Short character sums for composite moduli *†

Mei-Chu Chang‡
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

We establish new estimates on short character sums for arbitrary composite moduli with small prime factors. Our main result improves on the Graham-Ringrose bound for square free moduli and also on the result due to Gallagher and Iwaniec when the core $q' = \prod_{p|q} p$ of the modulus q satisfies $\log q' \sim \log q$. Some applications to zero free regions of Dirichlet L-functions and the Pólya and Vinogradov inequalities are indicated.

Introduction.

In this paper we will discuss short character sums for moduli with small prime factors. In particular, we will revisit the arguments of Graham-Ringrose and Postnikov. Our main result is an estimate valid for general moduli, which improves on the known estimates in certain situations.

It is well known that non-trivial estimates on short character sums are important to many number theoretical issues. In particular, they are relevant in establishing density free regions for the corresponding Dirichlet L-functions.

More specifically, we prove the following.

Let χ be a primitive multiplicative character to the modulus q, and let p be the largest prime divisor of q, $q' = \prod_{p|q} p$ and $K = \frac{\log q}{\log q'}$. Let I be an interval of size $|I| = N$. We will denote various constants by C.

*2000 *Mathematics Subject Classification.* 11L40, 11M06.
†*Key words.* character sums, zero free regions
‡Research partially financed by the National Science Foundation.

Theorem 5. *Assume $q > N > p^C$ and*

$$\log N > (\log q)^{\frac{9}{10}} + C \frac{\log q'}{\log\log q'} \log 2K \tag{1}$$

Then

$$\Big|\sum_{x\in I} \chi(x)\Big| < Ne^{-\sqrt{\log N}}. \tag{2}$$

Note that assumption (1) of Theorem 5 is implied by the stronger and friendlier assumption

$$\log N > C\Big(\log p + \frac{\log q}{\log\log q}\Big). \tag{3}$$

Assumption (3) is weaker than Graham-Ringrose's condition

$$\log N > C\Big(\log p + \frac{\log q}{\sqrt{\log\log q}}\Big).$$

(The Graham-Ringrose estimate was established only for square free moduli.) Also, condition (1) is weaker than Postnikov-Gallagher-Iwaniec's assumption $\log N \gg \log q' + (\log q)^{\frac{2}{3}+\epsilon}$ in certain cases, namely when $\log q'$ becomes comparable with $\log q$.

Many techniques used in the paper are just elaborations of known arguments. What differs from methods previously used on similar problems is the use of a (new) mixed character sum estimate in conjunction with Postnikov's argument for powerful moduli, whose usual treatment exploits Vinogradov's exponential sum estimate at the end. This allows us to combine efficiently the methods introduced by Graham-Ringrose and Postnikov and obtain non-trivial bounds under less restrictive conditions for a large class of moduli.

Next, we turn to some (routine) consequences of Theorem 5.

Theorem 8. Let $M = (\log q)^{\frac{9}{10}} + \frac{\log q'}{\log\log q'} \log 2K + \log p$. Then

$$\Big|\sum_{n<x} \chi(n)\Big| \ll \sqrt{q}\sqrt{\log q}\sqrt{M}.$$

If q is square free, then the bound in Theorem 8 is

$$\sqrt{q}\left(\frac{\log q}{\sqrt{\log\log q}}+\sqrt{\log q}\sqrt{\log p}\right).$$

It gives an improvement on Goldmakher's result. (See [G], Theorem 1.)

Theorem 5 implies the following zero-free regions for the corresponding Dirichlet L-functions.

Theorem 11. *Let*

$$\theta = c\min\left(\frac{1}{\log p}, \frac{\log\log q'}{(\log q')\log 2K}, \frac{1}{(\log qT)^{9/10}}\right).$$

Then the Dirichlet L-function $L(s,\chi)=\sum_n \chi(n)n^{-s}$, $s=\rho+it$ *has no zeros in* $\rho > 1-\theta, \quad |t|<T$ *except for possible Siegel zeros.*

In certain ranges, this improves upon Iwaniec's condition [I]

$$\theta = \min\left\{c\frac{1}{(\log qT)^{\frac{2}{3}}(\log\log qT)^{\frac{1}{3}}}, \frac{1}{\log q'}\right\}.$$

Using the zero-free region above and the result from [HB2] on the effect of a possible Siegel zero, we obtain the following. (cf. the discussion in [HB1])

Corollary 12. *Assume q satisfies that* $\log p = o(\log q)$ *for* $p|q$. *If* $(a,q)=1$, *then there is a prime* $P\equiv a(\text{mod } q)$ *such that* $P < q^{\frac{12}{5}+O(1)}$.

Notation and Convention.

1. $e(\theta)=e^{2\pi i\theta}$, $e_p(\theta)=e(\frac{\theta}{p})$.
2. $\omega(q)=$ the number of prime divisors of q.
3. $\tau(q)=$ the number of divisors of q.
4. $q'=\prod_{p|q} p$, the core of q.
5. When there is no ambiguity, $p^{\varepsilon}=[p^{\varepsilon}]\in\mathbb{Z}$.
6. Modulus p (or q) is always sufficiently large.
7. For polynomials $f(x)$ and $g(x)$, the *degree* of $\frac{f(x)}{g(x)}$ is $\deg f(x)+\deg g(x)$.
8. $c, C=$ various constants.

