula for $N_1(q)$ allows us to use the Selberg-Delange method to prove the following theorem.

Theorem 1.4.4. *Let $N_1(q)$ be the counting function defined in* (1.10)*. For $Q \geq 3$, we have that*

$$\sum_{q \leq Q} N_1(q) = \frac{\mathscr{A} Q^2}{\sqrt{\log Q}} + O\left(\frac{Q^2}{(\log Q)^{3/2}}\right),$$

where $\mathscr{A} > 0$ is a constant given explicitly in (2.6)*.*

Analogously, we have the following classification for $S_2(\chi) \neq 0$ and q odd.

Theorem 1.4.5. *Let χ be a primitive character modulo q, where q is odd, $q = \prod_p p^{e_p}$ and $\chi = \prod_p \chi_p$ is the factorization of χ into characters of prime-powers modulus. For each p set α_p to be an integer such that $\chi_p(p+1) = e(\alpha_p / p^{e_p - 1})$. Then $S_2(\chi) \neq 0$ if and only if the following holds:*

(i) *χ_p is even for each p;*

(ii) *For each p with $e_p > 1$, the residue $\alpha_p q / p^{e_p}$ is a square modulo p.*

For odd q, let

$$N_2(q) := \{\chi \pmod q : \chi \text{ primitive and } S_2(\chi) \neq 0\}. \tag{1.11}$$

Theorem 1.4.6. *Let q be odd and $N_2(\cdot)$ be the function defined in* (1.11)*. Writing $q = \prod_p p^a$, then we have*

$$N_2(q) = \prod_{p\|q} \frac{p-3}{2} \prod_{\substack{p^a\|q \\ a>1}} \frac{p^{a-2}(p-1)^2}{4}.$$

Comparing the results in Theorem 1.2.1 and Theorem 1.2.2, we have seen that $C_\chi \neq 0$ if and only if $S_1(\chi) \neq 0$ but $S_2(\chi) \neq 0$ does not necessarily imply $A_\chi \neq 0$ unless we can determine the argument of $\chi(2)\tau(\chi)^{-1/2}S_2(\chi)$. In particular, when q is an odd prime we can show $A_\chi \neq 0$ if and only if $S_2(\chi) \neq 0$, by establishing the following proposition.

Theorem 1.4.7. *Let χ be a primitive Dirichlet character modulo p, where p is an odd prime. Let α_p be an integer such that $p \equiv 2\alpha_p + 1 \pmod 8$. Then we have*

$$\chi(2)\tau(\chi)^{-1/2}S_2(\chi) = \pm p^{-1/2}|S_2(\chi)| \cdot e(\alpha_p/8).$$

1.5 Essential components in integers

Throughout, we let $\mathbb{N}$ denote the set of nonnegative integers. Let A, B be subsets of $\mathbb{N}$. The *sum (difference) set* is defined to be

$$A \pm B := \{a \pm b : a \in A, b \in B\}.$$

For $k \in \mathbb{Z}^+$, the *k-fold sum set* is

$$kA = \underbrace{A + \cdots + A}_{k \text{ copies}}.$$

Let $A(n) = \#\{a \in A : 1 \leq a \leq n\}$ be the *counting function* of A. The *Schnirelmann density* of A is defined as

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n},$$

and the lower *asymptotic density* of A is

$$\underline{d}(A) = \liminf_{n \geq 1} \frac{A(n)}{n}.$$

A set $H \subset \mathbb{N}$ is called a *Schnirelmann essential component* if for any $A \subset \mathbb{N}$ with $0 < \underline{d}(A) < 1$, we have

$$\underline{d}(A + H) > \underline{d}(A).$$

The notion of essential components was introduced by Khinchin [22] and originally defined in Shnirelmann's density σ. As was proved by Plünnecke [28, Theorem 77, p. 116], a set of integers is a Schnirelmann essential component if and only if it is an asymptotic essential component and it contains both 0 and 1.

By the definition of essential components, one can expect that a set with more elements is more "likely" an essential component. Schnirelmann's inequality [30] implies that a set with positive Schnirelmann density is an essential component. Khinchin [22] proved that the set squares $Q = \{a^2 : a \in \mathbb{Z}\}$ is an essential component, though the set is of density zero. Note that, by Lagrange's four square theorem, we have $4Q = \mathbb{N}$. More generally, Erdős [8] proved that if H is an additive basis of $\mathbb{N}$, i.e. $kH = \mathbb{N}$ for some $k \in \mathbb{Z}$, then H is an essential component. Here, if $kH = \mathbb{N}$, we at least have $H(x) \gg x^{1/k}$. The question then arises: if H is an essential component how small can $H(x)$ be? Linnik [25] constructed an example of an essential component H such that $H(x) = O(\exp(\log^{\frac{9}{10}} x))$. For any given $\eta > 0$, Wirsing [38] constructed an example of an essential component H with $H(x) = O(\exp(\eta\sqrt{\log x}\log\log x))$.

Finally, Ruzsa [31] gave a complete answer to this question by proving the following theorems.

Theorem. (Ruzsa 1987) *For any $c > 0$, there exists an essential component H such that $H(x) \ll \log^{1+c} x$.*

Theorem. (Ruzsa 1987) *Suppose $H \subset \mathbb{N}$ is such that for any $\epsilon > 0$, $|H(x)| < \log^{1+\epsilon} x$ infinitely often. Then there is a set $A \subset \mathbb{N}$ such that*

$$0 < \underline{d}(A) = \underline{d}(A + H) < 1. \tag{1.12}$$

Consequently, there does not exist an essential component H such that $H(x) \ll \log^{1+o(1)} x$.

1.6 Wirsing's construction of thin essential component

In [38], Wirsing constructed essential components in $\mathbb{Z}$ with small counting functions. He also proved the following finite version of his main result.

Theorem. (Wirsing, 1974) *Let $n \geq 1$ and $A \subset \mathbb{Z}$ be any subset of $[1, 2^n]$. Let $H = \{\pm 2^k : k \geq 0\} \cup \{0\}$ and $B = (A + H) \cap [1, 2^n]$. Then we have*

$$|B| \geq |A| + \sqrt{\frac{2}{n}}|A| \left(1 - \frac{|A|}{2^n}\right).$$

Wirsing's argument is elementary, very simple and surprisingly effective. With Thái Hoàng Lê, we will adapt Wirsing's argument to prove an analogous result for vector spaces over a finite field. The adaptation is straightforward for $\mathbb{F}_2^n$, but less so for $\mathbb{F}_p^n$.

Theorem 1.6.1. *Let p be a prime and $e_1, \dots, e_n$ be a basis of $\mathbb{F}_p^n$. Put $H = \{e_1, \dots, e_n\} \cup \{0\}$. Then for any $A \subset \mathbb{F}_p^n$, we have*

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{p^n}\right)$$

for some constant $c(p) > 0$. We can take $c(2) = \sqrt{2}$ and $c(p) = \Omega(p^{-3/2})$.

As an application, we will deduce quickly the following generalization of a theorem of Sanders ([34, Theorem 1.2]). By the *density* of a subset $A \subset X$ in X, we mean $\frac{|A|}{|X|}$.

Theorem 1.6.2. *Let p be a prime. Then there is a constant $c'(p) > 0$ such that the following holds. If $A \subset \mathbb{F}_p^n$ has density $\alpha > 1/2 - \frac{c'(p)}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.*

Sanders' theorem is a special case of Theorem 1.6.2 when $p = 2$. In Section 5.1 we will prove a general result for Cartesian products (Theorem 5.1.1 below). Theorems 1.6.1 and 1.6.2 are proved in Sections 5.2 and 5.3, respectively.

1.7 Essential components in vector spaces over finite fields

In view of the influential finite field model in additive combinatorics, it is natural to study the analog of essential components when $\mathbb{N}$ is replaced by a vector space over a finite field.

Let $\mathbb{F} = \mathbb{F}_p$ be the finite field over p elements, where p is prime. Let

$$G := \oplus_{i=0}^{\infty}\mathbb{F} = \{(x_0, x_1, \dots) : x_i \in \mathbb{F}, x_i \neq 0 \text{ for finitely many i}\}.$$

Additively, G is isomorphic to the group $\mathbb{F}[t]$ of polynomials over $\mathbb{F}$. We will write $\mathbb{F}[t]$ and G interchangeably and refer to elements of G as both vectors and polynomials, though no arithmetic structure of $\mathbb{F}[t]$ is involved. Let $G_n = \{x \in \mathbb{F}[t] : \deg x < n\}$,

then as an additive group, $G_n \cong \mathbb{F}^n$. We also define $G_0 = \{0\}$. If A is a subset of G, then by A_n we denote $A \cap G_n$. We define the lower asymptotic density of A to be

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{|A_n|}{p^n}.$$

The upper asymptotic density $\overline{d}$ and asymptotic density d are defined similarly. We say a set $H \subset G$ is an essential component if whenever $0 < \underline{d}(A) < 1$, we have

$$\underline{d}(A) < \liminf_{n\to\infty} \frac{|A_n + H_n|}{p^n}.$$

Note that $\liminf_{n\to\infty} \frac{|A_n+H_n|}{p^n}$ is not necessarily the same as $\underline{d}(A+H) = \liminf_{n\to\infty} \frac{|(A+H)_n|}{p^n}$. In contrast to $\mathbb{N}$, G is a group and in general we have $A_n + H_n \subsetneq (A+H)_n$. Since A and H are both infinite sets, little else can be said about $(A+H)_n$ in terms of A_n and H_n. This observation, made precise by the following Proposition, shows that $\underline{d}(A+H)$ is of little interest and our notion is a natural analog of the notion of essential components in $\mathbb{N}$.

Proposition 1.7.1. *If $H \subset G$ is infinite, then there is a set $A \subset G$ such that $d(A) = 0$ and $A + H = G$.*

Proof. Since H is infinite, we can find a sequence $(h_n)_{n=1}^{\infty} \subset H$ such that $\deg(h_n) > \max(\deg(h_{n-1}), 2n)$ for any $n > 1$. Let

$$A := \cup_{n=1}^{\infty}(G_n - h_n).$$

Then for any n, $A + H \supset (G_n - h_n) + h_n = G_n$, showing that $A + H = G$. On the other hand, notice that every element in $G_n - h_n$ has degree equal to $\deg(h_n)$. Thus

$$\overline{d}(A) = \lim_{n\to\infty} \frac{|\cup_{j=1}^{n}(G_j - h_j)|}{p^{\deg(h_n)}} = \lim_{n\to\infty} \frac{\sum_{j=1}^{n} p^j}{p^{\deg(h_n)}} = 0.$$

□

The problem of essential components in $\mathbb{F}[t]$ was already studied by Burke [5], who proved the following analog of Erdős' theorem: If H is a basis of order $\leq k$, that is, $kH_n = G_n$ for any $n \in \mathbb{Z}^+$, then H is an essential component. Clearly, if H is a basis of order $\leq k$ then $|H_n| \gg n^{1/k}$.

In this thesis, we prove the following analogs of Ruzsa's Theorems.

Theorem 1.7.2. *For any $c > 0$, there exists an essential component $H \subset G$ such that $|H_n| \ll n^{1+c}$.*

Theorem 1.7.3. *Suppose $H \subset G$ is such that for any $\epsilon > 0$, $|H_n| < n^{1+\epsilon}$ infinitely often. Then for any $0 < \delta < 1$, there is a set $A \subset G$ such that*

$$\delta = \underline{d}(A) = \liminf_{n\to\infty} \frac{|A_n + H_n|}{p^n}. \tag{1.13}$$

Consequently, there does not exist an essential component H such that $|H_n| \ll n^{1+o(1)}$.

We remark that our conclusion (1.13) is more precise than Ruzsa's (1.12) in that the density of A can be any prescribed number. The proofs of Theorems 1.7.2 and 1.7.3 will parallel Ruzsa's Theorems in Section 1.5. In our proofs many details are cleaner thanks to the vector space structure of G_n, but some of the arguments don't carry to G_n in a straightforward way, not least because of the fact that there is no linear ordering on G. In proving Theorem 1.7.3, we adapt Ruzsa's idea of "niveau sets", namely the set of points at which the Fourier transform of a function is large. The idea was first introduced by Ruzsa in proving Theorem 1.5 and has found applications in other problems (see [32], [11], [39]) and in particular in vector spaces ([39]). In the context of vector spaces, niveau sets are particularly pleasant.

Similarly to Theorem 1.5, the construction in Theorem 1.7.2 is probabilistic. It is therefore desirable to have an explicit example of an essential component with small

counting function. We construct the following analog of Wirsing's construction. Our construction is based on an isoperimetric-type inequality (see Lemma 6.1.6), which was inspired by Wirsing's argument. Also, our construction is not a straightforward adaptation of Wirsing's, due to differences between $\mathbb{N}$ and $\mathbb{F}[t]$.

If $x = (x_0, x_1, \ldots) \in G$, we define the *support* of x to be $\mathrm{supp}(x) = \{i : x_i \neq 0\}$.

Theorem 1.7.4 (Ge-Lê 2019)**.** *Let* $\mathbf{1}_n := 1 + t + \cdots + t^{n-1}$*. Then for any* $\eta > 0$*, the set*

$$H = \cup_{n=1}^{\infty} \left\{ x + \mathbf{1}_n : x \in G_n, |\mathrm{supp}(x)| \leq \eta\sqrt{n} \right\}$$

is an essential component in G *and has counting function* $|H_n| = \exp\left(O_p\left(\eta\sqrt{n}\log n\right)\right)$.

2 EVALUATION OF THE GAUSS TYPE SUMS

In this chapter, we study the sum

$$S_1(\chi) = \sum_{n=1}^{2q} \chi(n)\, e\left(\frac{-n^2}{2q}\right), \qquad \text{and} \qquad S_2(\chi) = \sum_{n=1}^{q} \chi(n)\, e\left(\frac{-2n^2}{q}\right),$$

where χ is a primitive character (mod q). We will evaluate $S_1(\chi)$ and $S_2(\chi)$ by relating them to the sum

$$S_3(\psi, r) = \sum_{n=1}^{q_2} \psi(n^2) e\left(\frac{rn^2}{q_2}\right),$$

where ψ is a primitive character mod q_2 and r is coprime to q_2. Via a standard application of the Chinese Remainder Theorem, we can factor $S_3(\psi, r)$ as

$$S_3(\psi, r) = \prod_p \psi_p(q_2/p^{e_p})^2 S_3(\psi_p, rq_2/p^{e_p}), \tag{2.1}$$

where $q_2 = \prod_p p^{e_p}$ and $\psi = \prod_p \psi_p$.

The relationship between $S_1(\chi)$ and $S_3(\psi, r)$ comes from the fact that when χ is a primitive even character (mod q) and q is even, there is a primitive character ψ mod $2q$ such that $\psi^2 = \chi$, so $S_1(\chi) = S_3(\psi, -1)$ for this character ψ mod $q_2 = 2q$. If q is odd or χ does not have a square root then we will find that it is easy to show that $S_1(\chi) = 0$, so anytime the sum is nonzero we will be able to evaluate it this

way. Similarly, by the fact that if $S_2(\chi) \neq 0$ then $\chi = \psi^2$ for some primitive $\psi \pmod q$, we can write $S_2(\chi) = S_2(\psi^2) = S_3(\psi, -2)$. Therefore, Theorem 1.4.1 and Theorem 1.4.5 are direct corollaries of the next proposition.

Proposition 2.0.1. *Let $\psi = \prod_p \psi_p$ be a primitive character mod $q = \prod_p p^{e_p}$, where each factor ψ_p is a primitive character mod p^{e_p}. Set α_2 to be an integer such that $\psi_2(5) = e(\alpha_2/2^{e_2-2})$, and for each odd prime p set α_p to be an integer such that $\psi_p(p+1) = e(\alpha_p/p^{e_p-1})$. Then $S_3(\psi, r) \neq 0$ if and only if*

(i) *$e_2 < 5$, or $e_2 = 5, 6$ and $\alpha_2 \equiv -3rq/2^5 \pmod{2^{e_2-3}}$, or $e_2 > 6$ and $\alpha_2 \equiv rq/2^{e_2} \pmod 8$; and*

(ii) *for each odd prime p such that p^2 divides q, the residue $-\alpha_p rq/p^{e_p}$ is a square modulo p.*

When the sum is nonzero, our proof will give an explicit evaluation in terms of Gauss sums. It seems tedious to write out all of the cases when e_2 is small, but when $e_2 > 6$ we can write this as

$$S_3(\psi, r) = 2^{\nu+2} \prod_{p|q} \psi_p\left(\frac{q\overline{r}}{p^{e_p}}\right) \prod_{p^2|q} \tau(\psi_p) \prod_{p\| q} \left(\tau(\psi_p) + \epsilon_p\left(\frac{rq}{p}\right)\tau(\epsilon_p\psi_p)\right), \qquad (2.2)$$

where ν is the number of primes p dividing q such that p_2 divides q, and $\epsilon_p(n) = (\frac{n}{p})$ is the quadratic character mod p.

2.1 Gauss sums

Before we can estimate $S_3(\psi, r)$, we first establish some tools about Gauss sums.

Lemma 2.1.1. *Let χ be a primitive character mod p^a for some $a > 1$, and ψ a character mod p^b for some $b \leq a/2$. For any integer ℓ in the range $a/2 \leq \ell \leq a - b$*

let α be an integer such that

$$\chi(p^\ell + 1) = e\left(\frac{\alpha}{p^{a-\ell}}\right).$$

Then

$$\tau(\psi\chi) = \psi(-\alpha)\tau(\chi).$$

Proof. We first note that $(mp^\ell + 1)(np^\ell + 1) = mnp^{2\ell} + (m+n)p^\ell + 1$, and $2\ell \geq a$ by hypothesis, so $\chi(np^\ell + 1)$ is an additive character as a function of n, and more specifically

$$\chi(np^\ell + 1) = e(n\alpha/(p^{a-\ell})).$$

We now split the Gauss sum $\tau(\psi\chi)$ into the various arithmetic progressions mod p^ℓ, writing

$$\tau(\psi\chi) = \sum_{n=1}^{p^{a-\ell}} \sum_{m=0}^{p^\ell - 1} \psi(np^\ell + m)\chi(np^\ell + m) e\left(\frac{np^\ell + m}{p^a}\right)$$

As we restrict to the case where $\ell \geq b$, $\psi(np^\ell + m)$ depends only on m, so we move it outside the inner sum and evaluate $\chi(np^\ell + m)$ as $\chi(m)$ times and additive character, writing this sum as

$$\begin{aligned}\tau(\psi\chi) &= \sum_{\substack{m=1 \\ p\nmid m}}^{p^\ell - 1} \psi(m)\chi(m) \sum_{n=1}^{p^{a-\ell}} \chi(\overline{m}np^\ell + 1) e\left(\frac{np^\ell + m}{p^a}\right) \\ &= \sum_{\substack{m=1 \\ p\nmid m}}^{p^\ell - 1} \psi(m)\chi(m) e\left(m/p^a\right) \sum_{n=1}^{p^{a-\ell}} e\left(\frac{\overline{m}n\alpha + n}{p^{a-\ell}}\right),\end{aligned}$$

where $\overline{m}$ denotes the inverse of m modulo p^a. We now see that the innermost sum vanishes unless $m \equiv -\alpha \mod p^{a-\ell}$, in which case it is exactly $p^{a-\ell}$, so we find that

the sum is equal to

$$p^{a-\ell} \sum_{\substack{m=1 \\ p \nmid m \\ m \equiv -\alpha \mod p^{a-\ell}}}^{p^\ell - 1} \psi(m)\chi(m)e\left(m/p^a\right).$$

Finally, we note once again that $b \leq \ell$, so $\psi(m) = \psi(-\alpha)$ when $m \equiv -\alpha \mod p^{a-\ell}$, so the whole sum is

$$\psi(-\alpha)p^{a-\ell} \sum_{\substack{m=1 \\ p \nmid m \\ m \equiv -\alpha \mod p^{a-\ell}}}^{p^\ell - 1} \chi(m)e\left(m/p^a\right).$$

Considering that this expression is equally valid when ψ is the trivial character finishes the proof. □

We extract a few simpler variants of this lemma which allow us to consider only the values $\chi(p+1)$ (when p is odd) and $\chi(5)$ (when $p = 2$).

Lemma 2.1.2. *Let χ be a primitive character mod p^a for $p > 2$ and some $a > 1$, and ψ a character mod p. Let α be an integer such that*

$$\chi(p+1) = e\left(\frac{\alpha}{p^{a-1}}\right).$$

Then

$$\tau(\psi\chi) = \psi(-\alpha)\tau(\chi).$$

Proof. From the previous lemma we have

$$\tau(\psi\chi) = \psi(-\alpha')\tau(\chi),$$

where $\chi(p^{a-1}+1) = e(\alpha'/p)$. We need only show that $\alpha \equiv \alpha' \mod p$. The congruence

$$(p+1)^{p^{a-2}} \equiv p^{a-1}+1 \mod p^a$$

follows easily by expanding using the binomial theorem, from which we see that in fact $\chi(p^{a-1}+1) = e(\alpha/p)$. □

Lemma 2.1.3. *Let χ be a primitive character modulo $q = 2^a$, for $a > 6$, and let ϵ be a character mod 8. Let α be an integer such that*

$$\chi(5) = e(\alpha/2^{a-2}).$$

Then

$$\tau(\epsilon\chi) = \epsilon(\alpha)\tau(\chi).$$

Proof. From the Lemma 2.1.1 we have

$$\tau(\epsilon\chi) = \epsilon(-\alpha')\tau(\chi),$$

where $\chi(p^{a-3}+1) = e(\alpha'/p)$. For $l \geq 4$, applying the binomial theorem to $(2^2+1)^{7\cdot 2^{l-2}}$ we find the congruence $5^{7\cdot 2^{l-2}} \equiv 2^l + 1 \mod 2^{l+3}$. As the multiplicative order of 5 mod 2^{l+3} is 2^{l+1}, we find that the discrete logarithm of 2^l+1 with respect to 5 mod 2^a must be congruent to $7 \cdot 2^{l-2}$ mod 2^{l+1}. This means that

$$\chi(2^l+1) = \chi(5)^{7\cdot 2^{l-2}+k2^{l+1}}$$

for some integer k. That is,

$$\chi(2^l+1) = e\left(\frac{7\alpha + 8k}{2^{a-l}}\right)$$

for this integer k. When $l = a - 3$ this is simply

$$\chi(2^{a-3}+1) = e\left(\frac{7\alpha}{8}\right),$$

and now Lemma 2.1.1 finishes the proof. □

2.2 Evaluation of the main sum

We begin by studying the sum $S_3(\psi, r)$ when ψ is a primitive character of prime power conductor. For any modulus q, we can rewrite the sum S_3 as

$$S_3(\psi, r) = \sum_{n=1}^{q} \left(\sum_{\substack{\xi \bmod q \\ \xi^2 = \chi_0}} \xi(n) \right) \psi(n) e\left(\frac{rn}{q}\right),$$

as the inner sum detects squares mod q and counts them with the correct multiplicity. Interchanging the order of summation gives an expression for S_3 as a linear combination of Gauss sums; for a general modulus it seems complicated to directly evaluate this sum, however, so analyze it separately for each prime power dividing q and and factor S_3 using the Chinese remainder theorem. We separate the case $p = 2$, and will also see different behavior based on whether or not p^2 divides q.
For an even prime power modulus we have the following evaluations.

Lemma 2.2.1. *Let ψ be a primitive character* (mod 2^a) *for $a = 3, 4, 5, 6$. Let α be the integer such that $\psi(5) = e(\alpha/2^{a-2})$. We have*

$$S_3(\psi, r) = 2^{a-1} e(\tfrac{r}{2^a}),$$

if $\alpha \equiv -3r$ (mod 2^{a-3})*; zero otherwise.*

Proof. Write $S_3(\psi, r)$ as the following double sum

$$\begin{aligned} S_3(\psi, r) &= \sum_{m=0}^{1} \sum_{n=1}^{2^{a-2}} \psi^2((-1)^m 5^n) e\Big(\frac{r5^{2n}}{2^a}\Big) = 2 \sum_{n=1}^{2^{a-2}} \psi(5^{2n}) e\Big(\frac{r5^{2n}}{2^a}\Big) \\ &= 2 \sum_{n=1}^{2^{a-2}} e\Big(\frac{8n\alpha + r5^{2n}}{2^a}\Big) = 2\, e\Big(\frac{r}{2^a}\Big) \sum_{n=1}^{2^{a-2}} e\Big(\frac{n\alpha + \frac{r(5^{2n}-1)}{8}}{2^{a-3}}\Big) \end{aligned}$$

When $a = 3, 4, 5, 6$, we have the congruence relation $\frac{5^{2n}-1}{8} \equiv 3n \bmod 2^{a-3}$, which can be verified by checking all four cases. Putting the congruence relation into the above formula, we obtain the desired result. □

Proposition 2.2.2. *Let ψ be a primitive character mod 2^a, and let α be the integer such that $\psi(5) = e(\alpha/2^{a-2})$. We have the following.*

- *If $3 \le a \le 6$ and $\alpha \equiv -3r \pmod{2^{a-3}}$, then $|S_3(\psi, r)| = 2^{a-1}$;*
- *If $a > 6$ and $r \equiv \alpha \pmod 8$, then $S_3(\psi, r) = 4\overline{\psi}(r)\tau(\psi)$.*

In all other cases, $S_3(\psi, r) = 0$.

Proof. When $a \ge 6$, the sum is

$$\begin{aligned} S_3(\psi, r) &= \sum_{\xi \bmod 8} \sum_{n=1}^{2^a} \xi\psi(n) e(rn/2^a) \\ &= \sum_{\xi \bmod 8} \overline{\xi\psi}(r)\tau(\xi\psi). \end{aligned}$$

Now we can evaluate these Gauss sums using Lemma 2.1.3, and we find that

$$S_3(\psi, r) = \overline{\psi}(r)\tau(\psi) \sum_{\xi \bmod 8} \overline{\xi}(r)\xi(\alpha),$$

which completes the proof. □

Proposition 2.2.3. *Let ψ be a primitive character modulo $q = p^a$, for a prime $p > 2$. If $a = 1$ then $S_3(\psi, r) \neq 0$. Otherwise let α be the integer such that $\psi(p+1) = e(\alpha/p^{a-1})$. Then*

$$S_3(\psi, r) = \left(1 + \left(\frac{-\alpha r}{p}\right)\right) \overline{\psi}(r)\tau(\psi).$$

Proof. Again rewriting S_3 in terms of Gauss sums we have

$$S_3(\psi, r) = \overline{\psi}(r)(\tau(\psi) + \epsilon(r)\tau(\epsilon\psi)), \tag{2.3}$$

where ϵ denotes the quadratic character mod p. If $q = p$, then both ψ and ϵ are primitive characters. If $\psi = \epsilon$ then $\tau(\psi\epsilon) = -1$ and $S_3(\psi, r) = \overline{\psi}(r)(\tau(\psi) - \epsilon(r)) \neq 0$. Otherwise, $\epsilon\psi$ is a primitive character as well, we can express $\tau(\epsilon\psi)$ in terms of the Jacobi sum

$$\begin{aligned} J(\psi, \epsilon) =& \sum_{n=1}^{p} \psi(n)\epsilon(1-n) \\ =& \frac{\tau(\psi)\tau(\epsilon)}{\tau(\epsilon\psi)}. \end{aligned}$$

Putting in the evaluation of the Gauss sum for the quadratic character and rearranging we find that

$$\frac{\tau(\epsilon\psi)}{\tau(\psi)} = \frac{\sqrt{\pm p}}{J(\psi, \epsilon)}.$$

This ratio cannot be ± 1 because the Jacobi sum lies in the cyclotomic field $\mathbb{Q}(\zeta_{p-1})$ and $\sqrt{\pm p}$ does not. So $\tau(\psi) + \epsilon(r)\tau(\epsilon\psi)$ is nonzero.

If $a > 1$ we can use Lemma 2.1.2 to evaluate the second Gauss sum in terms of the first, and find that

$$S_3(\psi, r) = \overline{\psi}(r)(\tau(\psi) + \epsilon(-\alpha r)\tau(\psi)).$$

□

With this evaluation of S_3 for each prime power q, Proposition 2.0.1 follows from factoring S_3 using the Chinese Remainder Theorem as in equation (2.1).

We now return to the sum of main interest. The first thing we establish is that the sum vanishes if q is odd.

Lemma 2.2.4. *If χ is a character mod q, and q is odd, then $S_1(\chi) = 0$.*

Proof. From

$$e\left(\frac{-(n+q)^2}{2q}\right) = e(q/2)e(-n^2/2q),$$

we find that

$$\sum_{n=q+1}^{2q} \chi(n)e(-n^2/q) = e(q/2)\sum_{n=1}^{q} \chi(n)e(-n^2/q).$$

Thus, if q is odd the first and second halves of the defining sum for $S_1(\chi)$ have opposite signs and the whole sum vanishes. □

As was the case with S_3, it will be now convenient to express $S_1(\chi)$ as a linear combination of Gauss sums. In this case we do this by writing the additive character $e(a/b)$ in terms of multiplicative characters as

$$e(a/b) = \frac{1}{\varphi(b)} \sum_{\xi \bmod b} \tau(\xi)\overline{\xi}(n),$$

valid whenever $(a, b) = 1$. Putting this in the definition of $S_1(\chi)$ and interchanging the order of summation we find that q is even

$$\begin{aligned} S_1(\chi) =& \sum_{n=1}^{2q} \chi(n)e\left(\frac{-n^2}{2q}\right) \\ =& \frac{1}{\varphi(2q)} \sum_{n=1}^{2q} \chi(n) \sum_{\xi \bmod 2q} \overline{\xi}(-n^2)\tau(\xi) \\ =& \frac{1}{\varphi(2q)} \sum_{\xi \bmod 2q} \xi(-1)\tau(\xi) \sum_{n=1}^{2q} \overline{\xi}^2\chi(n). \end{aligned}$$

The inner sum vanishes unless $\xi^2 = \chi$, in which case it is $\varphi(2q)$, so we find that as long as q is even we have

$$S_1(\chi) = \sum_{\substack{\xi \bmod 2q \\ \xi^2=\chi}} \xi(-1)\tau(\xi). \tag{2.4}$$

From this expression we easily extract the following observation.

Lemma 2.2.5. *If $\chi = \prod_p \chi_p$ is primitive character mod $q = \prod_p p^{e_p}$ and any χ_p is odd then $S_1(\chi) = 0$.*

Proof. It is clear that if there does not exist a character ξ such that $\xi^2 = \chi$, then the right hand side of Equation (2.4) is an empty sum, so $S_1(\chi)$ vanishes. The condition that there exist such a character is exactly the condition that each factor χ_p is an even character. □

Remark 1. *Note that there are no primitive even characters mod 2, 3, or 4, so in order for the sum not to vanish, q must be divisible by 8, and if q is divisible by 3 then it is divisible by 9 as well.*

Now that we know that there is some primitive character ψ mod $2q$ such that $\psi^2 = \chi$, we can evaluate our sum as $S_1(\chi) = S_3(\psi, -1)$ using Proposition 2.0.1. The only task that remains is to consider is how the "logarithms" α_p change when we take the "square root" of χ.

Proof of Theorem 1.4.1. We have already established that if $S_1(\chi)$ does not vanish then there is some primitive character ψ mod $2q$ such that $S_1(\chi) = S_3(\psi, -1)$. Write $\psi = \prod_p \psi_p$, and $\chi = \prod_p \chi_p$, and also write

$$\chi_2(5) = e(\alpha_2/2^{e_2-2}) \quad \psi_2(5) = e(\beta_2/2^{e_2-1})$$

and for odd primes p define

$$\chi_p(p+1) = e(\alpha_p/p^{e_p-1}) \quad \psi_p(p+1) = e(\beta_p/p^{e_p-1}).$$

As $\psi_p(p+1)^2 = \chi_p(p+1)$, we see that there is only a single choice $\alpha_p \equiv 2\beta_p \pmod{p}$ for odd p. At the prime 2 we have the possibilities $\beta_2 \equiv \alpha_2 \pmod{2^{e_2-1}}$ and $\beta_2 \equiv \alpha_2 + 2^{e_2-2} \pmod{2^{e_2-1}}$. If $e_2 = 3$ then we are not concerned about the value of β_2; if $e_2 = 4$ then the value of β_2 is determined mod 4, while if $e_2 > 4$ then the value of β_2 is determined mod 8. In every case this is good enough to apply Proposition 2.0.1. □

2.3 Counting nonvanishing

In this section we count the number of primitive characters χ such that $S_1(\chi) \neq 0$. To that end, let $N_1(q)$ denote the number of such characters mod q; that is

$$N_1(q) = \#\left\{\text{primitive } \chi \pmod{q} \text{ such that } S_1(\chi) \neq 0\right\}.$$

This is not a multiplicative function (for example, $N_1(p) = 0$ but $N_1(8p) \neq 0$ for an odd prime p), but from the factorization of the sum using the Chinese Remainder Theorem, it is closely related to one.

As we have evaluated $S_1(\chi)$ by relating it to $S_3(\psi, r)$, it will be similar and convenient to first count the number of primitive ψ mod q such that $S_3(\psi, r) \neq 0$, which we label $N_3(q)$. As we will see in a moment, this number does not depend on r as long as r is coprime to q, and once it is clear that this number does not depend on r, it is apparent from the factorization (2.1) that it is close to a multiplicative function.

When $q = 2^a$ is a power of 2, a character $\chi \pmod{q}$ is determined by its values $\chi(-1) = \pm 1$ and $\chi(5) = e(\alpha/2^{a-2})$ for the 2^{a-2} different possible values of α. The

primitive characters are exactly those for which α is odd, and clearly every residue class modulo 8 is covered the same number of times by the possible values of α. As $N_3(2^a)$ depends only on α mod 8 we see that it is independent of r and, examining Proposition 2.2.2, we find

- $N_3(2) = 0$ (there are no primitive characters);
- for $2 \leq a < 5$, we have $N_3(2^a) = 2^{a-2}$ (the sum is always nonzero);
- $N_3(2^5) = 4$ (there are 8 primitive characters, and the sum vanishes for half of them);
- for $a > 5$ we have $N_2(2^a) = 2^{a-4}$ (there are 2^{a-2} primitive characters and the sum is nonzero one quarter of the time).

Here, this counting includes the case when $\psi^2 = \mathbf{1}$. We will exclude it later when we consider $\chi = \psi^2$ being primitive.

When q is prime, the sum $S_3(\psi, r)$ never vanishes, so $N_3(p) = \varphi(p) - 1 = p - 2$. (Again, this includes a primitive quadratic character, which will be dropped for counting $S_1(\chi) \neq 0$.) Otherwise for $q = p^q$ with $a > 1$, the vanishing or nonvanishing of the sum is determined by the congruence class of α mod p, where $\chi(p+1) = e(\alpha/p^{a-1})$ For half of the α mod p the sum will vanish and for the other half it will not. The primitive characters are exactly those for which $p \nmid \alpha$, and, as the character group is cyclic, each value of α occurs the same number of times. There are $\varphi(p^a) - \varphi(p^{a-1})$ primitive characters, and for half of them the sum does not vanish, so $N_3(p^a) = p^{a-2}(p-1)^2/2$ when $a > 1$.

Now, if 8 divides q then for every primitive character ψ mod $2q$, such that no factor ψ_p is quadratic, the character ψ^2 has conductor q. So we can compute $N_1(q)$ by computing $N_3(2q)$ and adjusting for the multiplicity of squares and each quadratic character mod p. Specifically speaking, for each odd prime $p^a \mid q$

- if $a = 1$ then $N_1(p) = (N_3(p) - 1)/2 = \frac{1}{2}(p-3)$;
- if $a > 1$ then $N_1(p^a) = N_3(p^a)/2 = \frac{1}{4}p^{a-2}(p-1)^2$.

For $2^a \mid q$,

- if $a < 3$ then $N_1(2^a) = 0$;
- if $3 \le a \le 5$ then $N_1(2^a) = 1$;
- if $a \ge 6$ then we $N_1(2^a) = \lceil N_3(2^a)/2 \rceil = \lceil 2^{a-5} \rceil$.

Therefore we find that for $a \ge 3$

$$N_1(q) = \lceil 2^{a-5} \rceil \prod_{p \| q} \frac{p-3}{2} \prod_{\substack{p^a \| q \\ a>1}} \frac{p^{a-2}(p-1)^2}{4}. \tag{2.5}$$

Similarly, to count how many primitive $\chi \pmod q$ with odd q s.t. $S_2(\chi) \neq 0$, we still use the counting function $N_3(\cdot)$. For odd $p^a \mid q$,

- if $a = 1$ then $N_2(p) = (N_3(p) - 1)/2 = \frac{1}{2}(p-3)$;
- if $a \ge 2$ then $N_2(p^a) = N_3(p^a)/2 = \frac{1}{4}p^{a-2}(p-1)^2$.

Therefore for odd q,

$$N_2(q) = \prod_{p \| q} \frac{p-3}{2} \prod_{\substack{p^a \| q \\ a>1}} \frac{p^{a-2}(p-1)^2}{4}.$$

With the formula (2.5) in hand, we now proceed to use the Selberg–Delange method to prove Theorem 1.4.4.

Proof of Theorem 1.4.4. From Proposition 1.4.3, we know that $N_1(2^a) = 0$ if $a = 1, 2$ and $N(2^a) = \lceil 2^{a-5} \rceil$ if $a \ge 3$. We define a multiplicative function N_0 supported on odd positive integers by $N_0(1) = 1$, $N_0(p) = \frac{p-3}{2}$, and $N_0(p^a) = \frac{p^{a-2}(p-1)^2}{4}$ for odd

primes p and $a \geq 2$. Then, for odd positive integers k, Proposition 1.4.3 implies that $N_1(2^a k) = N_1(2^a)N_0(k)$ and we can formally expand the Dirichlet series

$$\begin{aligned} F(s) := \sum_{q=1}^{\infty} \frac{N_1(q)}{q^{s+1}} &= \left(\frac{1}{2^{3(s+1)}} + \frac{1}{2^{4(s+1)}} + \sum_{a \geq 5} \frac{2^{a-5}}{2^{a(s+1)}} \right) \\ &\quad \times \prod_{p \neq 2} \left(1 + \frac{p-3}{2p^{s+1}} + \sum_{a \geq 2} \frac{p^{a-2}(p-1)^2}{4p^{a(s+1)}} \right) \\ &= f(s)\, g(s) \prod_{p} \left(1 + \frac{1}{2p^s} \right), \end{aligned}$$

where

$$f(s) = \left(\frac{1}{2^{3(s+1)}} + \frac{1}{2^{4(s+1)}} + \frac{1}{2^{4s+5}(2^s - 1)} \right) \left(1 - \frac{1}{2^{s+2}} + \frac{1}{2^{s+4}(2^s - 1)} \right)^{-1}$$

and

$$g(s) = \prod_{p} \left(1 - \frac{3}{(2p^s + 1)p} + \frac{(p-1)^2}{2p^2(p^s - 1)(2p^s + 1)} \right).$$

For any $\varepsilon > 0$, we claim that $F(s)\zeta(s)^{-1/2}$ is analytic (and its Dirichlet series is uniformly bounded) in the half-plane $\mathrm{Re}(s) \geq 1/2 + \varepsilon$. First note that $f(s)\, g(s)$ is analytic, nonzero, and uniformly bounded for $\mathrm{Re}(s) \geq \varepsilon$. If we let

$$h(s) = \prod_{p} \left(1 - \frac{1}{4p^{2s}} \right) \left(1 + \frac{1}{2p^{2s} + p^s - 1} \right),$$

then $h(s)$ is analytic, nonzero, and uniformly bounded in the half-plane $\mathrm{Re}(s) \geq 1/2 + \varepsilon$, and satifies

$$\prod_{p} \left(1 + \frac{1}{2p^s} \right)^2 = \frac{\zeta(s)}{\zeta(2s)}\, h(s).$$

Therefore

$$F(s)\, \zeta(s)^{-1/2} = f(s)\, g(s)\, h(s)^{1/2}\, \zeta(2s)^{-1/2},$$

and the claim follows. Thus, for $Q \geq 3$, using the Selberg–Delange method as stated in [36, Theorem 5.2, Chapter II], we derive that

$$\sum_{q \leq Q} \frac{N_1(q)}{q} = \frac{f(1)\, g(1)}{\Gamma(1/2)} \sqrt{\frac{h(1)}{\zeta(2)}} \frac{Q}{\sqrt{\log Q}} + O\Big(\frac{Q}{(\log Q)^{3/2}} \Big).$$

Summing by parts, it follows that

$$\sum_{q \leq Q} N(q) = \frac{f(1)\, g(1)}{2\,\Gamma(1/2)} \sqrt{\frac{h(1)}{\zeta(2)}} \frac{Q^2}{\sqrt{\log Q}} + O\Big(\frac{Q^2}{(\log Q)^{3/2}} \Big). \tag{2.6}$$

This completes the proof of Theorem 1.4.4. □

2.4 A direct proof for $C_\chi \in \mathbb{R}$ when modulus is $8p$

Although we know $Z_\chi(t)$ is real and hence the leading coefficient C_χ must be real, we think this argument is seemingly a very roundabout manner. We seek to prove $C_\chi \in \mathbb{R}$ in a direct way. In particular, when $q = 8p$ for odd prime p we can prove the following proposition which immediately implies $C_\chi \in \mathbb{R}$.

Proposition 2.4.1. *Let χ be a primitive character* (mod q)*, where $q = 8p$ for $p > 2$. Let $S_1(\chi) = \sum_{n=1}^{2q} \chi(n) e(\frac{-n^2}{2q})$. Then, $e(\frac{1}{16})\tau(\chi)^{-1/2} S_1(\chi) \in \mathbb{R}$.*

Proof. Let $D_\chi = e(\frac{1}{16})\tau(\chi)^{-1/2} S_1(\chi)$. We claim if $S_1(\chi) \neq 0$, then D_χ^2 has to be positive. In order for $S_1(\chi) \neq 0$, we assume $\chi = \chi_2 \chi_p$, where χ_2 is the even primitive character (mod 8) and $\chi_p = \psi_p^2$ for some primitive character ψ (mod p). For convenience, we let ϵ be the quadratic character (mod p).

By the Chinese Remainder Theorem, we can deduce

$$S_1(\chi) = \chi_2(p)\chi_p(4) \left(\sum_{n=1}^{16} \chi_2(n) e\Big(\frac{-pn^2}{16}\Big) \right) \left(\sum_{m=1}^{p} \chi_p(m) e\Big(\frac{-m^2}{p}\Big) \right)$$

and

$$\tau(\chi) = \chi_2(p)\chi_p(8)\,\tau(\chi_2)\tau(\chi_p).$$

If follows from Lemma 2.2.1 that

$$\sum_{n=1}^{16} \chi_2(n) e\Big(\frac{-pn^2}{16}\Big) = 2^3\, e\Big(\frac{-p}{16}\Big).$$

Now, on rewriting $S_2(\psi_p, -1)$ as a linear combination of two Gauss sums using (2.3), we can deduce that

$$\begin{aligned}
D_\chi^2 &= 2^6\, e\Big(\frac{1-p}{8}\Big)\chi_2(p)\chi_p(2)\,\frac{S_2(\psi_p,-1)^2}{\tau(\chi_2)\tau(\chi_p)} \\
&= 2^{9/2}\, e\Big(\frac{1-p}{8}\Big)\epsilon(2)\psi_p(4)\,\frac{(\tau(\psi_p)+\epsilon(-1)\tau(\psi_p\epsilon))^2}{\tau(\psi_p^2)} \\
&= 2^{9/2}\, e\Big(\frac{1-p}{8}\Big)\epsilon(2)\,\psi_p(4)J(\psi_p,\psi_p)\,\left(1+\epsilon(-1)\frac{\tau(\psi_p\epsilon)}{\tau(\psi_p)}\right)^2 \\
&= 2^{11/2}\,\left(\mathrm{Re}\Big(\frac{J(\psi_p,\epsilon)}{\tau(\psi_p)}\Big)+\epsilon(-1)\right)\cdot e\Big(\frac{1-p}{8}\Big)\epsilon(2)\tau(\epsilon),
\end{aligned}$$

where we applied the identity $\psi_p(4)J(\psi_p,\psi_p) = J(\psi_p,\epsilon)$ [1, Theorem 2.1.4], which is valid for $p > 2$ and ψ_p is nontrivial. Since $J(\psi_p,\epsilon)/\tau(\psi_p) \neq \pm 1$, we have a strict inequality $-1 < \mathrm{Re}(J(\psi_p,\epsilon)/\tau(\psi_p)) < 1$. It follows that if $\epsilon(-2)e(\frac{1-p}{8})\tau(\epsilon)$ is positive then D_χ^2 is positive. By classical results on quadratic Gauss sums and case checking, one can see $\epsilon(-2)e(\frac{1-p}{8})\tau(\epsilon) > 0$ for all odd p, which completes the proof. □

2.5 Nonvanishing of A_χ when q is prime

We have seen that $S_1(\chi) \neq 0$ only if χ is a square, which hence is even. Following the same method, we have a similar observation.

Observation 1. *When q is odd, $S_2(\chi) = \sum_{\psi^2=\chi} \tau(\psi)\overline{\psi}(-2)$. If χ is not a square of a character, then $S_2(\chi) = 0$.*

Proof. Putting the Fourier transform

$$e(\tfrac{-2n^2}{q}) = \frac{1}{\varphi(q)} \sum_{\psi(q)} \tau(\psi)\overline{\psi}(-2n^2)$$

into $S_2(\chi)$ we see that

$$S_2(\chi) = \sum_{\psi(q)} \tau(\psi)\overline{\psi}(-2) \cdot \frac{1}{\varphi(q)} \sum_{n=1}^{q} (\chi\overline{\psi}^2)(n) = \begin{cases} \sum_{\psi^2=\chi} \tau(\psi)\overline{\psi}(-2), & \text{if } \psi^2 = \chi, \\ 0, & \text{otherwise,} \end{cases}$$

which completes the proof. □

Proof of Proposition 1.4.7. Since $S_2(\chi) = 0$ if χ is not a square, from now on we assume $\chi = \psi^2$. Using a Fourier transform, we can write

$$S_2(\chi) = \sum_{\psi^2=\chi} \tau(\psi)\overline{\psi}(-2).$$

Let

$$C = \frac{\chi(2)\left(\tau(\psi)\overline{\psi}(-2) + \tau(\psi\epsilon)\overline{\psi\epsilon}(-2)\right)}{\tau(\psi^2)^{1/2}}.$$

We can deduce that

$$\begin{aligned} C^2 &= \frac{\psi(4)(\tau(\psi) + \epsilon(-2)\tau(\psi\epsilon))^2}{\tau(\psi^2)} \\ &= \psi(4)\tau(\psi)^2 \left(1 + \epsilon(-2)\frac{\tau(\psi\epsilon)}{\tau(\psi)}\right)^2 \cdot \frac{J(\psi,\psi)}{\tau(\psi)^2} \\ &= \left(1 + \epsilon(-2)\frac{\tau(\epsilon)}{J(\psi,\epsilon)}\right)^2 \cdot \psi(4)\, J(\psi,\psi) \\ &= \left(1 + 2\epsilon(-2)\frac{\tau(\epsilon)}{J(\psi,\epsilon)} + \frac{\tau(\epsilon)^2}{J(\psi,\epsilon)^2}\right) \cdot J(\psi,\epsilon) \\ &= 2\left(\mathrm{Re}\Big(\frac{J(\psi,\epsilon)}{\tau(\epsilon)}\Big) + \epsilon(-2)\right) \cdot \tau(\epsilon), \end{aligned}$$

where we applied the identity $\psi(4)J(\psi,\psi) = J(\psi,\epsilon)$ (see [1, Theorem 2.1.4]), which is valid for odd prime modulus p and ψ nontrivial (mod p). Note that

$$\tau(\epsilon) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 (\text{mod } 4) \\ i\sqrt{p} & \text{if } p \equiv 3 (\text{mod } 4) \end{cases}$$

For $\epsilon(-2)$ we have

$$\epsilon(-1) = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod } 4) \\ -1 & \text{if } p \equiv 3 (\text{mod } 4) \end{cases}$$

and

$$\epsilon(2) = \begin{cases} 1 & \text{if } p \equiv 1, 7 (\text{mod } 8) \\ -1 & \text{if } p \equiv 3, 5 (\text{mod } 8) \end{cases}$$

Recall that we have proved in Proposition 2.2.3 that $\frac{J(\psi,\epsilon)}{\tau(\epsilon)} \neq \pm 1$. The sign of $\epsilon(-2)$ determines the sign of $\text{Re}(\frac{J(\psi,\epsilon)}{\tau(\epsilon)}) + \epsilon(-2)$. Combining all 4 cases, we have seen that

$$\epsilon(-2)\tau(\epsilon) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \,(\text{mod } 8) \\ i\sqrt{p} & \text{if } p \equiv 3 \,(\text{mod } 8) \\ -\sqrt{p} & \text{if } p \equiv 5 \,(\text{mod } 8) \\ -i\sqrt{p} & \text{if } p \equiv 7 \,(\text{mod } 8) \end{cases}$$

Therefore, for c_p such that $p \equiv 2c_p + 1$ (mod 8) we have

$$C = \pm p^{-1/2} |S_2(\chi)| e(\tfrac{c_p}{8}),$$

which completes the proof. □

3 PROOF OF THEOREM 1.2.1 and THEOREM 1.3.1

3.1 Preliminaries

3.1.1 Notation

We can handle Theorems 1.2.1 and 1.3.1 simultaneously, if we work with a general definition of L-functions following Iwaniec-Kowalski [19, Chapter 5]. We say that $L(f,s)$ is an L-function of f if we have the following conditions:

- $L(f,s)$ is a Dirichlet series with Euler product of degree $d \geq 1$,

$$L(f,s) = \sum_{n \geq 1} \lambda_f(n) n^{-s} = \prod_p (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1}$$

  with $\lambda_f(1) = 1$, $\lambda_f(n) \in \mathbb{C}$, and $\alpha_i(p) \in \mathbb{C}$. These $\alpha_i(p)$, for $1 \leq i \leq d$, are called the *local roots or local parameters* of $L(f,s)$ at p with $|\alpha_i(p)| < p$ for all p.

- There is a gamma factor

$$\gamma(f,s) = \pi^{-ds/2} \prod_{j=1}^{d} \Gamma\left(\frac{s + \kappa_j}{2}\right)$$

  where the numbers $\kappa_j \in \mathbb{C}$ are called the *local parameters* of $L(f,s)$ at infinity.