1 Mixed character sums.

The following theorem is from [C1] for prime modulus.

Theorem 1. *Let $P(x) \in \mathbb{R}[X]$ be an arbitrary polynomial of degree $d \geq 1$, p a sufficiently large prime, $I \subset [1, p]$ an interval of size*

$$|I| > p^{\frac{1}{4}+\kappa} \tag{1.1}$$

(for some $\kappa > 0$) and χ a nontrivial multiplicative character (mod p)*. Then*

$$\Big|\sum_{n\in I} \chi(n) e^{iP(n)}\Big| < |I|\, p^{-c\,\kappa^2 d^{-2}}. \tag{1.2}$$

In the proof of Theorem 1, the assumption p being prime is only used in order to apply Weil's bound on complete exponential sums. (For Weil's bound, see Theorem 11.23 in [IK])

Let $f \in \mathbb{Z}[x]$ be a polynomial of degree d and let χ be a multiplicative character (mod q) and of order $r > 1$.

Weil's Theorem. *Let $q = p$ be prime. Suppose f(mod p) is not a r-th power. Then we have*

$$\Big|\sum_{x=1}^{p} \chi(f(x))\Big| \leq d\,\sqrt{p}.$$

For $q = p_1 \cdots p_k$ square free, since $|\sum_{x=1}^{q} \chi(f(x))| \leq \prod_{i=1}^{k} |\sum_{x=1}^{p_i} \chi_i(f(x))|$, where χ_i is a multiplicative character (mod p_i), we have the following version of Weil's estimate.

Weil's Theorem'. *Let q be square free and let $q_1|q$ be such that for any prime $p|q_1$, f(mod p) has a simple root or a simple pole. Then*

$$\Big|\sum_{x=1}^{q} \chi(f(x))\Big| \leq d^{\,\omega(q_1)} \frac{q}{\sqrt{q_1}}.$$

Therefore, we have the following.

Theorem 1'. *Let $P(x) \in \mathbb{R}[X]$ be an arbitrary polynomial of degree $d \geq 1$, $q \in \mathbb{Z}$ square free and sufficiently large, $I \subset [1, q]$ an interval of size*

$$|I| > q^{\frac{1}{4}+\kappa} \tag{1.3}$$

(for some $\kappa > 0$) and χ a nontrivial multiplicative character (mod q). *Then*

$$\Big| \sum_{n \in I} \chi(n) e^{iP(n)} \Big| < |I| \, q^{-c\kappa^2 d^{-2}} \tau(q)^{4(\log d) d^{-2}}. \tag{1.4}$$

2 Postnikov's Theorem.

An immediate application is obtained by combining Theorem 1' with Postnikov's method (See [P], [Ga], [I], and [IK] §12.6).

Postnikov's Theorem. *Let χ be a primitive multiplicative character* (mod q), *$q = q_0^m$. Then*

$$\chi(1 + q_0 u) = e_q\big(F(q_0 u)\big).$$

Here $F(x) \in \mathbb{Z}[X]$ is a polynomial of the form

$$F(x) = BD\Big(x - \frac{x^2}{2} + \cdots \pm \frac{x^{m'}}{m'}\Big) \tag{2.1}$$

with

$$D = \prod_{\substack{k \leq m' \\ (k, q_0) = 1}} k, \quad m' = 2m$$

and $B \in \mathbb{Z}, (B, q_0) = 1$.

Remark. In [IK] the above theorem was proved for $\chi(1 + q'u) = e_q(F(q'u))$, where $q' = \prod_{p|q} p$ is the core of q. That argument works verbatim for our case.

Theorem 2. *Let $q = q_0^m q_1$ with $(q_0, q_1) = 1$ and q_1 square free.*

Assume $I \subset [1, q]$ an interval of size

$$|I| > q_0 q_1^{\frac{1}{4}+\kappa}. \tag{2.2}$$

Let χ be a multiplicative character $\pmod q$ *of the form*

$$\chi = \chi_0 \chi_1$$

with $\chi_0 (\bmod\, q_0^m)$ *arbitrary and* $\chi_1 (\bmod\, q_1)$ *primitive. Then*

$$\Big| \sum_{n \in I} \chi(n) \Big| \ll |I| q_1^{-c\kappa^2 m^{-2}} \tau(q_1)^{c(\log m) m^{-2}}. \tag{2.3}$$

Proof. For $a \in [1, q_0], (a, q_0) = 1$ fixed, using Postnikov's Theorem, we write

$$\chi_0(a + q_0 x) = \chi_0(a) \chi_0(1 + q_0 \bar{a} x) = \chi_0(a) e_{q_0^m}\big(F(q_0 \bar{a} x)\big), \tag{2.4}$$

where

$$a\bar{a} = 1 \pmod{q_0^m}.$$

Hence

$$\Big| \sum_{n \in I} \chi(n) \Big| \le \sum_{(a, q_0) = 1} \Big| \sum_{a + q_0 x \in I} e_{q_0^m}\big(F(q_0 \bar{a} x)\big) \chi_1(a + q_0 x) \Big|. \tag{2.5}$$