- There is an integer $N_f \geq 1$, called the *conductor* of $L(f,s)$ such that $\alpha_i(p) \neq 0$ for *unramified primes* $p \nmid N_f$, $1 \leq i \leq d$.

- Let the *complete L-function* be

$$\Lambda(f,s) = N_f^{s/2}\gamma(f,s)L(f,s).$$

It is analytic in the half-plane $\mathrm{Re}(s) > 1$ and admits analytic continuation to a meromorphic function in $\mathbb{C}$ of order 1 with at most poles at $s = 0$ and $s = 1$. Moreover, it satisfies the *functional equation*

$$\Lambda(f,s) = \epsilon_f \Lambda(\overline{f}, 1-s),$$

where ϵ_f is a complex number with $|\epsilon_f| = 1$, and $\overline{f}$ is the dual of f for which $\lambda_{\overline{f}}(n) = \overline{\lambda}_f(n)$.

In our case, we write the functional equation in the following asymmetric form

$$L(f,s) = G_f(s)\, L(\overline{f}, 1-s),$$

where $L(\overline{f},s) = \overline{L(f,\overline{s})}$ and

$$G_f(s) = \epsilon_f\, N_f^{1/2-s}\pi^{d(-1/2+s)} \prod_{j=1}^{d} \frac{\Gamma(\frac{1}{2}(1-s+\kappa_j))}{\Gamma(\frac{1}{2}(s+\kappa_j))}.$$

The *Z-function associated to f* is defined as

$$Z_f(t) := G_f(\tfrac{1}{2}+it)^{-1/2} L(f, \tfrac{1}{2}+it).$$

Since in this thesis we focus on L-functions with degree $d \leq 2$, we may assume κ_j are either real or in conjugate pairs[1]. Combining the assumption with the definition

[1]Though this assumption does not hold in general, it is valid for the L-functions under consideration in this thesis.

of $Z_f(t)$,

$$\begin{aligned}\overline{Z_f(t)} &= \overline{G_f(\tfrac{1}{2}+it)}^{-1/2}\overline{L(f,\tfrac{1}{2}+it)} = \overline{G_f(\tfrac{1}{2}+it)}^{1/2}\overline{L(\overline{f},\tfrac{1}{2}-it)} \\ &= \overline{\epsilon_f}^{1/2}\, N_f^{it/2}\pi^{-dit}\prod_{j=1}^{d}\frac{\Gamma(\frac{1}{2}(\overline{\frac{1}{2}-it+\kappa_j}))^{1/2}}{\Gamma(\frac{1}{2}(\overline{\frac{1}{2}+it+\kappa_j}))^{1/2}}\, L(f,\tfrac{1}{2}+it) \\ &= \left(\epsilon_f\, N_f^{-it}\pi^{dit}\prod_{j=1}^{d}\frac{\Gamma(\frac{1}{2}(\frac{1}{2}-it+\overline{\kappa_j}))}{\Gamma(\frac{1}{2}(\frac{1}{2}+it+\overline{\kappa_j}))}\right)^{-1/2} L(f,\tfrac{1}{2}+it) = Z_f(t).\end{aligned}$$

This assumption guarantees that, for all real t, $Z_f(t)$ is real, $|Z_f(t)| = |L(f,\frac{1}{2}+it)|$, and hence the zeros of $Z_f(t)$ correspond to the zeros of $L(f,s)$ on the critical line with odd multiplicity.

For technical reasons, we will first prove an asymptotic formula for $\int_T^{2T} Z_f(t)dt$ and then combine estimates over dyadic intervals $(T/2^j, T/2^{j-1}]$ for $j \geq 1$ to obtain the desired theorems.

3.1.2 Stationary phase lemmas

Throughout, we let

$$\mathcal{T}_f = \frac{N_f^{1/d}T}{2\pi}.$$

and $c = 1 + 1/\log \mathcal{T}_f$. In this section, our goal is to prove the following lemma.

Lemma 3.1.1. *Assume that*

$$|L(f,\tfrac{1}{2}+it)| \ll (|t|+1)^{d/4} \quad \textit{and} \quad \sum_{n\geq 1}\frac{|\lambda_f(n)|}{n^c} \ll (\log T)^{\beta} \tag{3.1}$$

for some $\beta \geq 0$. Then

$$\int_T^{2T} Z_f(t)\,\mathrm{d}t = A_f \sum_{\mathcal{T}_f < n^{2/d} \leq 2\mathcal{T}_f} \lambda_f(n)\, n^{1/d-1/2}\, e\left(-\frac{d}{2}\left(\frac{n^2}{N_f}\right)^{1/d}\right) + O\big(T^{d/4}(\log T)^{\beta}\big) + O\left(T^{1-d/4} \max_{\alpha\in\{1,2\}} \left\{ \sum_{\frac{3\alpha}{4}\mathcal{T}_f \leq n^{2/d} \leq \frac{5\alpha}{4}\mathcal{T}_f} \frac{|\lambda_f(n)|}{|n^{2/d} - \alpha\mathcal{T}_f| + \sqrt{T}} \right\}\right),$$

where

$$A_f = \pi\, e\left(\frac{1}{8}\sum_{j=1}^{d} \mathrm{Re}(\kappa_j) + \frac{1}{8} - \frac{d}{16}\right)\sqrt{\frac{8}{\epsilon_f\, d\, N_f^{1/d}}}.$$

and the implied constants depend on the representation f.

To prove Lemma 3.1.1, we invoke the following the lemma from Gonek [9] as our main tool.

Lemma 3.1.2. *Let $\ell > 0$ and $a \in \mathbb{R}$ be fixed. For large x with $x < r \leq 2x$, we have*

$$\int_x^{2x} t^a \left(\frac{t}{re}\right)^{it\ell} \mathrm{d}t = \sqrt{\frac{2\pi}{\ell}}\, r^{a+\frac{1}{2}}\, e^{-ir\ell + \frac{\pi i}{4}} + \mathcal{E}(a,\ell,r,x),$$

where

$$\mathcal{E}(a,\ell,r,x) = O\big((\ell x)^a\big) + O\left(\frac{(\ell x)^{a+1}}{\ell\,|x-r| + \sqrt{\ell x}}\right) + O\left(\frac{(\ell x)^{a+1}}{\ell\,|2x-r| + \sqrt{\ell x}}\right).$$

When $r \leq x$ or $r > 2x$, there is no main term.

Proof. This is a straightforward consequence of [9, Lemma 2], after a suitable variable change. □

Proof of Lemma 3.1.1. Making the variable change $s = \frac{1}{2} + it$, we have

$$\int_T^{2T} Z_f(t)\,\mathrm{d}t = \frac{1}{i}\int_{1/2+iT}^{1/2+2iT} G_f(s)^{-1/2}\, L(f,s)\,\mathrm{d}s.$$

The function $G_f(s)$ is analytic and nonzero for $\mathrm{Re}(s) \geq 1/2$ and $\mathrm{Im}(s) \geq T$ when T is sufficiently large. So we can define a branch of $G_f(s)^{-1/2}$ in this region corresponding to the principal branch of the logarithm. Applying Cauchy's Theorem to the positively oriented rectangle with vertices

$$\left[\tfrac{1}{2} + iT, c + iT, c + 2iT, \tfrac{1}{2} + 2iT\right]$$

implies that

$$\int_T^{2T} Z_f(t)\,\mathrm{d}t = \frac{1}{i}\int_{c+iT}^{c+2iT} G_f(s)^{-1/2}\,L(f,s)\,\mathrm{d}s + H_1 - H_2,$$

where $c = 1 + 1/\log \mathcal{T}_f$ and

$$H_k = \frac{1}{i}\int_{1/2+kiT}^{c+kiT} G_f(s)^{-1/2}\,L(f,s)\,\mathrm{d}s$$

for $k = 1, 2$. Note that trivially

$$|H_k| \leq \left(c - \tfrac{1}{2}\right) \max_{\frac{1}{2}\leq\sigma\leq c} \left|G_f(\sigma + kiT)^{-1/2}\,L(f, \sigma + kiT)\right|. \tag{3.2}$$

Since $|G_f(\frac{1}{2} + it)| = 1$ for $t \in \mathbb{R}$, by (3.1) we see that

$$\left|G_f(\tfrac{1}{2} + it)^{-1/2}\,L(f, \tfrac{1}{2} + it)\right| \ll t^{d/4} \tag{3.3}$$

as $t \to \infty$. Also, by Stirling's formula for the gamma function, we have

$$\begin{aligned} &G_f(\sigma + it)^{-1/2} \\ &= \frac{e\left(\frac{1}{8}\sum_{j=1}^d \mathrm{Re}(\kappa_j) - \frac{d}{16}\right)}{\epsilon_f^{1/2}} \left(N_f^{1/d}\frac{t}{2\pi}\right)^{d(\sigma-\frac{1}{2})/2} \left(N_f^{1/d}\frac{t}{2\pi e}\right)^{itd/2} \left\{1 + O_f\left(\frac{1}{|t|}\right)\right\}, \end{aligned} \tag{3.4}$$

uniformly for σ in a compact interval and t sufficiently large. Again by (3.1), we deduce that

$$\left|G_f(c+it)^{-1/2}\, L(f, c+it)\right| \ll t^{d/4} \sum_{n\geq 1} \frac{|\lambda_f(n)|}{n^c} \ll t^{d/4} (\log T)^{\beta} \tag{3.5}$$

as $t \to \infty$. Using (3.3) and (3.5), an application of Phragmén-Lindelöf principle now implies that maximum in (3.2) occurs at $\sigma = c$ and thus

$$|H_1| + |H_2| \ll T^{d/4} (\log T)^{\beta}.$$

Next we expand $L(f, s)$ as an absolutely convergent Dirichlet series, interchange the sum and the integral, and then make the variable change $s = c + it$, to see that

$$\begin{aligned}
&\frac{1}{i} \int_{c+iT}^{c+2iT} G_f(s)^{-1/2}\, L(f, s)\, \mathrm{d}s = \sum_{n\geq 1} \frac{\lambda_f(n)}{n^c} \int_T^{2T} G_f(c+it)^{-1/2} n^{-it}\, \mathrm{d}t \\
&= \epsilon_f^{-1/2}\, e\Big(\tfrac{1}{8} \textstyle\sum_{j=1}^{d} \mathrm{Re}(\kappa_j) - \frac{d}{16}\Big) \\
&\times \sum_{n\geq 1} \frac{\lambda_f(n)}{n^c} \int_T^{2T} \left(N_f^{1/d} \frac{t}{2\pi}\right)^{d(c-\frac{1}{2})/2} \left(N_f^{1/d} \frac{t}{2\pi n^{2/d} e}\right)^{itd/2} \mathrm{d}t \\
&+ O\big(T^{d/4} (\log T)^{\beta}\big)\,.
\end{aligned}$$

Here the second equality comes after applying Stirling's formula for $G_f(c+it)^{-1/2}$ in (3.4) and then using (3.1) to obtain the big-O term. Making the variable change $N_f^{1/d}\, t/(2\pi) \mapsto t$ and then combining estimates, we have deduced that

$$\begin{aligned}
\int_T^{2T} Z_f(t)\, \mathrm{d}t = \epsilon_f^{-1/2}\, e\Big(\tfrac{1}{8} \textstyle\sum_{j=1}^{d} \mathrm{Re}(\kappa_j) - \frac{d}{16}\Big)\, \frac{2\pi}{N_f^{1/d}} \\
\times \sum_{n\geq 1} \frac{\lambda_f(n)}{n^c} \int_{\mathcal{T}_f}^{2\mathcal{T}_f} t^{d(c-\frac{1}{2})/2} \left(\frac{t}{n^{2/d} e}\right)^{it\pi d N_f^{-1/d}} \mathrm{d}t \\
+ O\big(T^{d/4} (\log T)^{\beta}\big)\,.
\end{aligned}$$

We now use Lemma 3.1.2 to estimate the integral on the right-hand side. The main term is

$$A_f \sum_{\mathcal{T}_f < n^{2/d} \le 2\mathcal{T}_f} \lambda_f(n)\, n^{1/d-1/2}\, e\left(-\frac{d}{2}\left(\frac{n^2}{N_f}\right)^{1/d}\right),$$

while the error term (using (3.1) and the notation in Lemma 3.1.2) is

$$\begin{aligned}
&\ll \sum_{n\ge 1} \frac{|\lambda_\pi(n)|}{n^c}\left\{T^{d/4} + \mathcal{E}\Big(\tfrac{d}{2}(c-\tfrac{1}{2}), \pi d N_\pi^{-1/d}, n^{2/d}, \mathcal{T}_\pi\Big)\right\} \\
&+ \sum_{n\ge 1} \frac{|\lambda_\pi(n)|}{n^c}\cdot \mathcal{E}\Big(\tfrac{d}{2}(c-\tfrac{1}{2}), \pi d N_\pi^{-1/d}, n^{2/d}, 2\mathcal{T}_\pi\Big) \\
&\ll T^{d/4}(\log T)^\beta + T^{1+d/4} \max_{\alpha\in\{1,2\}}\left\{\sum_{n\ge 1}\frac{|\lambda_\pi(n)|}{n^c}\frac{1}{|n^{2/d}-\alpha\mathcal{T}_\pi| + \sqrt{T}}\right\} \\
&\ll T^{d/4}(\log T)^\beta + T^{1-d/4} \max_{\alpha\in\{1,2\}}\left\{\sum_{\frac{3\alpha}{4}\mathcal{T}_\pi \le n^{2/d} \le \frac{5\alpha}{4}\mathcal{T}_\pi}\frac{|\lambda_\pi(n)|}{|n^{2/d}-\alpha\mathcal{T}_\pi| + \sqrt{T}}\right\}.
\end{aligned}$$

Combining estimates, the lemma now follows. □

3.2 Analysis for Dirichlet L-functions

Let χ be a primitive Dirichlet character (mod q). Recall that the Dirichlet L-function $L(s,\chi)$ is defined by

$$L(s,\chi) = \sum_{n\ge 1}\chi(n)n^{-s} = \prod_p (1-\chi(p)p^{-s})^{-1}$$

for $\mathrm{Re}(s) > 1$. We know that $L(s,\chi)$ is of degree $d = 1$ with conductor $N = q$ and the gamma factor is

$$\gamma(\chi, s) = \pi^{-s/2}\Gamma(\tfrac{1}{2}(s+\mathfrak{a}))$$

for integer $\mathfrak{a}$ such that $\chi(-1) = (-1)^{\mathfrak{a}}$. The functional equation of $L(s,\chi)$, in asymmetric form, is

$$L(s,\chi) = G_\chi(s)L(1-s,\overline{\chi})$$

for

$$G_\chi(s) = \epsilon_\chi q^{1/2-s}\pi^{-1/2+s}\frac{\Gamma(\frac{1}{2}(1-s+\mathfrak{a}))}{\Gamma(\frac{1}{2}(s+\mathfrak{a}))}$$

and $\epsilon_\chi = \frac{q^{1/2}}{i^{\mathfrak{a}}\tau(\chi)}$. Moreover, on the critical line by Phragmèn–Lindelöf we know

$$|L(\tfrac{1}{2}+it,\chi)| \ll (|t|+1)^{1/4},$$

and by a classical estimate we know

$$\sum_{n\geq 1}\frac{1}{n^{1+1/\log(qT)}} \ll_q \log T.$$

Combining these estimates with Lemma 3.1.1, we are ready to prove the main theorem.

3.2.1 Proof of Theorem 1.2.1

Applying above estimate into Lemma 3.1.1, we thus obtain that

$$\begin{aligned}\int_T^{2T} Z_\chi(t)\mathrm{d}t = A_\chi \sum_{\mathcal{T}_\chi < n^2 \leq 2\mathcal{T}_\chi} \chi(n)\sqrt{n}\, e\left(\frac{-n^2}{2q}\right) + O_q(T^{1/4}\log T) \\ + O_q\left(T^{3/4}\max_{\alpha\in\{1,2\}}\left\{\sum_{\frac{3\alpha}{4}\mathcal{T}_\chi < n^2 \leq \frac{5\alpha}{4}\mathcal{T}_\chi}\frac{1}{|n^2-\alpha\mathcal{T}_\chi|+\sqrt{T}}\right\}\right),\end{aligned} \tag{3.6}$$

where

$$A_\chi = \pi\, e\left(\frac{\mathfrak{a}}{8}+\frac{1}{16}\right)\sqrt{\frac{8}{\epsilon_\chi q}} \quad \text{and} \quad \mathcal{T}_\chi = \frac{qT}{2\pi}.$$

Here and throughout this proof, all implied constants are allowed to depend on q. It makes the calculations cleaner, if we first estimate the error terms and then sum over dyadic intervals (to recover the integral from 0 to T) before evaluating the main term. Since the second big-O term can be bounded in a similar manner when $\alpha = 1$ or $\alpha = 2$, we only give the details of how to estimate this term when $\alpha = 1$. In this

case, we partition the interval $[\sqrt{3\mathcal{T}_\chi/4}, \sqrt{5\mathcal{T}_\chi/4}]$ into three subintervals:

$$\begin{aligned} V_1 &= [\sqrt{\mathcal{T}_\chi} - \log T, \sqrt{\mathcal{T}_\chi} + \log T], \\ V_2 &= [\sqrt{3\mathcal{T}_\chi/4}, \sqrt{\mathcal{T}_\chi} - \log T), \text{ and} \\ V_3 &= (\sqrt{\mathcal{T}_\chi} + \log T, \sqrt{5\mathcal{T}_\chi/4}]. \end{aligned}$$

Accordingly, we define

$$S_j = T^{3/4} \sum_{n \in V_j} \frac{1}{|\mathcal{T}_\chi - n^2| + \sqrt{T}},$$

for $1 \le j \le 3$ so that this error term is $O(S_1 + S_2 + S_3)$. For $n \in V_1$, we have

$$S_1 \ll T^{3/4} \sum_{n \in V_1} \frac{1}{\sqrt{T}} \ll T^{1/4} |V_1| \ll T^{1/4} \log T.$$

For $n \in V_2$, by integral test we observe that

$$S_2 \ll T^{1/4} + T^{3/4} \int_{V_2} \frac{\mathrm{d}u}{\mathcal{T}_\chi + \sqrt{\mathcal{T}_\chi} - u^2}.$$

By partial fractions, the integral on the right-hand side is equal to

$$\frac{1}{2\sqrt{\mathcal{T}_\chi + \sqrt{\mathcal{T}_\chi}}} \int_{V_2} \left(\frac{1}{\sqrt{\mathcal{T}_\chi + \sqrt{\mathcal{T}_\chi}} - u} + \frac{1}{\sqrt{\mathcal{T}_\chi + \sqrt{\mathcal{T}_\chi}} + u} \right) \mathrm{d}u \ll \frac{\log T}{\sqrt{T}}.$$

Therefore, $S_2 \ll T^{1/4} \log T$. We can bound the contribution from the $n \in V_3$ similarly to $n \in V_2$ and conclude that $S_3 \ll T^{1/4} \log T$, as well. Estimating similarly when $\alpha = 2$, we conclude that

$$\int_T^{2T} Z_\chi(t) \, \mathrm{d}t \;=\; A_\chi \sum_{\sqrt{\mathcal{T}_\chi} < n \le \sqrt{2\mathcal{T}_\chi}} \chi(n) \sqrt{n} \, e\left(\frac{-n^2}{2q} \right) + O\big(T^{1/4} \log T \big) .$$

Summing dyadically over the intervals $[T/2,T],[T/4,T/2],[T/8,T/4],\dots$ and then using the definition of $\mathcal{T}_\chi$ and A_χ, we derive that

$$\int_0^T Z_\chi(t)\,\mathrm{d}t \;=\; \pi\, e\Big(\frac{\mathfrak{a}}{8}+\frac{1}{16}\Big)\sqrt{\frac{8}{\epsilon_\chi q}}\sum_{n\le\sqrt{\frac{qT}{2\pi}}}\chi(n)\,\sqrt{n}\,e\Big(\frac{-n^2}{2q}\Big)+O\big(T^{1/4}\log T\big)\,.$$

Recall that we let

$$S_1(\chi)=\sum_{n=1}^{2q}\chi(n)e\left(\frac{-n^2}{2q}\right).$$

Summing by parts implies that

$$\begin{aligned}
&\sum_{n\le x}\chi(n)n^{1/2}\,e\Big(\frac{-n^2}{2q}\Big)\\
&=x^{1/2}\sum_{n\le x}\chi(n)\,e\Big(\frac{-n^2}{2q}\Big)-\frac{1}{2}\int_1^x\left(\sum_{j=1}^{u}\chi(j)\,e\Big(\frac{-j^2}{2q}\Big)\right)\frac{1}{\sqrt{u}}\mathrm{d}u+O(x^{1/2})\\
&=\frac{S_1(\chi)}{2q}\,x^{3/2}-\frac{S_1(\chi)}{4q}\int_1^x\sqrt{u}\;\mathrm{d}u+O(x^{1/2})\\
&=\frac{S_1(\chi)}{3q}\,x^{3/2}+O(x^{1/2}).
\end{aligned}$$

Therefore, by taking $x=\sqrt{\mathcal{T}_\chi}$, we have proved

$$\begin{aligned}
\int_0^T Z_\chi(t)\mathrm{d}t&=\left(\frac{8}{q^{1/2}\tau(\chi)}\right)^{1/2}\frac{\pi\,e\big(\frac{\mathfrak{a}}{8}+\frac{1}{16}\big)\;S_1(\chi)}{3\,q}\left(\frac{qT}{2\pi}\right)^{3/4}+O(T^{1/4}\log T)\\
&=\frac{2^{3/4}\pi^{1/4}e(\frac{\mathfrak{a}}{8}+\frac{1}{16})}{3\,q^{1/2}\tau(\chi)^{1/2}}\,S_1(\chi)\,T^{3/4}+O(T^{1/4}\log T).
\end{aligned}$$

In fact, since we will prove (in Section 2.3) that if $\chi(-1)=-1$ then $S_1(\chi)=0$, we can drop $\mathfrak{a}$ in the leading coefficient, which completes the proof.

3.3 Analysis for degree two L-functions

In this section, we consider the case when f is a primitive classical automorphic form on $GL(2)$.

3.3.1 Proof for primitive holomorphic cusp forms

Let f be a Hecke-normalized primitive holomorphic cusp form, of weight $k \geq 1$, level q, with nebentypus ψ. Let its Fourier expansion at the cusp ∞ be

$$f(z) = \sum_{n \geq 1} \lambda_f(n) n^{(k-1)/2} e(nz).$$

Note that since it is Hecke-normalized, we have $\lambda_f(1) = 1$. The Hecke L-function of a Hecke-normalized primitive form f is defined by

$$L(f, s) = \sum_{n \geq 1} \lambda_f(n) n^{-s} = \prod_p (1 - \lambda_f(p) + \psi(p) p^{k-1-2s})^{-1}.$$

It is known that $L(f, s)$ is of degree $d = 2$ with conductor $N_f = q$ and the gamma factor is

$$\gamma(f, s) = \pi^{-s} \Gamma\left(\frac{s + (k-1)/2}{2}\right) \Gamma\left(\frac{s + (k+1)/2}{2}\right).$$

In particular, the functional equation is

$$L(f, s) = G_f(s) L(\overline{f}, 1 - s)$$

where

$$G_f(s) = \epsilon_f q^{1/2-s} \pi^{-1+2s} \frac{\Gamma(\frac{1}{2}(1 - s + (k-1)/2))}{\Gamma(\frac{1}{2}(s + (k-1)/2))} \frac{\Gamma(\frac{1}{2}(1 - s + (k+1)/2))}{\Gamma(\frac{1}{2}(s + (k+1)/2))}.$$

Next, by Phragmén-Lindelöf,

$$|L(f, \tfrac{1}{2} + it)| \ll (|t| + 1)^{1/2}.$$

Moreover, for $s = c = 1 + 1/\log(qT)$, we have

$$\sum_{n\geq 1} \frac{|\lambda_f(n)|}{n^c} \ll_f \log T.$$

Putting everything into Lemma 3.1.1, we obtain

$$\begin{aligned}\int_T^{2T} Z_f(t)\mathrm{d}t = A_f \sum_{\mathcal{T}_f < n \leq 2\mathcal{T}_f} \lambda_f(n) e\left(\frac{-n}{\sqrt{q}}\right) + O(T^{1/2}\log T) \\ + O\left(T^{1/2} \max_{\alpha\in\{1,2\}} \left\{ \sum_{\frac{3\alpha}{4}\mathcal{T}_f < n \leq \frac{5\alpha}{4}\mathcal{T}_f} \frac{|\lambda_f(n)|}{|n-\alpha\mathcal{T}_f| + \sqrt{T}} \right\}\right)\end{aligned}$$

where

$$A_f = \frac{2\pi e(\frac{k}{8})}{\epsilon_f^{1/2} q^{1/4}} \qquad \text{and} \qquad \mathcal{T}_f = \frac{q^{1/2}T}{2\pi}.$$

Here, we only give the details for estimating the second big-O term when $\alpha = 1$, since the error term can be bounded in a similar way when $\alpha = 1$ or 2. We partition the interval $[3\mathcal{T}_f/4, 5\mathcal{T}_f/4]$ into three subintervals:

$$\begin{aligned} V_1 &= [\mathcal{T}_f - \sqrt{T}, \mathcal{T}_f + \sqrt{T}], \\ V_2 &= [3\mathcal{T}_f/4, \mathcal{T}_f - \sqrt{T}), \qquad \text{and} \\ V_3 &= (\mathcal{T}_f + \log T, 5\mathcal{T}_f/4]. \end{aligned}$$

Accordingly, we define

$$E_j = T^{1/2} \sum_{n\in V_j} \frac{|\lambda_f(n)|}{|n-\mathcal{T}_f| + \sqrt{T}}$$

for $j = 1, 2, 3$. The second big-O term now is $O(E_1 + E_2 + E_3)$. By the classic work of Rankin and Shiu [35, Theorem 1], for any fixed $\varepsilon > 0$, we can derive (following

[3, proof of Lemma 2.2])

$$\sum_{x<n\leq x+h} |\lambda_f(n)| \ll_{\varepsilon,k,q} h(\log x)^{-\delta} \qquad \text{uniformly for } h \geq x^{\varepsilon}, \tag{3.7}$$

for some $\delta > 0$. Using this inequality, when $n \in V_1$ and $|n - \mathcal{T}_f| < \sqrt{T}$, by taking $h = \sqrt{T}$, we can deduce that

$$E_1 \ll_q \sum_{n\in V_1} |\lambda_f(n)| \ll \sqrt{T}(\log T)^{-\delta}.$$

To deal with E_2, we partition V_2 into

$$\bigcup_{j\geq 1} V_{2,j} = \bigcup_{j\geq 1} \Big(V_2 \cap [\mathcal{T}_f - 2^j\sqrt{T}, \mathcal{T}_f - 2^{j-1}\sqrt{T})\Big),$$

and correspondingly let

$$E_{2,j} = T^{1/2} \sum_{n\in V_{2,j}} \frac{|\lambda_f(n)|}{|n - \mathcal{T}_f| + \sqrt{T}}.$$

When $n \in V_{2,j}$, it is clear that $2^{j-1}\sqrt{T} \leq |n - \mathcal{T}_f| \leq 2^j\sqrt{T}$, thus we can deduce that

$$E_{2,j} \ll T^{1/2} \sum_{n\in V_{2,j}} \frac{|\lambda_f(n)|}{2^{j-1}\sqrt{T}} \ll 2^{-j} \sum_{n\in V_{2,j}} |\lambda_f(n)| \ll_q \sqrt{T}(\log T)^{-\delta},$$

where we applied (3.7) again by taking $h = 2^j T^{1/2}$. Since there are only $O_q(\log T)$ intervals of $V_{2,j}$, putting the estimates together, one obtains

$$E_2 \ll \sum_{j\geq 1} E_{2,j} \ll_q \sqrt{T}(\log T)^{1-\delta}.$$

In a similar manner, one can prove $E_3 \ll_q \sqrt{T}(\log T)^{1-\delta}$. Therefore, all error terms are $O(T^{1/2}\log T)$ and we can simplify the asymptotic formula to

$$\int_T^{2T} Z_f(t)\mathrm{d}t = A_f \sum_{\mathcal{T}_f < n \leq 2\mathcal{T}_f} \lambda_f(n) e(-n/\sqrt{q}) + O(T^{1/2}\log T).$$

To complete the proof, we next bound the sum in the above formula. A classical result of Wilton (see [17, Theorem 5.3]) shows that if f is a holomorphic cusp form, for any real α and $x \geq 1$ we have

$$\sum_{n \leq x} \lambda_f(n) e(\alpha n) \ll_f x^{1/2}\log x.$$

Bounding the main sum using the above inequality, we finally obtain the theorem for holomorphic cusp forms.

3.3.2 Proof for primitive Maass forms

Suppose f is a primitive Maass form of level q with nebentypus ψ which is an eigenfunction of the Laplace operator with eigenvalue $\lambda = \frac{1}{4} + r^2$, where $r \in \mathbb{R}$ or $ir \in [0, \frac{1}{2})$. Let $z = x + iy$. We write the Fourier expansion of f at ∞ to be

$$f(z) = \sqrt{y} \sum_{n \geq 1} \rho_f(n) K_{ir}(2\pi n y) SC(nx),$$

where $K_\nu(\cdot)$ is the K-Bessel function and $SC(x)$ is either $\sin(x)$ or $\cos(x)$. If $SC(x) = \sin(x)$, we say f is odd and if $SC(x) = \cos(x)$ we say f is even.
The L-function associated to f is defined by

$$L(f, s) = \sum_{n \geq 1} \rho_f(n) n^{-s}.$$

The gamma function is

$$\gamma(f,s) = \pi^{-s}\Gamma\left(\frac{s+\mathfrak{a}+ir}{2}\right)\Gamma\left(\frac{s+\mathfrak{a}-ir}{2}\right),$$

where $\mathfrak{a} = 0$ if f is even and $\mathfrak{a} = 1$ if f is odd. It satisfies the functional equation

$$L(f,s) = G_f(s)L(\overline{f}, 1-s),$$

where

$$G_f(s) = \epsilon_f q^{1/2-s}\pi^{-1+2s}\frac{\Gamma(\frac{1}{2}(1-s+\mathfrak{a}+ir))}{\Gamma(\frac{1}{2}(s+\mathfrak{a}+ir))}\frac{\Gamma(\frac{1}{2}(1-s+\mathfrak{a}-ir))}{\Gamma(\frac{1}{2}(s+\mathfrak{a}-ir))}.$$

On the half line, we have

$$|L(f, \tfrac{1}{2}+it)| \ll (|t|+1)^{1/2}.$$

By a classical result of Chandrasekharan and Harasimhan [7, equation(4.2)], using Rankin-Selberg method, for Maass form coefficients we have

$$\sum_{n\leq x}|\rho_f(n)|^2 = C_f x + O(x^{3/5}), \tag{3.8}$$

for some constant C_f. Applying Cauchy-Schwarz, summation by parts, and (3.8) we see that for $c = 1 + 1/\log(qT)$,

$$\begin{aligned}\sum_{n\geq 1}\frac{|\rho_f(n)|}{n^c} &\leq \Big(\sum_{n\geq 1}\frac{1}{n^c}\Big)^{1/2}\Big(\sum_{n\geq 1}\frac{|\rho_f(n)|^2}{n^c}\Big)^{1/2}\\ &\ll_q (\log T)^{1/2}\Big(\sum_{n\leq T}\frac{|\rho_f(n)|^2}{n^c} + \sum_{n>T}\frac{|\rho_f(n)|^2}{n^c}\Big)^{1/2}\\ &\ll_q \log T.\end{aligned}$$

Therefore, employing Lemma 3.1.1 we obtain

$$\int_T^{2T} Z_f(t)\,\mathrm{d}t = A_f \sum_{\mathcal{T}_f < n \le 2\mathcal{T}_f} \rho_f(n)\, e\!\left(\frac{-n}{\sqrt{q}}\right) + O\big(T^{1/2}\log T\big) + O\left(T^{1/2} \max_{\alpha\in\{1,2\}} \left\{ \sum_{\frac{3\alpha}{4}\mathcal{T}_f \le n \le \frac{5\alpha}{4}\mathcal{T}_f} \frac{|\rho_f(n)|}{|n-\alpha\mathcal{T}_f| + \sqrt{T}} \right\}\right),$$

where

$$A_f = 2\pi\, e\left(\tfrac{\mathfrak{a}}{4}\right) \epsilon_f^{-1/2} q^{-1/4} \qquad \text{and} \qquad \mathcal{T}_f = \frac{q^{1/2}T}{2\pi}.$$

Again, we only give the details for estimating the second big-O term when $\alpha = 1$, since the error term can be bounded in a similar way when $\alpha = 1$ or 2. We partition the interval $[3\mathcal{T}_f/4, 5\mathcal{T}_f/4]$ into three subintervals:

$$\begin{aligned} V_1 &= [\mathcal{T}_f - \sqrt{T}, \mathcal{T}_f + \sqrt{T}], \\ V_2 &= [3\mathcal{T}_f/4, \mathcal{T}_f - \sqrt{T}), \qquad \text{and} \\ V_3 &= (\mathcal{T}_f + \log T, 5\mathcal{T}_f/4]. \end{aligned}$$

Accordingly, we define

$$E_j = T^{1/2} \sum_{n\in V_j} \frac{|\rho_f(n)|}{|n-\mathcal{T}_f| + \sqrt{T}}$$

for $j = 1, 2, 3$. The second big-O term now is $O(E_1 + E_2 + E_3)$. We have to note that on short interval $[x, x+\sqrt{x}]$ we do not have the bound (3.7) for the sum of Maass form coefficients. Instead, if apply Cauchy-Schwarz with (3.8) and we have

$$\sum_{x\le n\le x+\sqrt{x}} |\rho_f(n)| \le x^{1/4} \left(\sum_{x\le n\le x+\sqrt{x}} |\rho_f(n)|^2 \right)^{1/2} \ll x^{\frac{11}{20}}. \tag{3.9}$$

Let us now look at the three errors. When $n \in V_1$ and $|n - \mathcal{T}_f| < \sqrt{T}$, the inequality (3.9) immediately implies

$$E_1 \ll_q \sum_{n \in V_1} |\rho_f(n)| \ll T^{\frac{11}{20}}.$$

To bound E_2, we again partition V_2 into

$$\bigcup_{j \geq 1} V_{2,j} = \bigcup_{j \geq 1} \Big(V_2 \cap [\mathcal{T}_f - 2^j \sqrt{T}, \mathcal{T}_f - 2^{j-1}\sqrt{T}) \Big),$$

and correspondingly let

$$E_{2,j} = T^{1/2} \sum_{n \in V_{2,j}} \frac{|\rho_f(n)|}{|n - \mathcal{T}_f| + \sqrt{T}}.$$

Similarly, when $n \in V_{2,j}$, we see $2^{j-1}\sqrt{T} \leq |n - \mathcal{T}_f|$ so that using (3.9) we obtain

$$E_{2,j} \ll T^{1/2} \sum_{n \in V_{2,j}} \frac{|\rho_f(n)|}{2^{j-1}\sqrt{T}} \ll 2^{-j} \sum_{n \in V_{2,j}} |\rho_f(n)| \ll_q T^{\frac{11}{20}}.$$

Since there are only $O_q(\log T)$ intervals of $V_{2,j}$, putting the estimates together, one obtains

$$E_2 \ll \sum_{j \geq 1} E_{2,j} \ll_q T^{\frac{11}{20}} \log T.$$

In a similar manner, one can prove $E_3 \ll_q T^{\frac{11}{20}} \log T$. Putting all errors together, we can simplify the asymptotic formula to

$$\int_T^{2T} Z_f(t) \mathrm{d}t = A_f \sum_{\mathcal{T}_f < n \leq 2\mathcal{T}_f} \lambda_f(n) e(-n/\sqrt{q}) + O(T^{\frac{11}{20}} \log T).$$

To complete the proof, it remains to bound the sum in the above formula. An estimate of Iwaniec [18, Theorem 8.1] shows that if f is a cusp form, for any real α

and $x \geq 1$ we have

$$\sum_{n \leq x} \rho_f(n) e(\alpha n) \ll_f x^{1/2} \log x,$$

which completes the proof.

4 PROOF OF THEOREM 1.2.2

4.1 Notation

Let χ be a primitive Dirichlet character (mod q). Recall that the Z-function associated to χ is defined to be

$$Z_\chi(t) = G_\chi(\tfrac{1}{2}+it)^{-1/2}\, L(\tfrac{1}{2}+it,\chi),$$

where

$$G_\chi(s) = \epsilon_\chi q^{1/2-s}\pi^{-1/2+s}\frac{\Gamma(\frac{1}{2}(1-s+\mathfrak{a}))}{\Gamma(\frac{1}{2}(s+\mathfrak{a}))}.$$

Throughout the chapter, we assume GRH and let γ denote a zero of $Z_\chi(t)$.

Note that $G_\chi(s)^{-1} = G_{\overline{\chi}}(1-s)$ and

$$\frac{G'_\chi}{G_\chi}(s) = \frac{G'_{\overline{\chi}}}{G_{\overline{\chi}}}(1-s).$$

On differentiating both sides of the definition of $Z(t)$, we see

$$\begin{aligned} Z'_\chi(t) &= \tfrac{-i}{2}G_{\overline{\chi}}(\tfrac{1}{2}-it)^{-1/2}G'_{\overline{\chi}}(\tfrac{1}{2}-it)L(\tfrac{1}{2}+it,\chi) + iG_{\overline{\chi}}(\tfrac{1}{2}-it)^{1/2}L'(\tfrac{1}{2}+it,\chi) \\ &= iG_{\overline{\chi}}(\tfrac{1}{2}-it)^{1/2}L(\tfrac{1}{2}+it)\left(-\frac{1}{2}\frac{G'_\chi}{G_\chi}(\tfrac{1}{2}+it) + \frac{L'}{L}(\tfrac{1}{2}+it,\chi)\right). \end{aligned}$$

For convenience, we define

$$\mathcal{G}_\chi(s) := -\frac{1}{2}\frac{G'_\chi}{G_\chi}(s) + \frac{L'}{L}(s,\chi).$$

With this notation, we can write $Z'_\chi(t)$ as

$$Z'_\chi(t) = iG_\chi(\tfrac{1}{2}+it)^{-1/2}L(\tfrac{1}{2}+it,\chi)\mathcal{G}_\chi(\tfrac{1}{2}+it) = iZ_\chi(t)\mathcal{G}_\chi(\tfrac{1}{2}+it)$$

and the functional equation implies

$$\mathcal{G}_\chi(s) = -\mathcal{G}_{\overline{\chi}}(1-s).$$

Here, we would like to mention that since $Z_\chi(t)$ is a real function for all real t, $Z'_\chi(t)$ is real as well, which implies that $i\mathcal{G}_\chi(\frac{1}{2}+it)$ is real for $t \in \mathbb{R}$.

4.2 Preliminary estimates for the proof of Theorem 1.2.2

In this section, we list the tools that we will establish and we prove Theorem 1.2.2. Let

$$\mathcal{M}(x,q) = \sum_{n\leq x}(\log *\Lambda)(n)\sqrt{n}\,\chi(n)e(\tfrac{-n^2}{2q})$$
$$\mathcal{S}(x,q) = \sum_{n\leq x}\log(n)^2\sqrt{n}\,\chi(n)e(\tfrac{-n^2}{2q}).$$

We first express $\sum_{0<\gamma<T} Z'_\chi(t)$ in terms of the above sums by establishing the following proposition.

Proposition 4.2.1. *Let χ be a primitive character modulo q. Let $Z_\chi(t)$ be the Z-function associated to χ and let γ be the zeros of $Z_\chi(t)$. Then, under GRH, we*

have

$$\sum_{0<\gamma<T} Z'_\chi(\gamma)$$
$$= 2^{3/2}\mathrm{Re}\left[e(\tfrac{5}{16})(q\epsilon_\chi)^{-1/2}(\mathcal{M}(\sqrt{qT/2\pi},q)-\mathcal{S}(\sqrt{qT/2\pi},q))\right]+O_q(T^{1/4}\log^3 T),$$

The whole Section 4.3 will be the proof of this proposition. Moreover, $\mathcal{M}(x,q)$ and $\mathcal{S}(x,q)$ can evaluated using summation by parts and Perron's formula.

Lemma 4.2.2. *For large x, we have*

$$\mathcal{S}(x,q)=\frac{S_1(\chi)}{27q}x^{3/2}(9\log^2 x-12\log x+8)+O_q(x^{\frac{1}{2}}\log^2 x).$$

Let

$$f_q(s)=\prod_{p|q}(1-p^{-s}),$$

and C_j be the Stieltjes constants. We now state the estimates for $\mathcal{M}(x,q)$.

Lemma 4.2.3. *When q is even, for large x we have*

$$\mathcal{M}(x,q)=\frac{S_1(\chi)}{54\,q}x^{3/2}P_2(\log x)+O_q(x(\log x)^{\frac{7}{2}}),$$

where $P_2(x)=a_2x^2+a_1x+a_0$ with

$$a_0=8+12C_0+18C_0^2+54C_1+12\frac{f'_q(1)}{f_q(1)}-18C_0\frac{f'_q(1)}{f_q(1)}+18\frac{f'_q(1)^2}{f_q(1)^2}-27\frac{f''_q(1)}{f_q(1)}$$
$$a_1=-12-18C_0-18\frac{f'_q(1)}{f_q(1)}$$
$$a_2=9.$$

Lemma 4.2.4. *When q is odd, for large x we have*

$$\mathcal{M}(x,q)=\frac{S_2(\chi)\chi(2)}{27\,q}x^{3/2}P_1(\log x)+O_q(x(\log x)^{\frac{7}{2}}).$$

where $P_1(x) = b_1 x + b_0$ *with*

$$b_0 = -12\log(2) + 18C_0\log(2) - 45\log^2(2) + 18\log(2)\frac{f_q'(1)}{f_q(1)},$$
$$b_1 = 18\log(2).$$

Proof of Theorem 1.2.2. Assuming the above tools, we can now easily deduce Theorem 1.2.2. For $\mathcal{T}_\chi = \frac{qT}{2\pi}$, when q is odd, we have

$$\sum_{0<\gamma<T} Z_\chi'(\gamma) = A_\chi \mathcal{T}_\chi^{\frac{3}{4}}(\log \mathcal{T}_\chi + C_q) + O_q(T^{\frac{1}{2}}(\log T)^{\frac{7}{2}}),$$

where

$$A_\chi = \mathrm{Re}[ie(\tfrac{1}{16})\tau(\chi)^{-\frac{1}{2}}\chi(2)S_2(\chi)]\,\frac{2^{\frac{3}{2}}\log(2)}{3q^{\frac{5}{4}}}$$

and

$$C_q = 2C_0 - 5\log(2) - \frac{4}{3} - 2\sum_{p|q}\frac{p\log p}{p-1}.$$

When q is even, we have shown that

$$\sum_{0<\gamma<T} Z_\chi'(\gamma) = \mathrm{Re}[ie(\tfrac{1}{16})\tau(\chi)^{-1/2}S_1(\chi)]\cdot \mathcal{T}_\chi^{\frac{3}{4}} P_2^*(\log \mathcal{T}_\chi) + O_q(T^{\frac{1}{2}}(\log T)^{\frac{7}{2}}),$$

for some quadratic polynomial $P_2^*(x) \in \mathbb{R}[x]$ with coefficients depending on q. Since $Z_\chi(t)$ is real-valued for real t, the integral $\int_0^T Z_\chi(t)\,dt$ is real. Recall from Theorem 1.2.1, that $e(\frac{1}{16})\tau(\chi)^{-1/2}S_1(\chi)$ times a real number is the leading coefficient in the asymptotic formula for $\int_0^T Z_\chi(t)\,dt$. Hence $e(\frac{1}{16})\tau(\chi)^{-1/2}S_1(\chi) \in \mathbb{R}$ and so $ie(\frac{1}{16})\tau(\chi)^{-1/2}S_1(\chi)$ is purely imaginary. Therefore $\mathrm{Re}[ie(\frac{1}{16})\tau(\chi)^{-1/2}S_1(\chi)] = 0$, which completes the proof of Theorem 1.2.2. □

4.3 Proof of Proposition 4.2.1

We begin the proof with the formula

$$Z'_\chi(t) = iG_{\overline{\chi}}(\tfrac{1}{2} - it)^{1/2} L(\tfrac{1}{2} + it, \chi) \left(-\frac{1}{2} \frac{G'_\chi}{G_\chi}(\tfrac{1}{2} + it) + \frac{L'}{L}(\tfrac{1}{2} + it, \chi) \right).$$

For convenience, we define

$$\mathcal{G}_\chi(s) := -\frac{1}{2} \frac{G'_\chi}{G_\chi}(s) + \frac{L'}{L}(s, \chi).$$

With this notation, we can rewrite the functional equation as

$$\mathcal{G}_\chi(s) = -\mathcal{G}_{\overline{\chi}}(1 - s).$$

Let $c = 1 + \frac{1}{\log(qT)}$. Since we assume GRH, applying residue theorem, the sum $\sum_{0<\gamma<T} Z'_\chi(\gamma)$ hence can be expressed as a contour integral over the positive oriented rectangle $\square$ with vertices $c + i, c + iT, 1 - c + iT$, and $1 - c + i$. Specifically, we have

$$\sum_{0<\gamma<T} Z'_\chi(\gamma) = \frac{1}{2\pi i} \int_\square iG_\chi(s)^{-1/2} L(s, \chi) \mathcal{G}_\chi(s) \frac{\xi'_\chi}{\xi_\chi}(s) ds. \tag{4.1}$$

By Phragmén-Lindelöf for $s = \beta + iT$, $1 - c \leq \beta \leq c$, we have

$$\left| G_\chi(s)^{-1/2} L(s, \chi) \mathcal{G}_\chi(s) \frac{\xi'_\chi}{\xi_\chi}(s) \right| \ll_q T^{1/4} \log^3 T,$$

which implies that the horizontal integrals are $O_q(T^{1/4} \log^3 T)$. Next, we focus on evaluating the vertical contours. Let the vertical integral of $\mathrm{Re}(s) = c$ be

$$I = \frac{1}{2\pi} \int_{c+i}^{c+iT} G_\chi(s)^{-1/2} L(s, \chi) \mathcal{G}_\chi(s) \frac{\xi'_\chi}{\xi_\chi}(s) ds.$$

The integral of $\mathrm{Re}(s) = 1 - c$ is

$$\begin{aligned}
&\frac{-i}{2\pi i}\int_{1-c+i}^{1-c+iT} G_\chi(s)^{-1/2} L(s,\chi)\mathcal{G}_\chi(s)\,\frac{\xi_\chi'}{\xi_\chi}(s)ds \\
&\quad= \frac{1}{2\pi}\int_{c-i}^{c-iT} G_\chi(1-s)^{-1/2} L(1-s,\chi)\mathcal{G}_\chi(1-s)\,\frac{\xi_\chi'}{\xi_\chi}(1-s)ds \\
&\quad= \frac{1}{2\pi}\int_{c-i}^{c-iT} G_{\overline{\chi}}(s)^{-1/2} L(s,\overline{\chi})\mathcal{G}_{\overline{\chi}}(s)\,\frac{\xi_{\overline{\chi}}'}{\xi_{\overline{\chi}}}(s)ds \\
&\quad= \frac{-1}{2\pi}\int_{c+i}^{c+iT} G_{\overline{\chi}}(\overline{s})^{-1/2} L(\overline{s},\overline{\chi})\mathcal{G}_{\overline{\chi}}(\overline{s})\,\frac{\xi_{\overline{\chi}}'}{\xi_{\overline{\chi}}}(\overline{s})\,ds = \overline{I}.
\end{aligned}$$

Therefore, the original sum can expressed as

$$\sum_{0<\gamma<T} Z_\chi'(\gamma) = 2\mathrm{Re}(I) + O_q(T^{1/4}\log^3 T).$$

Next we shall estimate integral I using stationary phase. Stirling's formula implies that for $s = \sigma + it$ and $t > 0$,

$$G_\chi(s) = \epsilon_\chi\, e^{\pi i(\frac{1}{4}-\frac{\mathfrak{a}}{2})}\left(\frac{qt}{2\pi}\right)^{1/2-\sigma}\left(\frac{qt}{2\pi e}\right)^{-it}\left\{1 + O\left(\frac{1}{t}\right)\right\}.$$

Put $s = c + it$, we hence have

$$G_\chi(s)^{-1/2} = G_{\overline{\chi}}(1-s)^{1/2} = \epsilon_\chi^{-1/2} e^{\pi i(\frac{\mathfrak{a}}{4}-\frac{1}{8})}\left(\frac{qt}{2\pi}\right)^{c/2-1/4}\left(\frac{qt}{2\pi e}\right)^{it/2}\left\{1 + O\left(\frac{1}{t}\right)\right\}.$$

Since $\frac{\Gamma'(s)}{\Gamma(s)} = \log s + O(\frac{1}{|s|})$ for $|\arg s| < \pi - \delta$ and $|s| \geq 1/2$, for fixed σ and $t > 0$

$$\frac{G_\chi'(s)}{G_\chi(s)} = \frac{G_{\overline{\chi}}'(1-s)}{G_{\overline{\chi}}(1-s)} = -\log\left(\frac{qt}{2\pi}\right) + O\left(\frac{1}{t}\right).$$

Moreover, by the functional equation, for fixed σ and $t > 0$,

$$\frac{\xi_\chi'(s)}{\xi_\chi(s)} = \frac{1}{2}\log\left(\frac{qt}{2\pi}\right) + \frac{L'}{L}(s,\chi) + O\left(\frac{1}{t}\right).$$

Putting these estimates into I, we observe that

$$\begin{aligned} I &= \frac{i}{2\pi}\int_1^T G_\chi(c+it)^{-1/2}L(c+it,\chi)\left(-\frac{1}{2}\frac{G_\chi'}{G_\chi}(c+it)+\frac{L'}{L}(c+it,\chi)\right) \\ &\quad\times\left(\frac{1}{2}\log\left(\frac{qt}{2\pi}\right)+\frac{L'}{L}(c+it,\chi)\right)dt+O(T^{1/4}\log^3 T) \\ &= J_1+J_2+J_3+O(T^{1/4}\log^3 T), \end{aligned}$$

where

$$J_1=\frac{ie(\frac{\mathfrak{a}}{8}-\frac{1}{16})}{8\pi\epsilon_\chi^{1/2}}\sum_{n=1}^\infty \chi(n)n^{-c}\int_1^T\left(\frac{qt}{2\pi}\right)^{\frac{c}{2}-\frac{1}{4}}\left(\frac{qt}{2\pi n^2 e}\right)^{\frac{it}{2}}\left(\log\frac{qt}{2\pi}\right)^2 dt,$$

$$J_2=-\frac{ie(\frac{\mathfrak{a}}{8}-\frac{1}{16})}{2\pi\epsilon_\chi^{1/2}}\sum_{n=1}^\infty \log(n)\chi(n)n^{-c}\int_1^T\left(\frac{qt}{2\pi}\right)^{\frac{c}{2}-\frac{1}{4}}\left(\frac{qt}{2\pi n^2 e}\right)^{\frac{it}{2}}\left(\log\frac{qt}{2\pi}\right) dt,$$

and

$$J_3=\frac{ie(\frac{\mathfrak{a}}{8}-\frac{1}{16})}{2\pi\epsilon_\chi^{1/2}}\sum_{n=1}^\infty (\log *\Lambda)(n)\chi(n)n^{-c}\int_1^T\left(\frac{qt}{2\pi}\right)^{\frac{c}{2}-\frac{1}{4}}\left(\frac{qt}{2\pi n^2 e}\right)^{\frac{it}{2}} dt.$$

To estimate these three integrals, we invoke a stationary phase.