Writing $\chi_1(a + q_0 x) = \chi_1(q_0) \chi_1(a \bar{q}_0 + x), q_0 \bar{q}_0 \equiv 1 (\bmod\, q_1)$, the inner sum in (2.5) is a sum over an interval $J = J_a$ of size $\sim \frac{|I|}{q_0}$ and Theorem 1' applies. □

3 Graham-Ringrose Theorem.

As a warm up, in this section we will reproduce Graham-Ringrose's argument. With some careful counting of the *bad* set, we are able to improve their condition on the size of the interval from $q^{1/\sqrt{\log \log q}}$ to $q^{C/\log \log q}$.

Theorem 3. *Let $q \in \mathbb{Z}$ be square free, χ a primitive multiplicative character* $\pmod q$*, and $N < q$. Assume*

1. *For all $p | q$, $p < N^{\frac{1}{10}}$.*
2. $\log N > C \frac{\log q}{\log \log q}$.

Then

$$\Big|\sum_{x=1}^{N}\chi(x)\Big| < Ne^{-\sqrt{\log N}}.$$

We will prove the following stronger and more technically stated theorem.

Theorem 3' *Assume $q = q_1 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square free. Factor*

$$\chi = \chi_1 \cdots \chi_r,$$

where $\chi_i (\text{mod } q_i)$ is arbitrary for $i < r$, and primitive for $i = r$. We further assume

(i). *For all $p|q_r, p > \sqrt{\log q}$.*

(ii). *For all i, $q_i < N^{\frac{1}{3}}$.*

(iii). $r < c \log\log q$.

Then

$$\Big|\sum_{x=1}^{N}\chi(x)\Big| < Ne^{-\sqrt{\log q_r}}.$$

Remark 3.1. To see that Theorem 3' implies Theorem 3, we write

$$q = \bar{p}_1 \cdots \bar{p}_\ell \cdot p_1 \cdot p_2 \cdots,$$

where

$$\bar{p}_1, \dots, \bar{p}_\ell < \sqrt{\log q}, \quad \text{and} \quad p_1 > p_2 > \cdots \geq \sqrt{\log q}.$$

Hence

$$\prod_{i=1}^{\ell} \bar{p}_i < e^{\sqrt{\log q}} < q^{\frac{1}{10}}. \tag{3.1}$$

Let $q_r = \prod_{i=1}^{k} p_i$ such that k is the maximum subject to the condition that $q_r < N^{\frac{1}{3}}$

Therefore, $p_1 q_r > N^{\frac{1}{3}}$. By (1), $q_r > N^{\frac{1}{3}-\frac{1}{10}} > N^{\frac{1}{5}}$.

We repeat this process on

$$\frac{q}{q_r}$$

to get q_{r-1} such that $N^{\frac{1}{3}} > q_{r-1} > N^{\frac{1}{5}}$. Then, we repeat it on $\frac{q}{q_r q_{r-1}}$ etc. After re-indexing, we have

$$q_r, q_{r-1}, \ldots, q_2 > N^{\frac{1}{5}}.$$

Hence $q > \left(N^{\frac{1}{5}}\right)^{r-1}$, which together with (2) give (iii). $\square$

Under the assumption of Theorem 3', we give the following

Definition. For $\bar{q}|q_r$ satisfying $\bar{q} > \sqrt{q_r}$, and $f \in \mathbb{Z}[x]$ of degree d, the pair $(f, \bar{q})$ is called *admissible* if

$$\prod_{\substack{p|\bar{q} \\ f \bmod p \text{ satisfies } (*)}} p \;>\; \frac{\bar{q}}{q_r^{\tau}}, \qquad \text{where } \tau = \frac{10}{\log\log q_r},$$

and (*) means

(*) (The polynomial) has a simple root or a simple pole.

Remark 3.2. If $(f, \bar{q})$ is admissible, χ primitive mod $\bar{q}$ and

$$\log d < \frac{1}{\tau} = \frac{\log\log q_r}{10} \tag{3.2}$$

then

$$\left|\sum_{x=1}^{\bar{q}} \chi(f(x))\right| < (\bar{q})^{\frac{7}{10}} q_r^{\frac{3}{10}\tau}.$$

Proof of Remark 3.2. We say p is good, if f mod p satisfies (*). For $p|\bar{q}|q_r$, assumption (i) implies that $p > \sqrt{\log q}$. In particular, (3.2) implies

$$p^{1/5} > (\log q)^{1/10} > d. \tag{3.3}$$

Weil's estimate gives

$$\left|\sum_{x=1}^{\bar{q}} \chi(f(x))\right| < \frac{\bar{q}}{\sqrt{q_1}}\, d^{\,\omega(q_1)} \tag{3.4}$$

where q_1 is the product of the good primes p. Using (3.3), we bound the character sum above by

$$\bar{q}\prod_{p|q_1}\frac{d}{\sqrt{p}} < \bar{q}\prod_{p|q_1} p^{-3/10} = \bar{q}q_1^{-3/10}.$$