Lemma 4.3.1 (stationary phase)**.** *Let T be a large number. If $1\le r\le T$, then*

$$\begin{aligned}\int_1^T\Big(\frac{t}{re}\Big)^{\frac{it}{2}}\Big(\frac{qt}{2\pi}\Big)^a\Big(\log\frac{qt}{2\pi}\Big)^m dt &= 2^{1-a}q^a\pi^{1/2-a}r^{a+1/2}e^{-ir/2+\pi i/4}\Big(\log\frac{qt}{2\pi}\Big)^m \\ &\quad+E(r,T)(\log T)^m,\end{aligned}$$

where

$$E(r,T)=O_q(T^a)+O_q\Big(\frac{T^{a+1}}{|T-r|+T^{\frac{1}{2}}}\Big).$$

Otherwise, there is no main term.

Proof. This is [9, Lemma 3] under a variable change. □

Putting this into J_1, J_2 and J_3, we obtain that

$$J_1 = \tfrac{-1}{2} J_2 = \frac{ie(\frac{\mathfrak{a}}{8} + \frac{1}{16})2^{1/2}}{(q\,\epsilon_\chi)^{1/2}} \sum_{n \le \sqrt{qT/2\pi}} \log(n)^2 \sqrt{n}\,\chi(n) e(\tfrac{-n^2}{2q}) + E_1(T),$$

and

$$J_3 = \frac{ie(\frac{\mathfrak{a}}{8} + \frac{1}{16})2^{1/2}}{(q\,\epsilon_\chi)^{1/2}} \sum_{n \le \sqrt{qT/2\pi}} (\log * \Lambda)(n) \sqrt{n}\,\chi(n) e(\tfrac{-n^2}{2q}) + E_2(T).$$

Therefore, the original sum can be written as

$$\sum_{0<\gamma<T} Z'_\chi(\gamma) = 2\mathrm{Re}(J_3) - 2\mathrm{Re}(J_1) + E_1(T) + E_2(T).$$

It remains to estimate errors $E_1(T)$ and $E_2(T)$. Note that

$$\begin{aligned} E_1(T) &\ll_q \sum_{n=1}^{\infty} \frac{T^{\frac{c}{2}-\frac{1}{4}} (\log T)^2}{n^c} + \sum_{n=1}^{\infty} n^{-c} \cdot \frac{T^{\frac{c}{2}+\frac{3}{4}} \log^2 T}{|qT - 2\pi n^2| + T^{1/2}} \\ &\ll_q T^{1/4} \log^3 T + T^{5/4} \log^2 T \sum_{n=1}^{\infty} \frac{1}{n^c(|qT - 2\pi n^2| + T^{1/2})}. \end{aligned}$$

When $n \in U_0 = \{n : |qT - 2\pi n^2| < T^{1/2}\}$,

$$\sum_{n \in U_0} \frac{1}{n^c(|qT - 2\pi n^2| + T^{1/2})} \ll T^{-1/2} \sum_{n \in U_0} n^{-c} \ll T^{-1}|U_0| \ll T^{-1}.$$

When $n \in U_\infty = \{n : |qT - 2\pi n^2| \ge T\}$,

$$\sum_{n \in U_\infty} \frac{1}{n^c(|qT - 2\pi n^2| + T^{1/2})} \ll T^{-1} \sum_{n \in U_\infty} n^{-c} \ll T^{-1} \log T.$$

When $n \in U_j = \{n : 2^{j-1} T^{1/2} \le |qT - 2\pi n^2| < 2^j T^{1/2}\}$, for $1 \le j \le \lceil \frac{\log T}{2 \log 2} \rceil$,

$$\sum_{n \in U_j} \frac{1}{n^c(|qT - 2\pi n^2| + T^{1/2})} \ll 2^{-j+1} T^{-1/2} \sum_{n \in U_j} n^{-c} \ll 2^{-j} T^{-1} |U_j| \ll T^{-1}.$$

Combining all estimates together, we see that $E_1(T) \ll_q T^{1/4}\log^3 T$. Similarly, we can obtain $E_2(T) \ll_q T^{1/4}\log^3 T$. Therefore Proposition 4.2.1 follows.

4.4 Evaluation of the sums using Perron

4.4.1 Generating Series

By a simple calculation, we observe that

$$\sum_{(n,q)=1}\frac{\Lambda(n)}{n^s} = -\frac{d}{ds}\log\left(\zeta(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right)\right) = -\frac{\zeta'(s)}{\zeta(s)} - \sum_{p|q}\frac{\log(p)}{p^s-1}$$

and

$$\begin{aligned}\sum_{(n,q)=1}\frac{\log n}{n^s} &= -\frac{d}{ds}\left(\zeta(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right)\right)\\ &= -\zeta'(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right) - \zeta(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right)\cdot\sum_{p|q}\frac{\log p}{p^s-1}.\end{aligned}$$

Therefore

$$\sum_{(n,q)=1}\frac{\Lambda * \log(n)}{n^s} = \zeta(s)\,\frac{f_q'(s)^2}{f_q(s)} + 2\zeta'(s)f_q'(s) + \frac{\zeta'(s)^2}{\zeta(s)}f_q(s),$$

where

$$f_q(s) = \prod_{p|q}\left(1-\frac{1}{p^s}\right).$$

4.4.2 Proof of Lemma 4.2.2

Since $S_1(\chi) = \sum_{n\le 2q}\chi(n)e(\frac{-n^2}{2q})$, we write

$$\sum_{n\le x}\chi(n)e(\tfrac{-n^2}{2q}) = \frac{x}{2q}S_1(\chi) + O(q).$$

With this formula, on summation by parts we can deduce that

$$\begin{aligned}\mathcal{S}(x,q) &= x^{\frac{1}{2}}\log^2 x\cdot\sum_{n\le x}\chi(n)e(\tfrac{-n^2}{2q}) - \int_1^x(\tfrac{1}{2}t^{-\frac{-1}{2}}\log^2 t + 2t^{-\frac{1}{2}}\log t)\sum_{n\le t}\chi(n)e(\tfrac{-n^2}{2q})dt\\ &= \frac{x^{\frac{3}{2}}\log^2 xS_1(\chi)}{2q} - \frac{S_1(\chi)}{2q}\int_1^x(\tfrac{1}{2}t^{\frac{1}{2}}\log^2 t + 2t^{\frac{1}{2}}\log t)dt + O_q(x^{\frac{1}{2}}\log^2 x)\\ &= \frac{S_1(\chi)}{2q}x^{\frac{3}{2}}\left(\log^2 x - \frac{1}{27}(9\log^2 x + 24\log x - 16)\right) + O_q(x^{\frac{1}{2}}\log^2 x)\\ &= \frac{S_1(\chi)}{27\,q}x^{\frac{3}{2}}(9\log^x - 12\log x + 8) + O_q(x^{\frac{1}{2}}\log^2 x),\end{aligned}$$

which completes the proof.

4.4.3 Proof of Lemma 4.2.3

When q is even, we have $(n,q) = (n,2q) = 1$. Applying the identity

$$e\Big(\frac{-n^2}{2q}\Big) = \frac{1}{\varphi(2q)}\sum_{\xi(2q)}\tau(\xi)\overline{\xi}(-n^2),$$

we can deduce that

$$\mathcal{M}(x,q) = \frac{1}{\varphi(2q)}\sum_{\xi(2q)}\tau(\xi)\overline{\xi}(-1)\sum_{\substack{n\le x\\(n,2q)=1}}(\Lambda*\log)(n)\sqrt{n}\,(\chi\cdot\overline{\xi}^2)(n). \tag{4.2}$$

Let $\psi = \chi\cdot\overline{\xi}^2$. For convenience, we let

$$F_1(s,\psi) = \sum_{(n,q)=1}\frac{(\Lambda*\log)(n)\psi(n)}{n^s} = L(s,\psi)\,\frac{f_q'(s)^2}{f_q(s)} + 2L'(s,\psi)f_q'(s) + \frac{L'(s,\psi)^2}{L(s,\psi)}f_q(s).$$

By Perron (see [27, Theorem 5.2]),

$$\sum_{n\le x}(\Lambda*\log)(n)\psi(n)\sqrt{n} = \frac{1}{2\pi i}\int_{c-iT}^{c+iT}F_1(s-\tfrac{1}{2},\psi)\frac{x^s}{s}ds + O(\log^2 x) + R,$$

where $c = \frac{3}{2} + \frac{1}{\log x}$

$$\begin{aligned} R &\ll \sum_{x/2<n<2x, n\neq x} \sqrt{n}\log^2 n \, \min\left(1, \frac{x}{T|x-n|}\right) + \frac{4^c + x^c}{T}\sum_n \frac{\log^2 n\sqrt{n}}{n^c} \\ &\ll \sum_{x/2<x<2x, |x-n|\geq \frac{x}{T}} \frac{x^{3/2}\log^2 n}{T|x-n|} + \frac{x^{3/2}(\log x)^2}{T} + \frac{x^{3/2}(\log x)^3}{T} \\ &\ll \frac{x^{3/2}(\log x)^2}{T}(\log T + \log x). \end{aligned}$$

Now shift the contour to $\mathrm{Re}(s) = \frac{1}{2} + \frac{1}{\log x}$. It follows that

$$\begin{aligned} \sum_{n\leq x}(\Lambda * \log)(n)\psi(n)\sqrt{n} = \operatorname*{Res}_{s=3/2}\Big(F_1(s-\tfrac{1}{2},\psi)\frac{x^s}{s}\Big) + \frac{1}{2\pi i}\int_{\frac{1}{2}+\frac{1}{\log x}-iT}^{\frac{1}{2}+\frac{1}{\log x}+iT} F_1(s,\psi)\frac{x^s}{s}ds \\ + O(\log^2 x) + O\left(\frac{x^{3/2}}{T}((\log x)^3 + (\log x)^2\log T + (\log T)^3)\right), \end{aligned}$$

where the residue is zero if ψ is not principal. Moreover, by the classical estimates we know

$$\int_{\frac{1}{2}+\frac{1}{\log x}}^{\frac{1}{2}+\frac{1}{\log x}+iT}\left|\frac{L'(s,\psi)}{L(s,\psi)}\right|^2 ds \ll_q T(\log T)^2, \qquad \int_{\frac{1}{2}+\frac{1}{\log x}}^{\frac{1}{2}+\frac{1}{\log x}+iT}|L'(s,\psi)|^2\, ds \ll_q T(\log T)^3.$$

Using Cauchy-Schwarz, we can obtain that

$$\begin{aligned} &\left|\int_{\frac{1}{2}+\frac{1}{\log x}}^{\frac{1}{2}+\frac{1}{\log x}+iT}\frac{L'(s,\psi)^2}{L(s,\psi)}\frac{x^s}{s}ds\right| \\ &\ll x^{\frac{1}{2}}\cdot\left(\int_0^T\left|\frac{L'(\frac{1}{2}+\frac{1}{\log x}+it,\psi)}{L((\frac{1}{2}+\frac{1}{\log x}+it,\psi)}\right|^2\frac{1}{t}dt\right)^{\frac{1}{2}}\cdot\left(\int_0^T\left|L'(\tfrac{1}{2}+\tfrac{1}{\log x}+it,\psi)\right|^2\frac{dt}{t}\right)^{1/2} \\ &\ll_q x^{\frac{1}{2}}(\log T)^{\frac{3}{2}}(\log T)^2 \ll_q x^{\frac{1}{2}}(\log T)^{\frac{7}{2}}. \end{aligned}$$

To balance all errors, we set $T = x$. Therefore, we obtain the following lemma.

Lemma 4.4.1. *Let q be a positive integer and ψ be a character modulo q. Further let $f_q(s) = \prod_{p|q}(1-p^{-s})$ and*

$$F_q(s) = \zeta(s)\,\frac{f_q'(s)^2}{f_q(s)} + 2\zeta'(s)f_q'(s) + \frac{\zeta'(s)^2}{\zeta(s)}f_q(s).$$

Then we have

$$\sum_{n\le x}(\Lambda{*}\log)(n)\psi(n)\sqrt{n} = \begin{cases} \operatorname*{Res}_{s=3/2}(F_q(s-\frac{1}{2})\frac{x^s}{s}) + O_q(x^{\frac{1}{2}}(\log x)^{\frac{7}{2}}), & \text{when } \psi \text{ is principal,} \\ O_q(x^{\frac{1}{2}}(\log x)^{\frac{7}{2}}), & \text{otherwise.} \end{cases}$$

In order to calculate the main term, by Lemma 4.4.1 we now assume $\chi = \xi^2$ so that $\chi\overline{\xi}^2 = \mathbf{1}_{2q} = \mathbf{1}_q$ for even q. Consequently, we can simplify (4.2) to

$$\mathcal{M}(x,q) = \frac{S_1(\chi)}{2\,\varphi(q)} \sum_{\substack{n<x \\ (n,q)=1}} (\Lambda * \log)(n)\sqrt{n} + O(x(\log x)^{\frac{7}{2}}).$$

Using *Mathematica*, one can check that the residue is

$$\begin{aligned} \operatorname*{Res}_{s=3/2}\Big(F_q(s-\tfrac{1}{2})\frac{x^s}{s}\Big) &= \frac{2x^{3/2}}{3}\frac{f_q'(1)^2}{f_q(1)} - \frac{4x^{3/2}}{9}(-2f_q'(1) + 3f_q''(1) + 3f_q'(1)\log(x)) \\ &+ \frac{x^{3/2}}{27}(8f_q(1) + 12C_0f_q(1) + 18C_0^2f_q(1) + 54f_q(1)C_1 - 12f_q'(1) - 18C_0f_q'(1) \\ &+ 9f_q''(1) - 12f_q(1)\log(x) - 18C_0f_q(1)\log(x) + 18f_q'(1)\log(x) + 9f_q(1)\log^2(x)). \end{aligned} \tag{4.3}$$

Finally, putting it into the main sum, we obtain

$$\mathcal{M}(x,q) = \frac{S_1(\chi)}{54\,q}x^{3/2}P_2(\log x) + O(x(\log x)^{\frac{7}{2}}),$$

where $P_2(x) = a_2x^2 + a_1x + a_0$ with

$$a_0 = 8 + 12C_0 + 18C_0^2 + 54C_1 + 12\frac{f_q'(1)}{f_q(1)} - 18C_0\frac{f_q'(1)}{f_q(1)} + 18\frac{f_q'(1)^2}{f_q(1)^2} - 27\frac{f_q''(1)}{f_q(1)}$$
$$a_1 = -12 - 18C_0 - 18\frac{f_q'(1)}{f_q(1)}, \qquad a_2 = 9,$$

which completes the proof.

4.4.4 Proof of Lemma 4.2.4

When q is odd, we split the sum into two parts and let

$$\mathcal{M}_0(x,q) = \sum_{2n<x} (\log * \Lambda)(2n)\sqrt{2n}\chi(2n)e(\tfrac{-2n^2}{q})$$
$$\mathcal{M}_1(x,q) = \sum_{\substack{n<x \\ (n,2q)}} (\log * \Lambda)(n)\sqrt{n}\chi(n)e(\tfrac{-n^2}{2q}).$$

Similarly, applying the proof of Lemma 4.4.1, the main term exists only if $\chi = \xi^2$. Now assume $\chi\overline{\xi}^2 = \mathbf{1}_q$, we can write $\mathcal{M}_0(x,q)$ as

$$\begin{aligned}\mathcal{M}_0(x,q) &= \frac{\chi(2)}{\varphi(q)} \sum_{\xi^2=\chi} \tau(\xi)\overline{\xi}(-2) \sum_{2n<x} (\log * \Lambda)(2n)\sqrt{2n}\,\mathbf{1}_q(2n) + O(x(\log x)^{\frac{7}{2}}) \\ &= \frac{S_2(\chi)\chi(2)}{\varphi(q)} \sum_{\substack{n<x \\ (n,q)=1 \\ 2|n}} (\log * \Lambda)(n)\sqrt{n} + O(x(\log x)^{\frac{7}{2}}).\end{aligned}$$

Moreover, by writing $\sum_{\xi^2=\chi} \tau(\xi)\overline{\xi}(-1) = \sum_{(m,2q)=1} \chi(m)e(\frac{-m^2}{2q})$, we obtain

$$\mathcal{M}_1(x,q) = \sum_{\substack{1\le m\le 2q \\ (m,2q)=1}} \chi(m)e(\tfrac{-m^2}{2q}) \cdot \frac{1}{\varphi(q)} \sum_{\substack{n<x \\ (n,2q)}} (\log * \Lambda)(n)\sqrt{n} + O(x(\log x)^{\frac{7}{2}}).$$

Here we note that if q is odd, then

$$\sum_{\substack{1\leq m\leq 2q\\(m,2q)=1}} \chi(m)e(\tfrac{-m^2}{2q}) = -S_2(\chi)\chi(2).$$

Hence,

$$\mathcal{M}_1(x,q) = -\frac{S_2(\chi)\chi(2)}{\varphi(q)} \sum_{\substack{n<x\\(n,2q)=1}} (\log *\Lambda)(n)\sqrt{n} + O(x(\log x)^{\frac{7}{2}}).$$

Furthermore, we observe that

$$\begin{aligned}\sum_{\substack{n<x\\(n,q)=1\\2|n}} (\Lambda * \log)(n)\sqrt{n} &= \left(\sum_{\substack{n<x\\(n,q)=1}} - \sum_{\substack{n<x\\(n,2q)=1}}\right)(\Lambda * \log)(n)\sqrt{n}\\ &= \operatorname*{Res}_{s=3/2}\left(F_q(s-\tfrac{1}{2})\frac{x^s}{s}\right) - \operatorname*{Res}_{s=3/2}\left(F_{2q}(s-\tfrac{1}{2})\frac{x^s}{s}\right) + O(x(\log x)^{\frac{7}{2}}).\end{aligned}$$

Now combining $\mathcal{M}_0(x,q)$ and $\mathcal{M}_1(x,q)$, we obtain that

$$\begin{aligned}&\mathcal{M}(x,q)\\ &= \frac{S_2(\chi)\chi(2)}{\varphi(q)}\left[\operatorname*{Res}_{s=3/2}\left(F_q(s-\tfrac{1}{2})\frac{x^s}{s}\right) - 2\operatorname*{Res}_{s=3/2}\left(F_{2q}(s-\tfrac{1}{2})\frac{x^s}{s}\right)\right] + O(x(\log x)^{\frac{7}{2}}).\end{aligned}$$

Finally, by computing the difference of two residues (using mathematica), we thus complete the proof.

5 ON THEOREMS OF WIRSING AND SANDERS

5.1 Wirsing's argument for Cartesian products

Let $(q_k)_{k=1}^{\infty}$ be a sequence of positive integers. Write $I_k = \{0, 1, \ldots, q_k - 1\}$. Define

$$Q_n = \prod_{k=1}^{n} I_k.$$

The *Hamming distance* between two elements $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ of Q_n is

$$d(\mathbf{x}, \mathbf{y}) := |\{1 \leq i \leq n : x_i \neq y_i\}|. \tag{5.1}$$

For a set $A \subset Q_n$ and $r \geq 0$, we define the neighborhood of A with radius r as

$$B(A, r) = B_n(A, r) = \{\mathbf{x} \in Q_n : \text{ there exists } \mathbf{y} \in A \text{ such that } d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

We will prove the following:

Theorem 5.1.1. *For any set $A \subset Q_n$, we have*

$$|B_n(A, 1)| \geq |A| + \sqrt{\frac{2}{\sum_{i=1}^{n}(q_i - 1)}}|A| \left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.2}$$

Remark 2. *After we proved the theorem, we learned that in the special case $Q_n = \{0, 1\}^n$, Theorem 5.1.1 appeared as* [6, Theorem 3] *with a very similar argument.*

We will need the following estimate in the proof of Theorem 5.1.1.

Lemma 5.1.2. *For any nonnegative real numbers $x_1, \ldots, x_m$, we have*

$$\sum_{1 \le i \le j \le m} (x_i + x_{i+1} + \cdots + x_j)^2 \le m \left(\sum_{i=1}^{m} (x_1 + \cdots + x_i) \right)^2 \tag{5.3}$$

Proof. This follows simply from comparing coefficients. For $1 \le k \le m$, the coefficient of x_k^2 in LHS is $k(m+1-k)$, while its coefficient in RHS is $m(m+1-k)^2$. For $1 \le k < l \le m$, the coefficient of $x_k x_l$ in LHS is $2k(m+1-l)$, while its coefficient in RHS is $2m(m+1-l)(m+1-k)$. □

Proof of Theorem 5.1.1. Let ζ_n be a sequence of positive reals which will be determined later. Ultimately, we will make the choice $\zeta_n = \sqrt{\frac{2}{\sum_{i=1}^{n}(q_i-1)}}$, but for now we will write them as generic numbers. The conditions imposed on the ζ_n's will come from the proof.

We will prove by induction on n that for any $A \subset Q_n$, we have

$$|B_n(A,1)| \ge |A| + \zeta_n |A| \left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.4}$$

When $n = 1$ and $A \subset Q_1$, we have $B_1(A,1) = Q_1$. We see easily that (5.4) is true whenever

$$\zeta_1 \le \frac{q_1}{q_1 - 1}. \tag{5.5}$$

For the inductive step, suppose (5.4) is true for all subsets of Q_{n-1} with a constant ζ_{n-1} in place of ζ_n. For $X \subset Q_{n-1}, Y \subset I_n$, we write

$$X \oplus Y = \{(\mathbf{x}, y) \in Q_n : \mathbf{x} \in X, y \in Y\}.$$

Let $A \subset Q_n$. For any $i \in I_n$, we define

$$A_i = \{\mathbf{a} \in Q_{n-1} : (\mathbf{a}, i) \in A\}.$$

Then clearly we have the partition

$$A = \bigsqcup_{i=0}^{q_n-1} A_i \oplus \{i\}, \tag{5.6}$$

and consequently

$$|A| = \sum_{i=0}^{q_n-1} |A_i|. \tag{5.7}$$

Our first observation is that for any $i \in I_n$, we have $A_i \oplus I_n \subset B_n(A,1)$. This leads to the bound

$$|B_n(A,1)| \geq q_n |A_i|. \tag{5.8}$$

for any $i \in I_n$. Next, we observe that for any $i \in I_n$, we have $B_{n-1}(A_i,1) \oplus \{i\} \subset B_n(A,1)$. Clearly the sets $B_{n-1}(A_i,1) \oplus \{i\}$ are disjoint. Thus we have yet another bound

$$|B_n(A,1)| \geq \sum_{i=0}^{q_n-1} |B_{n-1}(A_i,1)|. \tag{5.9}$$

Without loss of generality we may assume $|A_0| \geq |A_1| \geq \cdots \geq |A_{q_n-1}|$. From (5.8) and (5.7), we have

$$|B_n(A,1)| \geq |A| + \sum_{k=0}^{q_n-1} \left(|A_0| - |A_k|\right).$$

We distinguish two cases.

Case 1:

$$\sum_{k=0}^{q_n-1} \left(|A_0| - |A_k|\right) \geq \zeta_n |A| \left(1 - \frac{|A|}{|Q_n|}\right).$$

In this case (5.4) follows immediately.