Since $(f,\bar{q})$ is admissible, we have

$$\left|\sum_{x=1}^{\bar{q}}\chi(f(x))\right| < \bar{q}q_1^{-\frac{3}{10}} < (\bar{q})^{\frac{7}{10}}q_r^{\frac{3}{10}\tau}. \qquad \square$$

Proof of Theorem 3'. Take $M = \left[\sqrt{N}\,\right]$. Shifting the interval $[1,N]$ by yq_i for any $1 \le y \le M$, we get

$$\Big|\ \sum_{x=1}^{n}\chi(x)\ - \sum_{x=1}^{n}\chi(x+yq_1)\ \Big| \le 2yq_1 \lesssim Mq_1.$$

Averaging over the shifts gives

$$\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| \le \frac{1}{NM}\sum_{x=1}^{N}\Big|\sum_{y=1}^{M}\chi(x+yq_1)\Big| + O\left(\frac{Mq_1}{N}\right). \tag{3.5}$$

Let

$$\chi_1' = \chi_2\cdots\chi_r.$$

Using the q_1-periodicity of χ_1 and Cauchy-Schwarz on the double sum in (3.5), we have

$$\frac{1}{NM}\sum_{x=1}^{N}\Big|\sum_{y=1}^{M}\chi(x+yq_1)\Big| \le \left[\frac{1}{NM^2}\sum_{y,\,y'=1}^{M}\ \Big|\sum_{x=1}^{N}\chi_1'\left(\frac{x+q_1y}{x+q_1y'}\right)\Big|\ \right]^{1/2}. \tag{3.6}$$

For given (y,y'), we consider

$$f_{y,y'}(x) = \frac{x+q_1y}{x+q_1y'}$$

and distinguish among the pairs $(f_{y,y'},q_r)$ by whether or not they are admissible. Note that if $(f_{y,y'},q_r)$ is not admissible, then the product of *bad* prime factors of q_r is at least q_r^τ. We will estimate the size of the set of bad (y, y') and use trivial bound for the inner sum in (3.6).

$$\begin{aligned}
&\Big|\big\{(y, y') \in [1, M]^2 : (f_{y,y'}, q_r) \text{ is not admissible }\big\}\Big| \\
\le& \sum_{\substack{Q|q_r \\ Q>q_r^\tau}} \Big|\big\{(y, y') \in [1, M]^2 : Q|\ y - y'\ \big\}\Big| \\
\le& \sum_{\substack{Q|q_r \\ Q>q_r^\tau}} \frac{M^2}{Q} < 2^{\omega(q_r)}\frac{M^2}{q_r^\tau} < M^2 q_r^{-\frac{7}{\log\log M}} = M^2 q_r^{-\frac{7}{10}\tau}.
\end{aligned} \tag{3.7}$$

(For the second inequality, we note that $M > Q$.)

Hence (3.6) is bounded by

$$q_r^{-\frac{7}{20}\tau} + \Big|\frac{1}{N}\sum_{x=1}^{N} \chi_1'(f_1(x))\Big|^{\frac{1}{2}}, \tag{3.8}$$

where f_1 is the $f_{y,y'}$ with the maximal character sum among all admissible pairs. i.e.

$$\Big|\sum_{x=1}^{N} \chi_1'(f_1(x))\Big| = \max_{\substack{f_{y,y'} \\ (f_{y,y'},q_r) \text{ admissible}}} \Big|\sum_{x=1}^{N} \chi_1'(f_{y,y'}(x))\Big|. \tag{3.9}$$

Thus, there exists $\bar{q}_1|q_r$, $\bar{q}_1 > q_r^{1-\tau}$ and for any $p|\bar{q}_1$, f_1 mod p has property (*).

We will use induction to bound the second term in (3.8). After s steps, we reduce the problem to bounding the character sum

$$\frac{1}{N}\Big|\sum_{x=1}^{N} \chi_s'(f_s(x))\Big|, \tag{3.10}$$

where $\chi_s' = \chi_{s+1}\cdots\chi_r$, $f_s \in \mathbb{Z}[x]$ with $\deg f_s = 2^s$. Since $(f_s, \bar{q}_{s-1})$ is admissible, there is $\bar{q}_s|q_r$ such that $\bar{q}_s > q_r^{1-s\tau}$ and $\forall p|\bar{q}_s$ is good.

As before, the q_{s+1}-periodicity of χ_{s+1} and Cauchy-Schwarz give a bound on (3.10) by

$$\left[\frac{1}{NM^2}\sum_{y,\, y'=1}^{M} \Big|\sum_{x=1}^{N} \chi_{s+1}'\left(\frac{f_s(x+q_{s+1}y)}{f_s(x+q_{s+1}y')}\right)\Big|\right]^{1/2}. \tag{3.11}$$

Set

$$f_{s+1}(x) = \frac{f_s(x + q_{s+1}y)}{f_s(x + q_{s+1}y')} \ ,$$

where (y, y') is chosen as in (3.9), such that the inner character sum in (3.11) is the maximum.

We want to bound the set of bad (y, y'). For $p|\bar{q}_s$,

$$f_s(x) = (x-a)^{\pm 1} \prod_j (x - b_j)^{c_j}, \quad \text{where } a \neq b_j. \qquad \text{mod } p$$

Hence

$$f_{s+1}(x) = \left(\frac{x + q_{s+1}y - a}{x + q_{s+1}y' - a} \right)^{\pm 1} \prod_j \left(\frac{x + q_{s+1}y - b_j}{x + q_{s+1}y' - b_j} \right)^{c_j} .$$

For $y \neq y'$ mod p, if $a - q_{s+1}y$ is not a simple root or pole, then

$$a - q_{s+1}y = b_j - q_{s+1}y', \qquad \text{mod } p$$

for some j. Therefore,

$$\begin{aligned} &\left| \left\{ (y, y') \in [1, M]^2 : (f_{y,y'}, \bar{q}_s) \text{ is not admissible } \right\} \right| \\ \leq &\sum_{\substack{Q|\bar{q}_s \\ Q > q_r^\tau}} \left| \left\{ (y, y') \in [1, M]^2 : \forall p|Q, f_{y,y'} \text{ mod } p \text{ satisfies } (*) \right\} \right| \\ \leq &\sum_{\substack{Q|\bar{q}_s \\ Q > q_r^\tau}} \frac{M^2}{Q} \left(2^s\right)^{\omega(Q)} = M^2 \sum_{\substack{Q|\bar{q}_s \\ Q > q_r^\tau}} \frac{\left(2^s\right)^{\omega(Q)}}{Q} \ . \end{aligned} \tag{3.12}$$

By assumptions (i) and (iii),

$$\frac{\left(2^s\right)^{\omega(Q)}}{Q} \leq \prod_{p|Q} \frac{2^r}{p} < \prod_{p|Q} \frac{1}{\sqrt{p}} = \frac{1}{\sqrt{Q}} < q_r^{-\frac{\tau}{2}}, \tag{3.13}$$

and (3.12) is bounded by

$$M^2 \, \frac{2^{\omega(q_r)}}{q_r^{\tau/2}} < M^2 q_r^{-\tau/5}.$$

At the last step, we are bounding

$$\Big|\sum_{x=1}^{N}\chi_r(f_{r-1}(x))\Big|, \tag{3.14}$$

where $f_{r-1}\in\mathbb{Z}[x]$ with $\deg f_{r-1}=2^{r-1}$ and there is $\bar{q}_{r-1}|q_r$ such that $\bar{q}_{r-1}>q_r^{1-(r-1)\tau}>\sqrt{q_r}$ and $\forall p|\bar{q}_{r-1}$ is good. In particular, $(f_{r-1},\bar{q}_{r-1})$ is admissible and Remark 3.2 applies. (Recall that $q_r<N^{1/3}$.) Hence, we have

$$\Big|\sum_{x=1}^{N}\chi_r(f_{r-1}(x))\Big|<N\bar{q}_{r-1}^{-\frac14}<Nq_r^{-\frac18},$$

and we reach the final bound

$$\begin{aligned}\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| &\lesssim \left(q_r^{-\tau/5}\right)^{1/2^{r-1}}+\left(q_r^{-1/8}\right)^{1/2^{r-1}}\\ &\lesssim q_r^{-\frac{2}{\log\log q_r}\cdot\frac{1}{2^c\log\log q_r}}\\ &= e^{-\frac{\log q_r}{\log\log q_r(\log q_r)^c}}\\ &< e^{-\sqrt{\log q_r}}\end{aligned}$$

□

The proof of Theorem 3' also gives an argument for the following theorem.

Theorem 3" *Assume $q=q_1\dots q_r$ with $(q_i,q_j)=1$ for $i\neq j$, and q_r square free. Factor $\chi=\chi_1\dots\chi_r$, where $\chi_i(\text{mod } q_i)$ is arbitrary for $i<r$, and primitive for $i=r$.*
We further assume

(i). *For all $p|q_r, p>\sqrt{\log q}$.*

(ii). For all i, $q_i<N^{1/3}$.

(iii). $r<c\log\log q$.

Let

$$f(x)=\prod_j(x-b_j)^{c_j},\quad c_1=\pm1,\quad d=\deg f=\sum|c_j|.$$

Suppose that (f,q_r) is admissible *(as defined after the statement of Theorem 3'). Furthermore, assume* (iv). $d = \deg f < \left(\log q_r\right)^{\frac{1}{8}}$.

Then

$$\Big|\sum_{x=1}^{N} \chi(f(x))\Big| < Ne^{-\sqrt{\log q_r}}.$$

Remark 3.3. To modify the proof of Theorem 3', one only needs to multiply $\frac{M^2}{Q}$ by $d^{\omega(Q)}$ in (3.7) and replaced 2^s (respectively, 2^r) by $2^{s-1}d$ (resp. $2^{r-1}d$) in (3.12) (resp. (3.13)). Assumptions (i) and (iii) imply $2^r < p^{1/4}$, while assumptions (i) and (iv) imply $d < p^{1/4}$.