Case 2:

$$\sum_{k=0}^{q_n-1} \left(|A_0| - |A_k|\right) < \zeta_n |A| \left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.10}$$

Using (5.9) and the induction hypothesis for each $A_k \subset Q_{n-1}$, we have

$$\begin{aligned} |B_n(A,1)| &\geq \sum_{k=0}^{q_n-1} \left\{ |A_k| + \zeta_{n-1}|A_k| \left(1 - \frac{|A_k|}{|Q_{n-1}|}\right) \right\} \\ &= |A| + \zeta_{n-1}|A| - \frac{\zeta_{n-1}}{|Q_{n-1}|} \sum_{k=0}^{q_n-1} |A_k|^2. \end{aligned} \tag{5.11}$$

Moreover, one has

$$\sum_{k=0}^{q_n-1} |A_k|^2 = \frac{1}{q_n} \left(|A|^2 + \sum_{0 \leq i < j \leq q_n-1} \Big(|A_i| - |A_j| \Big)^2 \right). \tag{5.12}$$

For $i = 1, 2, \ldots, q_n - 1$, put $x_i = |A_{i-1}| - |A_i| \geq 0$. Then (5.10) reads

$$\sum_{i=1}^{q_n-1} (x_1 + \cdots + x_i) \leq \zeta_n |A| \left(1 - \frac{|A|}{|Q_n|}\right).$$

On the other hand,

$$\sum_{0 \leq i < j \leq q_n-1} \Big(|A_i| - |A_j| \Big)^2 = \sum_{1 \leq i \leq j \leq q_n-1} (x_i + x_{i+1} + \cdots + x_j)^2.$$

Thus Lemma 5.1.2 implies that

$$\sum_{k=0}^{q_n-1} |A_k|^2 \leq \frac{1}{q_n} \left(|A|^2 + (q_n - 1)\zeta_n^2 |A|^2 \left(1 - \frac{|A|}{|Q_n|}\right)^2 \right). \tag{5.13}$$

Putting this into (5.11), it follows that

$$\begin{aligned} |B_n(A,1)| &\geq |A| + \zeta_{n-1}|A| - \frac{\zeta_{n-1}}{|Q_n|} \left(|A|^2 + (q_n - 1)\zeta_n^2 |A|^2 \left(1 - \frac{|A|}{|Q_n|}\right)^2 \right) \\ &= |A| + \zeta_{n-1}|A| \left(1 - \frac{|A|}{|Q_n|}\right) - \frac{\zeta_{n-1}}{|Q_n|} \cdot (q_n - 1)\zeta_n^2 |A|^2 \left(1 - \frac{|A|}{|Q_n|}\right)^2 \\ &\geq |A| + \zeta_{n-1} \left(1 - (q_n - 1)\frac{\zeta_n^2}{4}\right) |A| \left(1 - \frac{|A|}{|Q_n|}\right). \end{aligned} \tag{5.14}$$

Here (5.14) follows from the fact that $\frac{|A|}{|Q_n|}\left(1-\frac{|A|}{|Q_n|}\right) \leq \frac{1}{4}$. Thus (5.4) follows if we have

$$\zeta_{n-1}\left(1-(q_n-1)\frac{\zeta_n^2}{4}\right) \geq \zeta_n. \tag{5.15}$$

We now choose $\zeta_n = \sqrt{\frac{2}{\sum_{i=1}^n (q_i-1)}}$. Then $\zeta_1 = \sqrt{\frac{2}{q_1-1}} \leq \frac{q_1}{q_1-1}$ and (5.5) is satisfied. The condition (5.15) is also satisfied, since

$$\zeta_n^2 = \zeta_{n-1}^2\left(1-(q_n-1)\frac{\zeta_n^2}{2}\right) \leq \zeta_{n-1}^2\left(1-(q_n-1)\frac{\zeta_n^2}{4}\right)^2.$$

□

It is possible to iterate (5.2) to give a non-trivial bound for $B(A,r)$ for arbitrary r, and this is what Wirsing did in [38, Section 4.3].

5.2 Proof of Theorem 1.6.1

We identify $\mathbb{F}_p^n$ with $Q_n = \{0,1,\dots,p-1\}^n$ via the map

$$(x_1,\dots,x_n) \mapsto \sum_{i=1}^n x_i e_i.$$

Let $E = \{e_1,\dots,e_n\}$. Then $B(A,1) = A \cup (A+E) \cup \cdots (A+(p-1)\cdot E)) \subset A+(p-1)H$ where $k \cdot E := \{ke_i : i = 1,\dots,n\}$. Theorem 5.1.1 implies that

$$|A+(p-1)H| \geq |A| + \sqrt{\frac{2}{(p-1)n}}|A|\left(1-\frac{|A|}{p^n}\right).$$

We will use Plünnecke's inequality in the following form ([31, Theorem 1.2.1]): if

$$\mu_k := \inf\left\{\frac{|X+kH|}{|X|} : X \subset A, X \neq \emptyset\right\}$$

then the sequence $\{\mu_k^{1/k}\}_{k=1}^\infty$ is decreasing.

For any $X \subset A$, $X \neq \emptyset$, we have

$$\frac{|X+(p-1)H|}{|X|} \geq 1+\sqrt{\frac{2}{(p-1)n}}\left(1-\frac{|X|}{p^n}\right) \geq 1+\sqrt{\frac{2}{(p-1)n}}\left(1-\frac{|A|}{p^n}\right).$$

Therefore,

$$\mu_{p-1}^{1/(p-1)} \geq \left(1+\sqrt{\frac{2}{(p-1)n}}\left(1-\frac{|A|}{p^n}\right)\right)^{1/(p-1)} \geq 1+\frac{c(p)}{\sqrt{n}}\left(1-\frac{|A|}{p^n}\right)$$

for some $c(p) = \Omega(p^{-3/2})$. Since

$$\frac{|A+H|}{|A|} \geq \mu_1 \geq \mu_{p-1}^{1/(p-1)},$$

Theorem 1.6.1 follows. If $p = 2$ then the use of Plünnecke's inequality is unecessary and we can take $c(2) = \sqrt{2}$.

5.3 Proof of Theorem 1.6.2

Let $A \subset \mathbb{F}_p^n$ be a subset of density $\alpha > \frac{1}{2} - \frac{c'(p)}{\sqrt{n}}$. By choosing $c'(p)$ sufficiently small we can certainly assume that $\alpha \geq 1/4$. Like Sanders, we will first show:

Claim 1: $A - A \supset (x+U)^c$ for some $x \in \mathbb{F}_p^n$ and subspace U of codimension 1 of $\mathbb{F}_p^n$.

To put it in a different way, $S := (A-A)^c$ is contained in an affine subspace of codimension 1. Suppose for a contradiction that this is not true. Let s be any element of S, then $S-s$ contains n linearly independent vectors. Call them $e_1, \ldots, e_n$. Put $H = \{0, e_1, \ldots, e_n\}$, then we have $s + H \subset S$. By definition of S, we have $(S+A) \cap A = \emptyset$. Hence,

$$\frac{|H+A|}{p^n} = \frac{|s+H+A|}{p^n} \leq \frac{|S+A|}{p^n} \leq 1-\alpha. \tag{5.16}$$

Sanders deduced a contradiction from this by repeated applications of Plünnecke's inequality and McDiarmid's inequality. Thanks to Theorem 1.6.1, we have a contradiction immediately. Indeed, since

$$\frac{|H+A|}{p^n} \geq \alpha + \frac{c(p)}{\sqrt{n}}\alpha(1-\alpha) \geq \alpha + \frac{3}{16}\frac{c(p)}{\sqrt{n}},$$

we have a contradiction if we choose $c'(p) \leq \frac{3}{32}c(p)$. Claim 1 follows.

For the rest of the proof we argue similarly to Sanders.

Claim 2: If $V \neq \{0\}$ is any subspace of $\mathbb{F}_p^n$, then $A - A \supset V \setminus (U + x)$ for some subspace U of codimension 1 of V and $x \in V$.

We observe that, by averaging over $t \in \mathbb{F}_p^n$, there is a translate $t + A$ such that the density of $(t + A) \cap V$ in V is at least α. Since $A - A \supset (t + A) \cap V - (t + A) \cap V$, Claim 2 follows from Claim 1.

Claim 3: $A - A \supset (x + U)^c$ for some subspace $U \lneq \mathbb{F}_p^n$ and $x \notin U$.

To see that this implies Theorem 1.6.2, let W be any subspace of codimension 1 of $\mathbb{F}_p^n$ such that $U \subset W$ and $x \notin W$ (the existence of W may be seen from taking a basis of $\mathbb{F}_p^n$ containing x and a basis of U). Then $A-A \supset (x+U)^c \supset (x+W)^c \supset W$.

We now prove Claim 3. Let U be the smallest subspace of $\mathbb{F}_p^n$ such that $(A - A) \supset (x + U)^c$ for some x. Such U exists by Claim 1. We now show that $x \notin U$. Suppose for a contradiction that $x \in U$, i.e. $U^c \subset A - A$. Since $\{0\} \subset A - A$, we have $\dim U \geq 1$. By Claim 2, there are a subspace U' of codimension 1 of U and $y \in U$ such that $A - A \supset U \setminus (U' + y)$. Therefore,

$$A - A \supset U^c \cup (U \setminus (U' + y)) = (U' + y)^c$$

contradicting the minimality of U.

5.4 Further discussions

It is instructive to compare Theorem 5.1.1 with other estimates for $B(A,1)$. The case $Q_n = \{0,1\}^n$ (i.e., the hypercube) has been extensively studied in the context of vertex isoperimetric inequalities for graphs. Harper's theorem [14] says that among all sets $A \subset \{0,1\}^n$ of size k, $|B(A,1)|$ is minimized when A is the first k elements in the simplicial ordering. For $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \{0,1,2\ldots\}^n$, we set $\mathbf{x} < \mathbf{y}$ in the simplicial ordering if either $\sum_{i=1}^n x_i < \sum_{i=1}^n y_i$, or $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i$ and for some j we have $x_j > y_j$ and $x_i = y_i$ for all $i < j$. In particular, if $|A| = \sum_{i=0}^r \binom{n}{i}$ then $|B(A,1)|$ is minimized when A is a Hamming ball with radius r. Our bound (5.2) is weaker than Harper's when the density of A is small, but is comparable when the density of A is bounded away from 0 and 1 (see (5.20) below).

Bollobás and Leader [2, Theorem 8] generalized Harper's theorem to $Q_n = \prod_{k=1}^n I_k$, though their notion of Hamming distance is quite different from ours. Like Harper's theorem, their result is optimal, but it does not seem straightforward to extract from their result an explicit bound like (5.2).

McDiarmid's inequality [26, Corollary 7.6] states that if $A \subset Q_n = \prod_{k=1}^n I_k$, then

$$\frac{|B(A,r)|}{|Q_n|} \geq 1 - \frac{|Q_n|}{|A|} \exp\left(-\frac{r^2}{2n}\right). \tag{5.17}$$

The bound (5.17) is useful when r is large (for an application, see [39]), but sometimes it is worse than trivial (e.g. when the density of A in Q_n is close to 0 or 1). On the other hand, the bound given by (5.2) is always non-trivial.

Plünnecke's inequality implies that for any sets A, B in a commutative group, we have

$$|kB| \leq \left(\frac{|A+B|}{|A|}\right)^k |A|.$$

It gives the following bound.

Proposition 5.4.1. *If $A \subset Q_n = \prod_{k=1}^n I_k$, then*

$$|B(A,1)| \geq |A| + \frac{1}{n}|A| \left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.18}$$

Proof. We identify each I_k with a commutative group G_k on q_k elements and Q_n with the group $\oplus_{k=1}^n G_k$. Then $B(A,1) = A + B$, where

$$B = \bigcup_{k=1}^{n} \{\mathbf{x} = (0, \ldots, 0, x_k, 0, \ldots, 0) \in Q_n : x_k \in G_k\}.$$

Clearly $nB = Q_n$, hence

$$|Q_n| \leq \left(\frac{|B(A,1)|}{|A|}\right)^n |A|.$$

which implies

$$|B(A,1)| \geq |A| \left(\frac{|A|}{|Q_n|}\right)^{-1/n} \geq |A| + \frac{1}{n}|A| \left(1 - \frac{|A|}{|Q_n|}\right)$$

as desired. □

In the special case where $q_1 = \ldots = q_n = q$, Theorem 5.1.1 becomes:

Corollary 5.4.2. *Let $q \geq 2$ and $Q_n = \{0, 1, \ldots, q-1\}^n$. Then for any $A \subset Q_n$, we have*

$$|B(A,1)| \geq |A| + \sqrt{\frac{2}{(q-1)n}}|A| \left(1 - \frac{|A|}{|Q_n|}\right). \tag{5.19}$$

The factor $\sqrt{n}$ in (5.19) is best possible in terms of order of magnitude. To see this, we take $q = 2$ and

$$A = \left\{(x_1, \ldots, x_n) \in \{0,1\}^n : \sum_{i=1}^{n} x_i \leq \frac{n}{2}\right\}.$$

Then

$$B(A,1) = \left\{ (x_1, \ldots, x_n) \in \{0,1\}^n : \sum_{i=1}^n x_i \leq \frac{n}{2} + 1 \right\}.$$

and

$$\frac{1}{2} \leq \frac{|A|}{|Q_n|} \leq \frac{|B_n(A,1)|}{|Q_n|} \leq \frac{1}{2} + O\left(\frac{1}{\sqrt{n}}\right) \tag{5.20}$$

where the last inequality follows from the central limit theorem (or from the fact that the largest binomial coefficient $\binom{n}{r}$ is $O\left(\frac{2^n}{\sqrt{n}}\right)$). On the other hand, there are many reasons to believe that the factor $\sqrt{q-1}$ in (5.19) should not be there. Indeed, in the spirit of the previous example, we take

$$A = \left\{ (x_1, \ldots, x_n) \in \{0,1,\ldots,q-1\}^n : \sum_{i=1}^n x_i \leq \frac{(q-1)n}{2} \right\}.$$

Then it is easy to see that

$$B(A,1) \supset \left\{ (x_1, \ldots, x_n) \in \{0,1,\ldots,q-1\}^n : \sum_{i=1}^n x_i \leq \frac{(q-1)(n+1)}{2} \right\}.$$

For this particular A, an application of the Berry-Esseen inequality shows that

$$|B(A,1)| \geq |A| + \frac{1}{O(\sqrt{n})}|A|\left(1 - \frac{|A|}{|Q_n|}\right)$$

where $O(\sqrt{n})$ is independent of q. Furthermore, both the bounds (5.17) and (5.18) do not depend on the q_i's. Thus it is natural to ask.

Question. *Is there a function $f : [0,1] \to \mathbb{R}$ such that $f > 0$ on $(0,1)$ and*

$$\frac{|B(A,1)|}{|Q_n|} \geq \alpha + \frac{1}{\sqrt{n}} f(\alpha)$$

for all $Q_n = \prod_{k=1}^n I_k$ and $A \subset Q_n$ of density α?

If the answer to this question is affirmative then the constant $c(p)$ in Theorem 1.6.1 can be taken to be $\Omega(p^{-1})$ and it is easy to see that this is best possible.

6 ESSENTIAL COMPONENTS IN POLYNOMIALS OVER FINITE FIELDS

6.1 Preliminaries

6.1.1 Notation

Recall that we use G and $\mathbb{F}[t]$ interchangeably and an element of G can be viewed as both a vector and a polynomial. An element $x = (x_0, x_1, \ldots)$ of G is identified with the polynomial $\sum_{i=0}^{\infty} x_i t^i$. In particular, by $\deg x$, we mean the largest n such that $x_n \neq 0$. We define the *support* of x as $\mathrm{supp}(x) = \{i : x_i \neq 0\}$. We say that x is supported on a set I if $\mathrm{supp}(x) \subset I$. We define $e(x) = e^{2\pi i x}$ for $x \in \mathbb{R}$ and $e_p(x) = e(x/p)$ for $x \in \mathbb{F}$ (so e_p is an additive character on $\mathbb{F}$). We will often make use of the following fact (where $\cdot$ denotes the scalar product):

$$\sum_{f \in G_n} e_p(x \cdot f) = \begin{cases} p^n, & \text{if } \mathrm{supp}(x) \cap [0, n) = \varnothing \\ 0, & \text{otherwise.} \end{cases} \tag{6.1}$$

6.1.2 Probability tools

Lemma 6.1.1 (Berry-Esseen inequality [12, Chapter 7, Theorem 6.1])**.** *Let $X, \{X_j\}_{j=1}^n$ be independent, identically distributed random variables. Let*

$$F(x) = \mathbf{P}\left(\frac{\sum_{j=1}^n X_j - n\mathbf{E}(X)}{\sqrt{n\mathbf{Var}(X)}} \leq x \right), \tag{6.2}$$

and let $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$ *be the cumulative distribution function of the standard normal distribution. Suppose* $\mathbf{E}(|X - \mathbf{E}(X)|^3) \leq K < \infty$*. Then*

$$\sup_x |F(x) - \Phi(x)| \leq \frac{C \cdot K}{n^{1/2} \mathbf{Var}(X)^{3/2}} \tag{6.3}$$

where C *is a constant less than* 0.8*.*

Our next tool is Bernstein's inequality. For real random variables, this can be found in [4, Corollary 2.11]. The complex case follows easily from applying the real case to the real and imaginary parts of Z_j.

Lemma 6.1.2 (Bernstein's inequality)**.** *Let* $\{Z_j\}_{j=1}^n$ *be independent bounded complex random variables such that* $\mathbf{E}(\sum Z_j) = A$ *and* $|Z_j - \mathbf{E}(Z_j)| \leq k$ *for all* $j = 1, \cdots, n$*. Suppose* $\sum_{j=1}^n \mathbf{Var}(Z_j) \leq \sigma^2$*. Then for all* $\lambda > 0$*,*

$$\mathbf{P}\left(|\sum_{j=1}^n Z_j - A| \geq \lambda\right) \leq 4 \exp\left(\frac{-\lambda^2}{4(\sigma^2 + k\lambda/3)}\right).$$

We also need the following version of the law of large numbers.

Lemma 6.1.3 (Kolmogorov's strong law of large numbers [29, p. 12])**.** *Let* $\{X_n\}$ *be a sequence of independent random variables with* $\mathbf{E}(X_n) = 0$ *for all* n*. Let* $\{a_n\}$ *be a non-decreasing unbounded sequence of positive numbers. If* $\sum_{n=1}^{\infty} \frac{\mathbf{E}(|X_n|^2)}{a_n^2} < \infty$*, then*

$$\lim_{n \to \infty} \frac{\sum_{j=1}^n X_j}{a_n} = 0 \quad \text{a. s.} \tag{6.4}$$

6.1.3 Fourier analysis tools

We need the following lemma of Ruzsa which relates essential components to the Fourier transform. Ruzsa proved it for general abelian groups, though we only need it for the case of G_n.

Lemma 6.1.4 ([31, Corollary 7.3]). *Let $K \subset G_n$ and arbitrary complex numbers $(c_k)_{k\in K}$ such that $\sum_{k\in K} c_k = 1$. Define*

$$\xi(x) = \sum_{k\in K} c_k e_p(k\cdot x)$$

for any $x \in G_n$. Suppose there is $\eta > 0$ such that $|\xi(x)| \le \eta$ for all $x \in G_n, x \neq 0$. Then for any set $A \subset G_n$, we have

$$|A+K| \ge |A| + (1-\eta^2)|A|\left(1 - \frac{|A|}{p^n}\right).$$

In other words, if there is a trigonometric polynomial supported on K, all of whose values (except the one at 0) are small, then K serves as an essential component in G_n. The most obvious choice for (c_k) is $c_k = \frac{1}{|K|}$; however, in our application we will have to choose a different function.

For completeness we reproduce Ruzsa's proof here.

Proof. Let $B := (A+K)^c$, then $B \cap (A+K) = \emptyset$. Therefore,

$$\begin{aligned} 0 &= \sum_{x\in G_n}\sum_{b\in B} e_p(-x\cdot b)\sum_{a\in A} e_p(x\cdot a)\sum_{k\in K} c_k e_p(k\cdot x) \\ &= \sum_{x\in G_n} \xi(x)\sum_{b\in B} e_p(-x\cdot b)\sum_{a\in A} e_p(x\cdot a). \end{aligned}$$

By separating the contribution of $x = 0$, we have

$$\begin{aligned} |B||A| &= -\sum_{\substack{x\in G_n\\ x\neq 0}} \xi(x)\sum_{b\in B} e_p(-x\cdot b)\sum_{a\in A} e_p(x\cdot a) \le \eta \sum_{\substack{x\in G_n\\ x\neq 0}} \left|\sum_{b\in B} e_p(-x\cdot b)\sum_{a\in A} e_p(x\cdot a)\right| \\ &\le \eta \left(\sum_{\substack{x\in G_n\\ x\neq 0}} \left|\sum_{b\in B} e_p(-x\cdot b)\right|^2\right)^{1/2} \left(\sum_{\substack{x\in G_n\\ x\neq 0}} \left|\sum_{a\in A} e_p(x\cdot a)\right|^2\right)^{1/2} \quad \text{Cauchy-Schwarz} \\ &= \eta\left(|A|(p^n-|A|)\right)^{1/2}\left(|B|(p^n-|B|)\right)^{1/2} \qquad \text{by Plancherel} \end{aligned}$$

Therefore, $|A||B| \leq \eta^2(p^n - |A|)(p^n - |B|)$ and

$$|B| \leq \frac{\eta^2 p^n(p^n - |A|)}{|A| + \eta^2(p^n - |A|)} = p^n \frac{\eta^2(1-\delta)}{\delta + \eta^2(1-\delta)}$$

where $\delta := \frac{|A|}{p^n}$. Since $|B| = p^n - |A + K|$, we have

$$\begin{aligned} \frac{|A+K|}{p^n} &\geq \frac{\delta}{\delta + \eta^2(1-\delta)} \\ &= \delta + \frac{(1-\eta^2)\delta(1-\delta)}{\delta + \eta^2(1-\delta)} \\ &\geq \delta + (1-\eta^2)\delta(1-\delta), \end{aligned}$$

where we applied $\delta + \eta^2(1-\delta) \leq \delta + (1-\delta) = 1$. □

6.1.4 Combinatorics tools

Lemma 6.1.5. *Let $n \in \mathbb{Z}^+$ and $C \subset G_n$ be a subset of G_n with $|C| = \delta p^n > 0$. Then exists $x \in G_n$ such that*

$$|(C - x) \cap G_m| \geq \delta p^m \tag{6.5}$$

for all $0 \leq m \leq n$. In particular, $x \in C$.

The proof of this lemma can be found in [24, p. 12]. For completeness we include the proof here.

Proof. We prove the lemma by induction on n. When $n = 1$ we can take x to be any element of C. Suppose the lemma is true for subsets of G_{n-1}. Since we have the partition

$$G_n = \cup_{\alpha \in \mathbb{F}}(G_{n-1} + \alpha t^{n-1}),$$

there must be $\alpha \in \mathbb{F}$ such that $|C \cap (G_{n-1} + \alpha t^{n-1})| \geq \delta p^{n-1}$. Therefore, $|(C - \alpha t^{n-1}) \cap G_{n-1}| \geq \delta p^{n-1}$. Applying the induction hypothesis to the set $(C - \alpha t^{n-1}) \cap G_{n-1}$, we

see that there is $y \in G_{n-1}$ such that

$$|(C - \alpha t^{n-1} - y) \cap G_m| \geq \delta p^m \tag{6.6}$$

for all $0 \leq m \leq n-1$. Therefore, (6.5) is true with $x = \alpha t^{n-1} + y$. The assertion $x \in C$ follows from applying (6.5) with $m = 0$. □

In proving Theorem 1.7.4 we need the following isoperimetric-type inequality.

Lemma 6.1.6 (Corollary 5.4.2)**.** *Put* $K_n = \{x \in G_n : |\mathrm{supp}(x)| \leq 1\}$. *Then for any* $A \subset G_n$, *we have*

$$|A + K_n| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{p^n}\right)$$

for some constant $c(p) > 0$.

6.2 Proof of Theorem 1.7.2

In this section, we fix $0 < c < 1$. Let $(X_f)_{f \in G}$ be a family of independent random variables taking values in $\{0, 1\}$ and

$$b_f = \mathbf{P}(X_f = 1) = \frac{\deg(f)^c}{p^{\deg(f)}} \tag{6.7}$$

if $\deg(f) \geq 1$; $b_f = 1$ if $\deg(f) \leq 0$. Then the X_f's are Bernoulli and

$$\mathbf{E}(X_f) = b_f, \qquad \mathbf{Var}(X_f) = b_f(1 - b_f). \tag{6.8}$$

Now we define

$$H := \{f \in G : X_f = 1\}. \tag{6.9}$$

On the one hand, we claim that $|H_n| \ll n^{1+c}$ holds almost surely. In order to see this, we apply Lemma 6.1.3 to the independent random variables $Y_n = \sum_{\deg(f)=n} X_f -$

$n^c(1-p^{-1})$ and the sequence $a_n = n^{1+c}$ for $n \geq 1$. Since $\mathbf{E}(Y_n) = 0$ for all $n \geq 1$ and $\sum_{n=1}^{\infty} a_n^{-2}\mathbf{E}(|Y_n|^2) \leq \sum_{n=1}^{\infty} n^{-2-c} < \infty$, Lemma 6.1.3 implies that

$$\lim_{n\to\infty} \frac{|H_{n+1}| - \mathbf{E}(|H_{n+1}|)}{n^{1+c}} = \lim_{n\to\infty} \frac{\sum_{j=1}^{n} Y_j}{n^{1+c}} = 0 \qquad \text{a.s.} \tag{6.10}$$

Thus, as $n \to \infty$, $||H_n| - \mathbf{E}(|H_n|)| = o(n^{1+c})$ and $|H_n| \ll \mathbf{E}(|H_n|) \ll n^{1+c}$ holds almost surely.

On the other hand, we will prove that H is an essential component of G almost surely. This is the purpose of the remaining of this section.

The strategy is to use Lemma 6.1.4 and produce a trigonometric polynomial supported on H_n, all of whose values are small except the one at 0. A first step is the following, which guarantees that the trigonometric polynomial is small on a set S, as long as $|S|$ is not too big.