4 Graham-Ringrose for mixed character sums.

The technique used to prove Theorem 1' may be combined with the method of Graham-Ringrose for Theorem 3' to bound short mixed character sums with highly composite modulus (see also [IK] p. 330–334).

Let $q = q_1 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square free, such that (i) and (iii) of Theorem 3' hold .

Let

$$\chi = \chi_1 \cdots \chi_r,$$

where $\chi_i (\text{mod } q_i)$ is arbitrary for $i < r$, and primitive for $i = r$.

Let $I \subset [1, q]$ be an interval of size $N < q$, and let $f(x) = \alpha_d x^d + \cdots + \alpha_0 \in \mathbb{R}[x]$ be an arbitrary polynomial of degree d.

Assuming (ii) of Theorem 3' and an appropriate assumption on d, we establish a bound on

$$\sum_{x \in I} \chi(x) e^{if(x)}. \tag{4.1}$$

The case $f = 0$ corresponds to Theorem 3'. The main idea to bound (4.1) is as follows. First, we repeat part of the proof of Theorem 1 in order to remove the factor $e^{if(x)}$ at the cost of obtaining a character sum with polynomial argument. Next, we invoke Theorem 3" to estimate these sums.

Write $q = q_1 Q_1$ with $Q_1 = q_2 \dots q_r$, and denote $\mathcal{Y}_1 = \chi_2 \dots \chi_r$.

Choose $M \in \mathbb{Z}$ such that

$$M \cdot \max q_i < N, \quad \text{and} \quad M < \sqrt{N}. \tag{4.2}$$

Using shifted product method as in (3.5), we have

$$\sum_{x\in I} \chi(x) e^{if(x)} = \frac{1}{M} \sum_{\substack{x\in I\\ 0\leq y<M}} \chi(x+q_1 y) e^{if(x+q_1 y)} + O(q_1 M), \tag{4.3}$$

$$\begin{aligned} \frac{1}{M}\Big| \sum_{\substack{x\in I\\ 0\leq y<M}} \chi(x+q_1 y) e^{if(x+q_1 y)} \Big| &= \frac{1}{M}\Big| \sum_{\substack{x\in I\\ 0\leq y<M}} \chi_1(x) \mathcal{Y}_1(x+q_1 y) e^{if(x+q_1 y)} \Big| \\ &\leq \frac{1}{M} \sum_{x\in I} \Big| \sum_{0\leq y<M} \mathcal{Y}_1(x+q_1 y) e^{if(x+q_1 y)} \Big|. \end{aligned} \tag{4.4}$$

Next, we write

$$f(x+q_1 y) = f_0(x) + f_1(x) y + \cdots + f_d(x) y^d.$$

Fix $\theta = \theta(q) > 0$ and subdivide $\mathbb{T}^{d+1}$ in cells $U_\alpha = B\big(\xi_\alpha, \frac{\theta}{M^d}\big) \subset \mathbb{T}^{d+1}$.

Denote

$$\Omega_\alpha = \{x \in I : \big(f_0(x), \dots, f_d(x)\big) \in U_\alpha \mod 1\}.$$

Hence, for $x \in \Omega_\alpha$

$$\begin{aligned} f(x+q_1 y) &= \xi_{\alpha,0} + \xi_{\alpha,1} y + \cdots + \xi_{\alpha,d} y^d + O(\theta) \\ e^{if(x+q_1 y)} &= e^{i(\xi_{\alpha,0}+\cdots+\xi_{\alpha,d} y^d)} + O(\theta) \end{aligned} \tag{4.5}$$

The number of cells is

$$\sim \Big(\frac{M^d}{\theta}\Big)^{d+1}. \tag{4.6}$$

Substituting (4.5) in (4.4) gives

$$\begin{aligned} &\frac{1}{M} \sum_{x\in I} \Big| \sum_{0\leq y<M} \mathcal{Y}_1(x+q_1 y) e^{if(x+q_1 y)} \Big| \\ =&\frac{1}{M} \sum_{\alpha} \sum_{x\in\Omega_\alpha} \Big| \sum_{0\leq y\leq M} C_\alpha(y) \mathcal{Y}_1(x+q_1 y) \Big| + O(\theta N), \end{aligned} \tag{4.7}$$

where $|C_\alpha(y)| = 1$.

Next, applying Hölder to the triple sum in (4.7) with $k \in \mathbb{Z}_+$, we have

$$\sum_\alpha \sum_{x\in\Omega_\alpha} \Big| \sum_{0\le y\le M} C_\alpha(y)\mathcal{Y}_1(x+q_1y)\Big| \le N^{1-\frac{1}{2k}} \Big(\sum_\alpha \sum_{x\in I} \Big| \sum_{0\le y\le M} C_\alpha(y)\mathcal{Y}_1(x+q_1y)\Big|^{2k}\Big)^{\frac{1}{2k}}.$$

Therefore, up to an error of $O(\theta N)$, (4.7) is bounded by

$$N\left[\frac{1}{NM^{2k}}\left(\frac{M^d}{\theta}\right)^{d+1} \sum_{0\le y_1,\dots y_{2k}<M} \Big|\sum_{x\in I} \mathcal{Y}_1\Big(\frac{(x+q_1y_1)\cdots(x+q_1y_k)}{(x+q_1y_{k+1})\cdots(x+q_1y_{2k})}\Big)\Big|\right]^{\frac{1}{2k}}$$

$$= N\left(\frac{M^d}{\theta}\right)^{\frac{d+1}{2k}} \left[\frac{1}{NM^{2k}} \sum_{0\le y_1,\dots,y_{2k}<M} \Big|\sum_{x\in I} \mathcal{Y}_1\big(R_{y_1,\dots,y_{2k}}(x)\big)\Big|\right]^{\frac{1}{2k}}, \tag{4.8}$$

where

$$R_{y_1,\dots,y_{2k}}(x) = \frac{(x+q_1y_1)\cdots(x+q_1y_k)}{(x+q_1y_{k+1})\cdots(x+q_1y_{2k})}.$$

To bound the double sum in (4.8), we apply Theorem 3" with $f(x) = R_{y_1,\dots,y_{2k}}(x)$ for those tuplets $(y_1,\dots,y_{2k}) \in \{0,\dots,M-1\}^{2k}$ for which $(R_{y_1,\dots,y_{2k}}, q_r)$ is admissible. For the other tuplets, we use the trivial bound. If $(R_{y_1,\dots,y_{2k}}, q_r)$ is not admissible, then there is a divisor $Q|q_r$, $Q > q_r^\tau$, such that for each $p|Q$, the set $\{\pi_p(y_1),\cdots,\pi_p(y_{2k})\}$ has at most k elements. Here π_p is the natural projection from $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$. We distinguish the tuplets $(y_1,\dots,y_{2k})$ in the following contributions.

(a). *Suppose that there is $p|Q$ with $p > \sqrt{M}$.*

Then the number of p-bad tuplets $(y_1,\dots,y_{2k})$ is bounded by

$$\binom{2k}{k} M^k k^k \Big(1+\frac{M}{p}\Big)^k < (4k)^k M^{\frac{3}{2}k},$$

and summing over the prime divisors of q_r gives

$$\omega(q_r)(4k)^k M^{\frac{3}{2}k} < M^{\frac{7}{4}k}, \tag{4.9}$$

provided

$$k < M^{\frac{1}{5}}, \tag{4.10}$$

and

$$\log q_r < M. \tag{4.11}$$

(b). *Suppose $Q > M$ and $p \le \sqrt{M}$ for each $p|Q$.*

Take $Q_1|Q$ such that $\sqrt{M} < Q_1 < M$. The number of tuplets $(y_1, \dots, y_{2k})$ that are p-bad for each $p|Q_1$ is at most

$$\left(\frac{M}{Q_1}\right)^{2k} \prod_{p|Q_1} \binom{2k}{k} \; p^k \; k^k$$

$$< \left(\frac{M}{Q_1}\right)^{2k} \prod_{p|Q_1} (4kp)^k < \; (ck)^{k\omega(Q_1)} \frac{M^{2k}}{Q_1^k} < \; \frac{M^{2k}}{Q_1^{\frac{k}{3}}} < \; M^{\frac{11}{6}k},$$

provided

$$k < \min_{p|q_r} p^{\frac{1}{3}}. \tag{4.12}$$

Summing over all Q_1 as above gives the contribution

$$M^{\frac{11}{6}k+1} < M^{\frac{15}{8}k}. \tag{4.13}$$

(c). *Suppose $q_r^\tau < Q < M$.*

The number of tuplets $(y_1, \dots, y_{2k})$ that are p-bad for all $p|Q$ is at most $M^{2k}/Q^{\frac{k}{3}}$ and summation over these Q gives the contribution

$$2^{\omega(q_r)} \, \frac{M^{2k}}{Q^{\frac{k}{3}}} < \frac{M^{2k}}{q_r^{\;\frac{1}{4}k\tau}}. \tag{4.14}$$

Hence, in summary, the number of $(y_1, \dots, y_{2k})$ for which $(R_{y_1,\dots,y_{2k}}, q_r)$ is not admissible is at most

$$M^{2k}(M^{-\frac{k}{8}} + q_r^{-\frac{1}{4}k\tau}).$$

From (4.3)-(4.4) and (4.7)-(4.8) we obtain the estimate

$$\sum_{x\in I} \chi(x) e^{if(x)} < N \left(\frac{M^d}{\theta}\right)^{\frac{d+1}{2k}} \left[M^{-\frac{k}{8}} + q_r^{-\frac{1}{4}k\tau} + e^{-\sqrt{\log q_r}}\ \right]^{\frac{1}{2k}}$$

using Theorem 3" for the contribution of *good* tuplets $(y_1, \dots, y_{2k})$. Here we need to assume

$$2k < \big(\log q_r\big)^{\frac{1}{8}}, \tag{4.15}$$

which also implies (4.10) and (4.12), under assumption (i) and if (4.11) holds.