Lemma 6.2.1. *Let $0 < c < 1$ and n be sufficiently large depending on c. For $f \in G_n$, define*

$$w_0(f) = \frac{1}{p^n b_f} \tag{6.11}$$

(recall that $b_f = \mathbf{E}(X_f)$). Let

$$\xi_0(x) = \sum_{f\in G_n} w_0(f) X_f e_p(f \cdot x) \tag{6.12}$$

for $x \in G_n$. Then for any subset $S \subset G_n \setminus \{0\}$ with $|S| \leq \exp(\frac{n^c}{200})$, we have

$$\mathbf{P}\left(\left\{|\xi_0(0) - 1| < \frac{1}{3}\right\} \wedge \left\{\max_{x\in S} |\xi_0(x)| < \frac{1}{3}\right\}\right) \geq 1 - \exp\left(\frac{-n^c}{400}\right). \tag{6.13}$$

Proof of Lemma 6.2.1. By the definition of $w_0(f)$, for every $x \in G_n$, we have

$$\mathbf{E}(\xi_0(x)) = \frac{1}{p^n} \sum_{f \in G_n} e_p(x \cdot f) = \begin{cases} 0, & \text{if } x \neq 0 \\ 1, & \text{if } x = 0. \end{cases} \tag{6.14}$$

For every $x \in G_n$, we have

$$\begin{aligned} \mathbf{Var}(\xi_0(x)) &= \mathbf{Var}(\mathrm{Re}(\xi_0(x))) + \mathbf{Var}(\mathrm{Im}(\xi_0(x))) \\ &\leq 2 \sum_{f \in G_n} w_0(f)^2 b_f (1 - b_f) \leq \frac{2}{p^{2n}} \sum_{f \in G_n \setminus G_0} \frac{1}{b_f} < \frac{2}{p^{2n}} \sum_{j=1}^{n-1} \frac{p^{2j}}{j^c}. \end{aligned} \tag{6.15}$$

Note that since $\frac{p^{2(j+1)}}{(j+1)^c} / \frac{p^{2j}}{j^c} \geq \frac{p^2}{2} \geq 2$, it is easy to show that $\sum_{j=1}^{n-1} \frac{p^{2j}}{j^c} \leq \frac{p^{2n}}{n^c}$. Hence, for every $x \in G_n$ the variance is

$$\mathbf{Var}(\xi_0(x)) < 2n^{-c}. \tag{6.16}$$

Moreover, since $|w_0(f) e_p(f \cdot x)(X_f - \mathbf{E}(X_f))| \leq 2w_0(f) \leq 2n^{-c}$, Bernstein's inequality (Lemma 6.1.2) implies that

$$\begin{aligned} &\mathbf{P}\left(|\xi_0(x)| \geq \tfrac{1}{3}\right) \leq 4 \exp\left(\tfrac{-n^c}{80}\right) && \text{for } x \neq 0, \\ &\mathbf{P}\left(|\xi_0(0) - 1| \geq \tfrac{1}{3}\right) \leq 4 \exp\left(\tfrac{-n^c}{80}\right). \end{aligned} \tag{6.17}$$

Since $4(|S|+1) \leq 4\exp(\frac{n^c}{200}) + 4 < \exp(\frac{n^c}{100})$ holds for all sufficiently large n depending on c, using (6.17) and the union bound, we obtain that

$$\begin{aligned} \mathbf{P}\left(\left\{\max_{x \in S} |\xi_0(x)| \geq \frac{1}{3}\right\} \vee \left\{|\xi_0(0) - 1| \geq \frac{1}{3}\right\}\right) &\leq 4(|S|+1) \exp\left(\frac{-n^c}{80}\right) \\ &< \exp\left(\frac{n^c}{100} - \frac{n^c}{80}\right). \end{aligned}$$

In other words,

$$\mathbf{P}\left(\left\{\max_{x\in S}|\xi_0(x)|<\frac{1}{3}\right\}\wedge\left\{|\xi_0(0)-1|<\frac{1}{3}\right\}\right)\geq 1-\exp\left(\frac{n^c}{100}-\frac{n^c}{80}\right)$$
$$=1-\exp\left(\frac{-n^c}{400}\right),$$

as desired. □

The trigonometric polynomial ξ_0 given by Lemma 6.2.1 covers only a set S whose size is small compared to G_n. In the next Lemma, we will produce different trigonometric polynomials ξ_u, each covering a different set S_u, then "glue" these trigonometric polynomials together. We can do this as long as $|S_u|$ is not too big, and no element of S_u is supported on $[n-u,n)$.

Lemma 6.2.2. *Let $0<c<1$ and n be sufficiently large depending on c. Let u be an integer with $1\leq u<n^{1-c/3}$. For $f\in G_n$ we define*

$$w_u(f)=\begin{cases} w=((1-p^{-1})\sum_{j=n-u}^{n-1}j^c)^{-1}, & \text{if } n-u\leq \deg(f)<n,\\ 0, & \text{otherwise.}\end{cases} \tag{6.18}$$

Further, for $x\in G_n$, we define

$$\xi_u(x)=\sum_{f\in G_n}w_u(f)X_f e_p(f\cdot x). \tag{6.19}$$

Then for any subset $S_u\subset\{x\in G_n:\operatorname{supp}(x)\cap[0,n-u)\neq\emptyset\}$ with $|S_u|\leq\exp(\frac{un^c}{2000})$, we have

$$\mathbf{P}\left(\left\{|\xi_u(0)-1|<\frac{1}{3}\right\}\wedge\left\{\max_{x\in S_u}|\xi_u(x)|<\frac{1}{3}\right\}\right)\geq 1-\exp\left(\frac{-un^c}{6000}\right). \tag{6.20}$$

Proof of Lemma 6.2.2. We first see that

$$\mathbf{E}(\xi_u(0)) = \sum_{f\in G_n} w_u(f)b_f = \sum_{j=n-u}^{n-1}\sum_{\deg(f)=j} wb_f = 1.$$

For $\mathrm{supp}(x)\cap[0,n-u)\neq\emptyset$, we have

$$\begin{aligned}\mathbf{E}(\xi_u(x)) &= w\sum_{n-u\le\deg(f)<n}\mathbf{E}(X_f)e_p(x\cdot f) = w\sum_{j=n-u}^{n-1}\frac{j^c}{p^j}\sum_{\deg(f)=j}e_p(f\cdot x)\\ &= w\sum_{j=n-u}^{n-1}\frac{j^c}{p^j}\sum_{f\in G_{j+1}\setminus G_j}e_p(f\cdot x) = 0.\end{aligned} \tag{6.21}$$

For $n > 2^{3/c}$, we have $u\le n/2$ and $w = ((1-p^{-1})\sum_{j=n-u}^{n-1} j^c)^{-1} \le 2(u(n/2)^c)^{-1} \le 4(un^c)^{-1}$. Therefore,

$$\mathbf{Var}(\xi_u(x)) \le 2w^2\sum_{n-u\le\deg(f)<n}\mathbf{Var}(X_f) \le 2w^2\sum_{j=n-u}^{n-1} j^c\left(1-\frac{j^c}{p^j}\right) \le 2w^2un^c \le \frac{32}{un^c}. \tag{6.22}$$

Moreover, for each f, $|w_u(f)e_p(f\cdot x)(X_f-\mathbf{E}(X_f))|\le 2w\le 8(un^c)^{-1}$. By Bernstein's inequality, for $\mathrm{supp}(x)\cap[0,n-u)\neq\emptyset$, we have

$$\begin{aligned}&\mathbf{P}\left(|\xi_u(x)|\ge\tfrac{1}{3}\right)\le 4\exp\left(\tfrac{-un^c}{1200}\right),\\ &\mathbf{P}\left(|\xi_u(0)-1|\ge\tfrac{1}{3}\right)\le 4\exp\left(\tfrac{-un^c}{1200}\right).\end{aligned} \tag{6.23}$$

Note that $4(|S_u|+1)\le 4(\exp(\frac{un^c}{2000})+1) < \exp(\frac{un^c}{1500})$ holds for all sufficiently large n depending on c. From (6.23), we hence can deduce that

$$\begin{aligned}\mathbf{P}\left(\left\{\max_{x\in S_u}|\xi_u(x)|\ge\frac{1}{3}\right\}\vee\left\{|\xi_u(0)-1|\ge\frac{1}{3}\right\}\right) &\le 4(|S_u|+1)\exp\left(\frac{-un^c}{1200}\right)\\ &< \exp\left(\frac{un^c}{1500}-\frac{un^c}{1200}\right).\end{aligned}$$

Therefore, we obtain that

$$\mathbf{P}\left(\left\{\max_{x\in S_u}|\xi_u(x)|<\frac{1}{3}\right\}\wedge\left\{|\xi_u(0)-1|<\frac{1}{3}\right\}\right)\geq 1-\exp\left(\frac{un^c}{1500}-\frac{un^c}{1200}\right)$$
$$=1-\exp\left(\frac{-un^c}{6000}\right),$$

which completes the proof. □

As promised we will now glue different ξ_u's together. The point is that we need only $O_c(1)$ of them.

Lemma 6.2.3. *Let $0<c<1$ and n be sufficiently large depending on c and p. Let H be the set defined in* (6.9)*. There exists a (random) trigonometric polynomial*

$$\psi_n(x)=\sum_{f\in G_n}v_f e_p(f\cdot x)$$

supported on H_n with $\psi_n(0)=1$ and

$$\mathbf{P}\left(\max_{\substack{x\in G_n,\\ x\neq 0}}|\psi_n(x)|\geq 1-\frac{c}{12}\right)<\frac{3}{c}\exp\left(\frac{-n^c}{6000}\right). \tag{6.24}$$

Proof. We first take

$$u_j=\lfloor n^{1-jc/3}\rfloor \qquad \text{for } j=1,2,\dots,k \tag{6.25}$$

where $k=\lfloor\frac{3}{c}\rfloor-1$. Let $\xi_j(x)=\xi_{u_j}(x)$, $w_j(f)=w_{u_j}(f)$, where $\xi_{u_j}(x)$ and $w_{u_j}(f)$ are defined as in Lemma 6.2.2. Let

$$A_1=\{x:\operatorname{supp}(x)\cap[0,n-u_1)\neq\emptyset\}. \tag{6.26}$$

Since $n \log p < \frac{n^{1+2c/3}}{2000}$ for sufficiently large n, we note that $|A_1| < \exp(n \log p) < \exp(\frac{u_1 n^c}{2000})$ and hence A_1 satisfies the condition of Lemma 6.2.2. In general we let

$$A_j = \{x : \text{supp}(x) \subset [n - u_{j-1}, n) \text{ and } \text{supp}(x) \cap [n - u_{j-1}, n - u_j) \neq \varnothing\} \quad (6.27)$$

for $2 \leq j \leq k$. By the definition of u_j, we note that $u_{j-1} \log p < \frac{u_j n^c}{2000}$ for large n and hence $|A_j| \leq p^{u_{j-1}} \leq \exp(\frac{u_j n^c}{2000})$. Thus, all the sets A_j satisfy the condition of Lemma 6.2.2 and we obtain

$$\mathbf{P}\left(\left\{\max_{x \in A_j} |\xi_j(x)| < \frac{1}{3}\right\} \wedge \left\{|\xi_j(0) - 1| < \frac{1}{3}\right\}\right) \geq 1 - \exp\left(\frac{-u_j n^c}{6000}\right) \quad (6.28)$$

for $j = 1, 2, \ldots, k$. Finally, we let

$$A_0 = (G_n \setminus \{0\}) \setminus (\cup_{j=1}^k A_j) = \{x : \text{supp}(x) \subset [n - u_k, n)\}. \quad (6.29)$$

Since $u_k \log p < n^{2c/3} \log p < \frac{n^c}{200}$ for all sufficiently large n, $|A_0| = p^{u_k} - 1 < \exp(\frac{n^c}{200})$ holds and hence A_0 satisfies the condition of Lemma 6.2.1. Thus, for $\xi_0(x)$ defined in Lemma 6.2.1, we have

$$\mathbf{P}\left(\left\{\max_{x \in A_0} |\xi_0(x)| < \frac{1}{3}\right\} \wedge \left\{|\xi_0(0) - 1| < \frac{1}{3}\right\}\right) \geq 1 - \exp\left(\frac{-n^c}{400}\right). \quad (6.30)$$

We now define the trigonometric polynomial

$$\psi_n(x) := \frac{\sum_{j=0}^k \xi_j(x)}{\sum_{j=0}^k \xi_j(0)}. \quad (6.31)$$

Then clearly $\psi_n(0) = 1$ and ψ_n is supported on H_n because all the ξ_j are supported on H_n. Also, all the $\xi_j(0)$ are real and positive.

If all the events on the left hand sides of (6.28) and (6.30) occur, then $\sum_{j=0}^k \xi_j(0) \leq 4(k+1)/3$. If $x \in G_n \setminus \{0\}$ then there is at least one $i \in [1, k]$ such that $x \in A_i$ and

consequently $|\xi_i(x)| \le 1/3 \le \xi_i(0) - 1/3$. For all other $j \in [1,k]$ we bound trivially $|\xi_j(x)| \le \xi_j(0)$. Thus

$$|\psi_n(x)| = \frac{\left|\sum_{j=0}^{k} \xi_j(x)\right|}{\sum_{j=0}^{k} \xi_j(0)} \le 1 - \frac{1/3}{\sum_{j=0}^{k} \xi_j(0)} < 1 - \frac{1/3}{4(k+1)/3} < 1 - \frac{c}{12}. \tag{6.32}$$

Consequently,

$$\begin{aligned}
&\mathbf{P}\left(\max_{\substack{x\in G_n,\\ x\neq 0}} |\psi_n(x)| \ge 1 - \frac{c}{12}\right) \\
&\le \mathbf{P}\Big(\Big\{\text{there exists a } j \in [1,k] \text{ s.t. (6.28) fails}\Big\} \vee \Big\{\text{inequality (6.30) fails}\Big\}\Big) \\
&< \sum_{j=1}^{k} \exp\left(\frac{-u_j n^c}{6000}\right) + \exp\left(\frac{-n^c}{400}\right) < \frac{3}{c}\exp\left(\frac{-n^c}{6000}\right).
\end{aligned}$$

This completes the proof. □

Proof of Theorem 1.7.2. By Lemma 6.2.3, for a sufficiently large number M, we have

$$\sum_{n>M}^{\infty} \mathbf{P}\left(\max_{x\neq 0} |\psi_n(x)| \ge 1 - \frac{c}{12}\right) < \sum_{n>M}^{\infty} \frac{3}{c}\exp\left(\frac{-n^c}{6000}\right) < \infty. \tag{6.33}$$

Therefore, by the Borel-Cantelli Lemma, the events $\{\max_{\substack{x\in G_n,\\ x\neq 0}} |\psi_n(x)| \ge 1 - \frac{c}{12}\}$ occur for only finitely many n, almost surely.

Let A be any subset of $\mathbb{F}[t]$ with $\underline{d}(A) = \delta \in (0,1)$. Using Lemma 6.1.4 with $\eta = 1 - \frac{c}{12}$, we obtain that

$$\liminf_{n\to\infty} \frac{|A_n + H_n|}{p^n} \ge \liminf_{n\to\infty} \left\{ \frac{|A_n|}{p^n} + \left(\frac{c}{6} - \frac{c^2}{144}\right)\frac{|A_n|}{p^n}\left(1 - \frac{|A_n|}{p^n}\right)\right\} \quad \text{almost surely.} \tag{6.34}$$

The right-hand side of (6.34) is easily seen to be $\ge \delta + (\frac{c}{6} - \frac{c^2}{144})\delta(1-\delta)$, since the function $x \mapsto x + ax(1-x)$ for with $a = \frac{c}{6} - \frac{c^2}{144}$ is continuous and increasing on $(0,1)$. Thus $\liminf_{n\to\infty} \frac{|A_n+H_n|}{p^n} > \delta$ almost surely, which finishes the proof. □

6.3 Proof of Theorem 1.7.3

We first begin with the following Lemma, which says that if $|H_n| < n^{1+\epsilon/2}$ infinitely often, then we can find a subsequence of n such that the elements of H are well-spaced in G_n.

Lemma 6.3.1. *Suppose $H \subset G$ and $\epsilon > 0$ are such that $|H_n| < n^{1+\epsilon/2}$ infinitely often. Then there are infinitely n such that*

$$|H_n| < n^{1+\epsilon} \qquad \text{and} \qquad |H_n| - |H_m| \leq n^{\epsilon}(n-m) \qquad \text{for any } 1 \leq m \leq n. \quad (6.35)$$

Proof. Suppose for a contradiction that there exists $N_0 > 0$ such that for all $u > N_0$, if $|H_u| < u^{1+\epsilon}$ then there is $1 \leq v < u$ such that

$$|H_u| - |H_v| > u^{\epsilon}(u-v). \quad (6.36)$$

By the hypothesis, there exists $n > \max\{2N_0, 4^{1+1/\epsilon}\}$ such that

$$|H_n| < n^{1+\epsilon/2}. \quad (6.37)$$

Since $n > 4^{1+1/\epsilon}$, we have

$$n^{1+\epsilon/2} \leq (n/2)^{1+\epsilon}.$$

Note that for any $n/2 \leq m \leq n$, we have

$$|H_m| \leq |H_n| < n^{1+\epsilon/2} \leq (n/2)^{1+\epsilon} \leq m^{1+\epsilon}. \quad (6.38)$$

We apply (6.36) to $u = n$ and find $m_1 \in [1, n)$ such that $|H_n| - |H_{m_1}| > n^{\epsilon}(n - m_1)$. We put $m_0 = n$. Suppose we have found m_{i-1}. As long as $m_{i-1} \geq n/2$, thanks to (6.38), we can apply (6.36) with $u = m_{i-1}$ to find $m_i = v \in [1, m_{i-1})$. Let k be the

greatest integer such that $m_{k-1} \geq n/2$, then $m_k < n/2$ and

$$|H_{m_{i-1}}| - |H_{m_i}| > m_{i-1}^{\epsilon}(m_{i-1} - m_i) > (n/2)^{\epsilon}(m_i - m_{i-1}) \tag{6.39}$$

for all $1 \leq i \leq k$. Summing these inequalities over $1 \leq i \leq k$, we get

$$|H_n| > (n - m_k)(n/2)^{\epsilon} \geq (n/2)^{1+\epsilon}. \tag{6.40}$$

This inequality contradicts (6.37). This completes the proof. □

Lemma 6.3.2. *Suppose n and H satisfy the property* (6.35)*. Let $k = \lfloor \frac{1}{4\epsilon} \rfloor$. If n is sufficiently large, then there are $r_1, \ldots, r_k \in G_n$ of disjoint supports such that for any $1 \leq j \leq k$, $\mathrm{supp}(r_j) \subset [n - \lfloor \sqrt{n} \rfloor, n)$ and*

$$H_n \subset \langle r_j \rangle^{\perp} \cup \cap_{i=1}^{j-1} \langle r_i \rangle^{\perp}, \tag{6.41}$$

were $\langle r_i \rangle^{\perp}$ is the orthogonal complement in G_n of r_i. Consequently, for any $h \in H_n$, we have $h \cdot r_i = 0$ for all $i = 1, \ldots, k$ with at most one exception.

Proof. First let $d_1 := 1$ and r_1 be any vector supported on $\{n-1\}$. Since $\langle r_1 \rangle^{\perp} = G_{n-1}$, all elements in $H_n \setminus \langle r_1 \rangle^{\perp}$ are not in H_{n-1}. By inequality (6.35) we hence have that $\left| H_n \setminus \langle r_1 \rangle^{\perp} \right| \leq n^{\epsilon}$. Let $d_2 := \lfloor n^{\epsilon} \rfloor + d_1 + 2$. We shall find r_2 with $\mathrm{supp}(r_2) \subset [n-d_2, n-d_1)$ such that $H_n \setminus \langle r_1 \rangle^{\perp} \subset \langle r_2 \rangle^{\perp}$. The subspace $\langle H_n \setminus \langle r_1 \rangle^{\perp} \rangle^{\perp}$ has dimension at least $n - \lfloor n^{\epsilon} \rfloor - 1$ and the subspace spanned by $\{t \in G_n : \mathrm{supp}(t) \subset [n-d_2, n-d_1)\}$ has dimension $d_1 - d_2 = \lfloor n^{\epsilon} \rfloor + 2$. The sum of these dimensions is greater than n, which implies that the two subspaces have nonzero intersection. Thus we can find a vector r_2 supported on $[n - d_2, n - d_1)$ satisfying $h \cdot r_2 = 0$ for all $h \in H_n \setminus \langle r_1 \rangle^{\perp}$.

In general, suppose we have found $\{r_i\}_{i=1}^{j-1}$ and $\{d_i\}_{i=1}^{j-1}$ such that $\text{supp}(r_i) \in [n - d_i, n - d_{i-1})$. We next want to find r_j satisfying

$$H_n \setminus \cap_{i=1}^{j-1} \langle r_i \rangle^{\perp} \subset \langle r_j \rangle^{\perp}. \tag{6.42}$$

Since $H_n \setminus \cap_{i=1}^{j-1} \langle r_i \rangle^{\perp}$ is supported on $[0, n - d_{j-1})$, by property (6.35), we have $|H_n \setminus \cap_{i=1}^{j-1} \langle r_i \rangle^{\perp}| \leq n^{\epsilon} d_{j-1}$ and hence $\langle H_n \setminus \cap_{i=1}^{j-1} \langle r_i \rangle^{\perp} \rangle^{\perp}$ has dimension at least $n - \lfloor n^{\epsilon} d_{j-1} \rfloor - 1$. Further by letting

$$d_j := \lfloor n^{\epsilon} d_{j-1} \rfloor + d_{j-1} + 2, \tag{6.43}$$

the dimensions of the subspace spanned by $\{t \in G_n : \text{supp}(t) \subset [n - d_j, n - d_{j-1})\}$ is $d_j - d_{j-1} = \lfloor n^{\epsilon} d_{j-1} \rfloor + 2$. Thus the sum of the dimensions of these two subspaces is greater than n and their intersection must be nonzero, which yields a r_j such that $\text{supp}(r_j) \in (n - d_j, n - d_{j-1}]$ and $h \cdot r_j = 0$ for all $h \in H_n \setminus \cap_{i=1}^{j-1} \langle r_i \rangle^{\perp}$.

We can continue this process as long as $d_j < n$. From (6.43) we obtain that $d_j \leq (n^{\epsilon} + 3) d_{j-1}$ for all j. For $k = \lfloor \frac{1}{4\epsilon} \rfloor$, we have

$$d_k \leq (n^{\epsilon} + 3)^k < n^{2\epsilon k} < \lfloor \sqrt{n} \rfloor < n,$$

which means that we can construct k vectors $\{r_j\}_{j=1}^{k}$ of disjoint supports and

$$\text{supp}(r_j) \subset (n - \lfloor \sqrt{n} \rfloor, n),$$

for all $j = 1, \cdots, k$.

Now it remains to show that for every $h \in H_n$, $h \cdot r_j = 0$ holds for all $1 \leq j \leq k$ with at most one exception. On rewriting (6.42), we obtain the formula (6.41) for all $1 \leq j \leq k$. Take $h \in H_n$ and let ℓ be the first index such that $h \notin \langle r_\ell \rangle^{\perp}$. If $\ell = k$,

then r_k could be the exception. If $\ell < k$, by taking $\ell \le j \le k$ in (6.41), we know h has to be in $\langle r_i \rangle^\perp$ for all $\ell + 1 \le i \le k$, in which case r_ℓ is the exception. This completes the proof. □

Proposition 6.3.3. *Let $0 < \delta < 1$ and $\epsilon > 0$. Suppose $H \subset G$ is such that for any $\epsilon > 0$, $|H_n| < n^{1+\epsilon/2}$ infinitely often. Then for each sufficiently large n satisfying* (6.35)*, there exists a subset B_n satisfying the following four properties:*

(i) $\delta \le \frac{|B_n|}{p^n}$;

(ii) $\frac{|B_n + H_n|}{p^n} \le \delta + O(\epsilon^{1/2})$;

(iii) $\frac{|B_n \cap G_m|}{p^m} \ge \frac{|B_n|}{p^n}$ *for all* $0 \le m \le n$;

(iv) $G_{n-\lfloor\sqrt{n}\rfloor} \subset B_n$.

Proof. Let $k = \lfloor \frac{1}{4\epsilon} \rfloor$. For any sufficiently large n satisfying (6.35), let $\{r_j\}_{j=1}^k$ be vectors of disjoint supports and supported on $(n - \lfloor\sqrt{n}\rfloor, n)$ given by Lemma 6.3.2. For $f \in G_n$, we define $X_j(f) = \mathrm{Re}(e_p(f \cdot r_j))$. Since r_j is supported on $(n - \lfloor\sqrt{n}\rfloor, n)$, X_j is constant on translates of $G_{n-\lfloor\sqrt{n}\rfloor}$. Since the r_j's have disjoint supports, we can regard the X_j's as independent random variables from G_n to $\mathbb{R}$. It is easy to see that

$$\mathbf{E}(X_j) = 0, \qquad \mathbf{Var}(X_j) = \begin{cases} 1/2, & \text{if } p \neq 2 \\ 1, & \text{if } p = 2 \end{cases} \qquad \text{and} \qquad \mathbf{E}(|X_j - \mathbf{E}(X_j)|^3) \le 1. \tag{6.44}$$

Now we define

$$X = \sum_{j=1}^{k} X_j \tag{6.45}$$

and

$$F(x) = \begin{cases} \mathbf{P}(\sqrt{2/k}X \le x) & \text{if } p \neq 2 \\ \mathbf{P}(\sqrt{1/k}X \le x) & \text{if } p = 2. \end{cases}$$

By the Berry-Esseen inequality (Lemma 6.1.1), we have

$$\sup_{x\in\mathbb{R}} |F(x) - \Phi(x)| \leq \frac{2\sqrt{2}}{\sqrt{k}} \tag{6.46}$$

where $\Phi(x)$ is the cumulative distribution function of the standard normal distribution. For each $m \in \mathbb{Z}$, define the niveau set

$$S_m = \{f : f \in G_n, X(f) \geq m\}. \tag{6.47}$$

Then $G_{n-\lfloor\sqrt{n}\rfloor} = S_k \subset S_{k-1} \subset \cdots$. Since X is constant on translates of $G_{n-\lfloor\sqrt{n}\rfloor}$, if $x \in S_m$, then $x + G_{n-\lfloor\sqrt{n}\rfloor} \subset S_m$.

For any $h \in H_n$ and $f \in G_n$, we have

$$|X(f+h) - X(f)| = \left|\sum_{j=1}^{k} \mathrm{Re}(e_p(f \cdot r_j)(e_p(h \cdot r_j) - 1))\right| \leq 2 \tag{6.48}$$

since $h \cdot r_j = 0$ with at most one exception. From the definition of S_m, this implies that

$$S_m + H_n \subset S_{m-2} \tag{6.49}$$

for any m.

Let M be the largest integer such that $|S_M| \geq \delta p^n$, then $M < k$ if n is sufficiently large. We let $B_n = S_M$. By the definition of M, we have $|S_{M+1}| < \delta p^n$ and $G_{n-\lfloor\sqrt{n}\rfloor} \subset B_n$.

From (6.49) we have $B_n + H_n \subset S_{M-2}$ and

$$\begin{aligned}\frac{|B_n + H_n|}{|G_n|} &\leq \frac{|S_{M+1}|}{|G_n|} + \frac{|S_{M-2} \setminus S_{M+1}|}{|G_n|} \\ &\leq \delta + \frac{|\{f \in G_n : M-2 \leq X(f) < M+1\}|}{|G_n|} \\ &= \begin{cases} \delta + F(\sqrt{2/k}(M+1)) - F(\sqrt{2/k}(M-2)) & \text{if } p \neq 2, \\ \delta + F(\sqrt{1/k}(M+1)) - F(\sqrt{1/k}(M-2)) & \text{if } p = 2. \end{cases}\end{aligned} \tag{6.50}$$

The triangle inequality and (6.46) imply that for all $a > b$

$$|F(a) - F(b)| \leq |\Phi(a) - \Phi(b)| + 4\sqrt{2/k}. \tag{6.51}$$

Further, we note that

$$|\Phi(a) - \Phi(b)| = \frac{1}{\sqrt{2\pi}} \left| \int_a^b e^{-u^2/2} du \right| \leq |a - b|. \tag{6.52}$$

Combining this inequality with (6.51) and (6.50), we have

$$\frac{|B_n + H_n|}{p^n} \leq \delta + 7\sqrt{2/k} = \delta + O(\sqrt{\epsilon}). \tag{6.53}$$

Recall that by Lemma 6.1.5, there exists a vector $x_n \in B_n$ such that $\frac{|(B_n - x_n) \cap G_m|}{p^m} \geq \frac{|B_n|}{p^n}$ for all $0 \leq m \leq n$. Since $G_{n-\lfloor\sqrt{n}\rfloor} \subset B_n - x_n$, Proposition 6.3.3 follows by taking the shifted set as our new B_n. □

Proof of Theorem 1.7.3. Fix $0 < \delta < 1$, and suppose that for any $\epsilon > 0$, $|H_n| < n^{1+\epsilon}$ holds for infinitely many n. By Lemma 6.3.1, for each $k > 1$, there are infinitely many n such that $|H_n| < n^{1+1/k}$ and (6.35) holds with $\epsilon = 1/k$. Let n_k be such an n, and since there are infinitely many choices for n_k, we may require that $n_k - \lfloor\sqrt{n_k}\rfloor > 2n_{k-1}$ for any $k > 0$.

Let $B_{n_k} \subset G_{n_k}$ be the set provided by Proposition 6.3.3 with $\epsilon = 1/k$. Our goal is to glue the sets B_{n_k} together. Set

$$A := \bigcup_{k=1}^{\infty} (B_{n_k} \setminus G_{n_{k-1}}) \tag{6.54}$$

where we define $G_{n_0} = \emptyset$. (A simple union $\cup_{k=1}^{\infty} B_{n_k}$ won't work; this is where our construction differs from Ruzsa's.) Note that by Proposition 6.3.3 (iv), $B_{n_k} \supset G_{2n_{k-1}} \supset G_{n_{k-1}}$, so the union in (6.54) is a disjoint union.

For any $m > 0$, we have

$$\begin{aligned} A_m &= \bigcup_{n_l \geq m} \left(G_m \cap (B_{n_{l+1}} \setminus G_{n_l})\right) \cup \bigcup_{n_l < m} \left(G_m \cap (B_{n_{l+1}} \setminus G_{n_l})\right) \\ &= \bigcup_{n_l < m} \left(G_m \cap (B_{n_{l+1}} \setminus G_{n_l})\right). \end{aligned} \tag{6.55}$$

Claim 1: $\liminf_{n\to\infty} \frac{|A_n + H_n|}{|G_n|} \leq \delta$.

Indeed, from (6.55) we have $A_{n_k} = \cup_{l=1}^{k} \left(G_{n_k} \cap (B_{n_l} \setminus G_{n_{l-1}})\right) \subset \cup_{l=1}^{k} (G_{n_k} \cap B_{n_l})$ and

$$\begin{aligned} \frac{|A_{n_k} + H_{n_k}|}{|G_{n_k}|} &\leq \frac{|B_{n_k} + H_{n_k}|}{|G_{n_k}|} + \sum_{l=1}^{k-1} \frac{|B_{n_l} + H_{n_k}|}{|G_{n_k}|} \\ &\leq \delta + O(\epsilon_k^{-1/2}) + \frac{\sum_{l=1}^{k-1} n_k^{1+1/k} p^{n_l}}{p^{n_k}} \\ &\leq \delta + O(\epsilon_k^{-1/2}) + O(n_k^{1+1/k} p^{-n_k/2}) \end{aligned}$$

where on the second line we use Proposition 6.3.3 (ii) and the trivial bound $|B_{n_l} + H_{n_k}| \leq |H_{n_k}||B_{n_l}| \leq |H_{n_k}| p^{n_l}$. Letting $k \to \infty$, the claim follows.

Claim 2: $\liminf_{n\to\infty} \frac{|A_n|}{p^n} \geq \delta$.

Indeed, we will show that for any m with $n_k < m \leq n_{k+1}$, we have

$$\frac{|A_m|}{p^m} \geq \delta - \frac{1}{p^{n_{k-1}}}. \tag{6.56}$$

We distinguish two cases:

Case 1: When $2n_k < m \leq n_{k+1}$, from (6.55) we have

$$\begin{aligned} \frac{|A_m|}{p^m} &\geq \frac{|(B_{n_{k+1}} \setminus G_{n_k}) \cap G_m|}{p^m} = \frac{|(B_{n_{k+1}} \cap G_m) \setminus G_{n_k}|}{p^m} \\ &\geq \frac{|(B_{n_{k+1}} \cap G_m)| - |G_{n_k}|}{p^m} \\ &\geq \delta - \frac{1}{p^{m-n_k}} \geq \delta - \frac{1}{p^{n_k}}, \end{aligned} \tag{6.57}$$

by Proposition 6.3.3 (i), (iii), and the fact that $m \geq 2n_k$.

Case 2: When $n_k < m \leq 2n_k$, then again from (6.55) we have

$$A_m \supset \big((B_{n_{k+1}} \cap G_m) \setminus G_{n_k}\big) \cup \big((B_{n_k} \cap G_m) \setminus G_{n_{k-1}}\big) = (G_m \setminus G_{n_k}) \cup (B_{n_k} \setminus G_{n_{k-1}}),$$

where we have used the fact that $B_{n_k} \subset G_{n_k} \subset G_m \subset G_{2n_k} \subset B_{n_{k+1}}$. Hence,

$$\begin{aligned} \frac{|A_m|}{p^m} &\geq 1 - \frac{1}{p^{m-n_k}} + \frac{\delta}{p^{m-n_k}} - \frac{1}{p^{m-n_{k-1}}} \\ &\geq \delta - \frac{1}{p^{n_{k-1}}}, \end{aligned} \tag{6.58}$$

since $m > n_k > 2n_{k-1}$ and $1 - \frac{1}{a} + \frac{\delta}{a} \geq \delta$ for $a := p^{m-n_k} > 1$. Thus in any case (6.56) is true, and $\liminf_{n\to\infty} \frac{|A_n|}{|G_n|} \geq \delta$.

Putting everything together, we have

$$\delta \leq \liminf_{n\to\infty} \frac{|A_n|}{|G_n|} \leq \liminf_{n\to\infty} \frac{|A_n + H_n|}{|G_n|} \leq \delta, \tag{6.59}$$

which implies $\delta = \underline{d}(A) = \liminf_{n\to\infty} \frac{|A_n+H_n|}{|G_n|}$, as desired. □

6.4 Proof of Theorem 1.7.4

Recall that $\mathbf{1}_n := 1 + t + \cdots + t^{n-1}$ and

$$H = \cup_{n=1}^{\infty} \left\{ x + \mathbf{1}_n : x \in G_n, |\mathrm{supp}(x)| \leq \eta\sqrt{n} \right\}.$$

In order to prove that H is an essential component, we establish the following lemma.

Lemma 6.4.1. *Let $0 < \eta < 1$ be a real number and let $B_n = \{x : x \in G_n, |\mathrm{supp}(x)| \leq \eta\sqrt{n}\}$. Then for all $n \geq 4/\eta^2$ and $A_n \subset G_n$, we have*

$$|A_n + B_n| \geq |A_n| + c'|A_n| \left(1 - \frac{|A_n|}{p^n}\right)$$

where $c' > 0$ is a constant depending on p and η.

Proof. For $K_n = \{x : x \in G_n, |\mathrm{supp}(x)| \leq 1\}$, by Lemma 6.1.6, we know that for any $A_n \subset G_n$ with density $\frac{|A_n|}{p^n} = \delta$,

$$\frac{|A_n + K_n|}{p^n} \geq \delta + \frac{c(p)}{\sqrt{n}} \delta \left(1 - \delta\right) \tag{6.60}$$

for some constant $0 < c(p) \leq 1$. Since for $j \in \mathbb{Z}^+$ the j-fold sumset of K_n can be expressed as $jK_n = \{x : x \in G_n, |\mathrm{supp}(x)| \leq j\}$, we hence observe that

$$B_n = \lfloor \eta\sqrt{n} \rfloor K_n. \tag{6.61}$$

Let $\varphi(x) = x + \frac{c(p)}{\sqrt{n}} x(1-x)$ and let $\varphi^{(0)}(x) = x, \varphi^{(j)}(x) = \varphi(\varphi^{(j-1)}(x))$ for $j \geq 1$. It is clear that $\varphi(x)$ is increasing and bounded by 1 for all $0 < x < 1$. Thus, for $j \geq 1$,

by iterating the inequality (6.60) $\lfloor \eta\sqrt{n} \rfloor$ times, we obtain that

$$\frac{|A_n + \lfloor \eta\sqrt{n} \rfloor K_n|}{p^n} \geq \varphi^{(\lfloor \eta\sqrt{n} \rfloor)}(\delta). \tag{6.62}$$

Now, we claim that

$$\varphi^{(\lfloor \eta\sqrt{n} \rfloor)}(\delta) \geq \delta + \frac{\eta c(p)}{3}\delta(1-\delta). \tag{6.63}$$

On the one hand, if

$$\varphi^{(j)}(\delta)(1-\varphi^{(j)}(\delta)) > \left(1 - \frac{\eta c(p)}{3}\right)\delta(1-\delta)$$

holds for all $0 \leq j < \lfloor \eta\sqrt{n} \rfloor$, we write $\varphi^{(\lfloor \eta\sqrt{n} \rfloor)}(\delta) - \delta$ as a telescoping sum and deduce that

$$\begin{aligned}\varphi^{(\lfloor \eta\sqrt{n} \rfloor)}(\delta) - \delta &= \sum_{j=0}^{\lfloor \eta\sqrt{n} \rfloor - 1} \left(\varphi^{(j+1)}(\delta) - \varphi^{(j)}(\delta)\right) = \sum_{j=0}^{\lfloor \eta\sqrt{n} \rfloor - 1} \frac{c(p)}{\sqrt{n}}\, \varphi^{(j)}(\delta)\left(1 - \varphi^{(j)}(\delta)\right) \\ &\geq \frac{(\eta\sqrt{n}-1)c(p)}{\sqrt{n}} \cdot \frac{3 - \eta c(p)}{3} \cdot \delta(1-\delta) \geq \frac{\eta c(p)}{3}\delta(1-\delta),\end{aligned}$$

where we applied $\varphi^{(j+1)}(x) - \varphi^{(j)}(x) = \frac{c(p)}{\sqrt{n}}\varphi^{(j)}(x)(1-\varphi^{(j)}(x))$ for each $j < \lfloor \eta\sqrt{n} \rfloor$ and the fact that $\eta\sqrt{n} \geq 2$.

On the other hand, if there exists $0 \leq k < \lfloor \eta\sqrt{n} \rfloor$ such that

$$\varphi^{(k)}(\delta)(1-\varphi^{(k)}(\delta)) \leq \left(1 - \frac{\eta c(p)}{3}\right)\delta(1-\delta),$$

then

$$\begin{aligned}\frac{\eta c(p)}{3}\delta(1-\delta) &\le \delta(1-\delta) - \varphi^{(k)}(\delta)(1-\varphi^{(k)}(\delta)) \\ &\le |\varphi^{(k)}(\delta) - \delta| \cdot |\varphi^{(k)}(\delta) + \delta - 1| \\ &\le \varphi^{(k)}(\delta) - \delta \\ &\le \varphi^{(\lfloor \eta\sqrt{n} \rfloor)}(\delta) - \delta,\end{aligned}$$

since $\varphi(x)$ is increasing and bounded by 1. Combining two cases, we thus complete the proof with $c' = \frac{\eta c(p)}{3}$. □

With the notations defined in the previous lemma, we let

$$L_n := \mathbf{1}_n + B_n = \left\{ x + \mathbf{1}_n : x \in G_n, |\mathrm{supp}(x)| \le \eta\sqrt{n} \right\}.$$

Then

$$H = \cup_{n=1}^{\infty} L_n$$

and $H_n \supset L_n$ for any n. (The purpose of translating the B_n's by $\mathbf{1}_n$ is to make them sufficiently far away from the G_n's. If not, then $\cup_{n=1}^{\infty} B_n$ is also an essential component, but it is easy to see that $\cup_{n=1}^{\infty} B_n = G$.) Let $A_n \subset G$ be a subset with $\underline{d}(A) = \delta \in (0,1)$. Then for any n sufficiently large, we have

$$\frac{|A_n + H_n|}{p^n} \ge \frac{|A_n + L_n|}{p^n} = \frac{|A_n + B_n|}{p^n} \ge \frac{|A_n|}{p^n} + c'\frac{|A_n|}{p^n}\left(1 - \frac{|A_n|}{p^n}\right).$$

Taking lim inf of both sides, we have

$$\liminf_{n\to\infty} \frac{|A_n + H_n|}{p^n} \ge \liminf_{n\to\infty} \frac{|A_n|}{p^n} + c'\frac{|A_n|}{p^n}\left(1 - \frac{|A_n|}{p^n}\right) \ge \delta + c'\delta(1-\delta)$$

since the function $x \mapsto x + c'x(1-x)$ is increasing on (0,1). This shows that H is an essential component in G.

Next we estimate $|H_n|$. Since $L_n = \mathbf{1}_n + B_n$,

$$|L_n| = |B_n| = \sum_{k=0}^{\lfloor \eta\sqrt{n} \rfloor} \binom{n}{k} (p-1)^k \leq \eta\sqrt{n} \cdot p^{\eta\sqrt{n}} \cdot n^{\eta\sqrt{n}} = \exp\left(O_p(\eta\sqrt{n}\log n)\right).$$

Moreover, we can see that

$$L_n \subset \left\{x : x \in G_n, |\mathrm{supp}(x)| \geq n - \eta\sqrt{n}\right\}.$$

Suppose $L_m \cap G_n \neq \emptyset$. Let $x \in L_m \cap G_n$, then $m - \eta\sqrt{m} \leq |\mathrm{supp}(x)| \leq n$, which implies that $m \leq 2n$ if n is sufficiently large. Therefore,

$$\begin{aligned} |H_n| &= |H \cap G_n| = |\cup_{m=1}^{\infty}(L_m \cap G_n)| \\ &= \left|\cup_{m=1}^{2n}(L_m \cap G_n)\right| \leq 2n|L_{2n}| = \exp(O_p(\eta\sqrt{n}\log n)), \end{aligned}$$

which completes the proof.

6.5 Further discussions

Just like in $\mathbb{N}$, it is desirable to have explicit constructions of essential components in $\mathbb{F}_p[t]$ with small counting functions. Erdős [33, p. 147] asked whether the set $\{2^n 3^m : m, n \in \mathbb{N}\}$ is an essential component in $\mathbb{N}$. This is in keeping with the principle that multiplicative and additive structures don't mix well, as exemplified by sum-product estimates. Note that the counting function of this set is $O(\log^2 x)$. The following question is perhaps more tractable.

Problem 1. *Can one prove or disprove a similar statement in $\mathbb{F}_p[t]$? For example, is the set $\{t^n(t+1)^m : m, n \in \mathbb{N}\}$ an essential component in $\mathbb{F}_2[t]$?*

The problem of essential components also makes sense, and is perhaps even more natural in the finite setting, i.e. $\mathbb{F}_p^n$ (where p is fixed and $n \to \infty$). Again, using the

probabilistic method, Ruzsa [31, Section 8] showed that in any finite abelian group G, there is a set H with size $|H| = O(\log |G|)$ such that if $A \subset G$ has density δ, then $A + H$ has density $\geq \delta + c\delta(1 - \delta)$, where $c > 0$ is an absolute constant. (By making his argument explicit, we can choose $c = 5/9$ and $|H| \leq 25 \log |G|$.) Thus the following problem is interesting.

Problem 2. *Find a set $H \subset \mathbb{F}_p^n$ such that $|H| = O_p(n)$ (or even $O_p(n^{O(1)})$) with the property that whenever $A \subset \mathbb{F}_p^n$ has density $0 < \delta < 1$, $A + H$ has density $\delta + f(\delta)$, where $f : (0, 1) \to (0, \infty)$ is a function (independent of n)).*

In view of Lemma 6.1.6 , a natural candidate for H is a union of $O_p(1)$ vector space bases of $\mathbb{F}_p^n$.

BIBLIOGRAPHY

[1] B. C. Berndt, R. J. Evans, and K. S. Williams, **Gauss and Jacobi Sums**, Wiley-Interscience, 1st ed (1998).

[2] B. Bollobás, I. Leader, *Compressions and isoperimetric inequalities*, J. Combin. Theory Ser. A 56 (1991), no. 1, 47–62.

[3] A. R. Booker, M. B. Milinovich, and N. Ng, *Subconvexity for modular form L-functions in the t aspect*, Adv. Math. 341 (2019), 299–335.

[4] S. Boucheron, G. Lugosi, and P. Massart, **Concentration inequalities: A nonasymptotic theory of independence**, Oxford University Press, (2016).

[5] J. R. Burke, *A notion of density and essential components in $GF[p, x]$*, Acta Arith. 44 (1984), no. 4, 299–306.

[6] D. Christofides, D. Ellis, P. Keevash, *An approximate isoperimetric inequality for r-sets*, Electron. J. Combin. 20 (2013), no. 4, Paper 15, 12 pp.

[7] K. Chandrasekharan, R. Narasimhan, *Functional equations with multiple Gamma fatcotrs and the average order of arithmetical functions*, Ann. of Math., (2) 76 (1962), 93–136.

[8] P. Erdős, *On the arithmetical density of the sum of two sequences one of which forms a basis for the integers*, Acta. Arith., 1(2) (1935), 197–200.

[9] S. M. Gonek, *Mean values of the Riemann zeta-function and its derivatives*, Invent. math. 75 (1984), 123–141.

[10] S. M. Gonek, A. Ivić, *On the distribution of positive and negative values of Hardy's Z-function*, J. Number Theory (2017), 189–201.

[11] B. Green, *Some constructions in the inverse spectral theory of cyclic groups*, Combin. Probab. Comput. 12 (2003), no. 2, 127–138.

[12] A. Gut, *Probability: A Graduate Course (Springer Texts in Statistics)*, Springer-Verlag New York, (2013)

[13] H. Halberstam, K. F. Roth, **Sequences**. Springer-Verlag, New York, 1983.

[14] L. H. Harper, *Optimal numberings and isoperimetric problems on graphs*, J. Combinatorial Theory 1 (1966), 385–393.

[15] G. H. Hardy, *Sur les zeros de la fonction $\zeta(s)$*, Comp. Rend. Acad. Sci., 158 (1914), 1012–1014.

[16] A. Ivić, *On the integral of Hardy's function*, Arch. Math., 83 (2004), 41–47.

[17] H. Iwaniec, **Topics in classical automorphic forms**, Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997.

[18] H. Iwaniec, **Spectral methods of automorphic forms**, Second edition. Graduate Studies in Mathematics, 53. American Mathematical Society, Providence, RI; Revista Matemática Iberoamericana, Madrid, 2002.

[19] H. Iwaniec, E. Kowalski, **Analytic number theory**, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[20] M. Jutila, *Atkinson's formula for Hardy's function*, J. Number Theory, 129 (2009), 2853–2878.

[21] ———, *An asymptotic formula for the primitive of Hardy's function*, Ark. Mat., 49 (2011), 97–107.

[22] A. Khinchin, *Über ein metrisches Problem der additiven Zahlentheorie*, Mat. Sb., 40:2 (1933), 180–189.

[23] M. A. Korolev, *On the primitive of the Hardy function $Z(t)$*, Doklady Mathematics, 75 (2007) 295–298.

[24] T. H. Lê, **Topics in arithmetic combinatorics in function fields**, PhD Thesis, UCLA (2010).

[25] U. V. Linnik, *On Erdős's theorem on the addition of numerical sequences*, Rec. Math. [Mat. Sbornik] N.S., 10(52):1–2 (1942), 67–78.

[26] C. McDiarmid, *On the method of bounded differences*, **Surveys in combinatorics, 1989** (Norwich, 1989), volume 141 of London Math. Soc. Lecture Note Ser., pages 148–188. Cambridge Univ. Press, Cambridge, 1989.

[27] H. L. Montgomery, R. C. Vaughan, **Multiplicative number theory. I. Classical theory**, Cambridge Studies in Advanced Mathematics, 97. Cambridge University Press, Cambridge, 2007.

[28] H. Plünnecke, **Eigenschaften und Abschdtzungen von Wirkungsfunktionen**, Ges. Mathem. und Datenverarbeitung 22 (Bonn, 1969).

[29] Y. V. Prokhorov, V. Statulevicius (Eds.), **Limit Theorems of Probability Theory**, Springer-Verlag Berlin Heidelberg, (2000)

[30] I. Z. Ruzsa, *Sumsets and structure*, **Combinatorial number theory and additive group theory**, Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser Verlag, Basel, 2009.

[31] ———, *Essential components*, Proc. London Math. Soc. (3) 54 (1987), no. 1, 38–56.

[32] ———, *Arithmetic progressions in sumsets*, Acta Arith. 60 (1991), no. 2, 191–202.

[33] ———, *Erdős and the integers*, J. Number Theory 79 (1999), no. 1, 115–163.

[34] T. Sanders, *Green's sumset problem at density one half*, Acta Arith. 146 (2011), no. 1, 91–101.

[35] P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. 313 (1980), 161–170.

[36] G. Tenenbaum, **Introduction to analytic and probabilistic number theory**, Third edition. Translated from the 2008 French edition by Patrick D. F. Ion. Graduate Studies in Mathematics, 163. American Mathematical Society, Providence, RI, 2015.

[37] E. C. Titchmarsh, **The theory of the Riemann zeta-function**, 2nd ed., revised by D. R. Heath-Brown, Oxford Science Publications, 1986.

[38] E. Wirsing, *Thin essential components*, **Topics in number theory** (Proc. Colloq., Debrecen, 1974), pp. 429–442. Colloq. Math. Soc. János Bolyai, Vol. 13, North-Holland, Amsterdam, 1976.

[39] J. Wolf, *The structure of popular difference sets*, Israel J. Math. 179 (2010), 253–278.

VITA

The author was born on May 23, 1989 in Kunshan, Jiangsu China. He graduated from Suzhou High school in 2008 and then enrolled at Jilin Normal University, where he graduated with a B.S. in Mathematics in 2012. Later, he began his graduate studies at the University of Mississippi in number theory under the supervision of Professors Micah B. Milinovich and Thái Hoàng Lê. In the spring of 2015, he earned an M.S. in Mathematics. He is one of the two recipients of a 2018–2019 University of Mississippi College of Liberal Arts Graduate Student Achievement Award in the natural sciences.