Take $\theta = \frac{1}{M}$, $k = 50d^2$, assuming

$$d < \frac{1}{10}\Big(\log q_r\Big)^{\frac{1}{16}}, \tag{4.16}$$

(which implies (4.15),) then

$$\begin{aligned}\sum_{x\in I} \chi(x) e^{if(x)} &< NM^{\frac{(d+1)^2}{2k}} \Big(M^{-\frac{1}{16}} + e^{-\frac{\sqrt{\log q_r}}{2k}}\Big) \\ &< N\bigg(M^{-\frac{1}{20}} + \bigg(\frac{M^{(d+1)^2}}{e^{\sqrt{\log q_r}}}\bigg)^{\frac{1}{100d^2}}\bigg).\end{aligned}$$

Choose

$$M = \Big[\exp\Big(\frac{\sqrt{\log q_r}}{2(d+1)^2}\Big)\Big].$$

(So (4.11) is also satisfied.) We have

$$\sum_{x\in I} \chi(x) e^{if(x)} < Ne^{-\frac{\sqrt{\log q_r}}{200d^2}}.$$

Thus we proved

Theorem 4. *Assume $q = q_1 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square free. Factor $\chi = \chi_1 \dots \chi_r$, where $\chi_i (\mathrm{mod}\ q_i)$ is arbitrary for $i < r$, and primitive for $i = r$.*

We further assume

(i). *For all $p | q_r, p > \sqrt{\log q}$.*

(ii). *For all i, $q_i < N^{1/3}$.*

(iii). *$r < c \log\log q$.*

Let $f(x) \in \mathbb{R}[x]$ be an arbitrary polynomial of degree d. Assume

$$d < \frac{1}{10}\Big(\log q_r\Big)^{\frac{1}{16}}.$$

Then

$$\Big|\sum_{n\in I} e^{if(n)}\chi(n)\Big| < CNe^{-\frac{\sqrt{\log q_r}}{200d^2}}, \tag{4.17}$$

where I is an interval of size N.

Combined with Postnikov (as in the proof of Theorem 2), Theorem 4 then implies

Theorem 4' *Suppose $q = q_0 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square free. Assume $\bar{q}_0 | q_0$ and $q_0 | (\bar{q}_0)^m$ for some $m \in \mathbb{Z}_+$, and*

$$m < \frac{1}{20}\Big(\log q_r\Big)^{\frac{1}{16}}.$$

Factor $\chi = \chi_0 \dots \chi_r$, where $\chi_i (\mathrm{mod}\ q_i)$ is arbitrary for $i < r$, and primitive for $i = r$.

We further assume

(i). *For all $p | q_r, p > \sqrt{\log q}$.*

(ii). *For all i, $q_i < \big(N/\bar{q}_0\big)^{1/3}$.*

(iii). *$r < c \log\log q$.*

Then

$$\Big|\sum_{n\in I} \chi(n)\Big| < CNe^{-\frac{\sqrt{\log q_r}}{800m^2}}, \tag{4.18}$$

where I is an interval of size N.

Note that for Theorem 4' to provide a nontrivial estimate, we should assume at least

$$r \lesssim \log\log q_r$$

and

$$\log m \lesssim \log\log q_r.$$

5 The main theorem.

Theorem 4' as a consequence of Theorem 4 was stated mainly for expository reason. (cf. Proposition 7.) Our goal is to develop this approach further in order to prove the following stronger result.

Theorem 5. *Assume N satisfies*

$$q > N > \max_{p|q} p^{10^3} \tag{5.1}$$

and

$$\log N > (\log q)^{1-c} + C \log \left(2 \frac{\log q}{\log q'} \right) \frac{\log q'}{\log \log q} \ , \tag{5.2}$$

where $C, c > 0$ are some constants, and $q' = \prod_{p|q} p$.

Let χ be primitive (mod q) *and I an interval of size N. Then*

$$\Big| \sum_{x \in I} \chi(x) \Big| < N e^{-\sqrt{\log N}}. \tag{5.3}$$

We will prove Theorem 5 in the next section. In this section, we will set up the proof and discuss the implication of assumption (5.2).

Claim. We may assume the following

(1.) $q' > N^{\frac{1}{100}}$

(2.) $q = Q\, q_r = Q_1 \cdots Q_{r-1}\, q_r$, where $(Q_i, Q_j) = (Q_i, q_r) = 1$, (5.4)

$$r = 1 + 10 \left[\frac{\log Q'}{\log N} \right], \tag{5.5}$$

and

$$q_r = q_0^m, \ \ q_0 \text{ square free} \tag{5.6}$$

with

$$e^{(\log N)^{\frac{3}{4}}} < q_0 < N^{\frac{1}{10}}, \tag{5.7}$$

$$m \le (\log N)^{3\kappa}, \tag{5.8}$$

where $\kappa > 0$ a sufficiently small constant (e.g. $\sim 10^{-3}$). Also, the core of Q_s satisfies

$$Q_s' < N^{\frac{1}{5}} \ \text{ for } s = 1, \dots, r-1. \tag{5.9}$$

(3.) There exist $q_1, \cdots, q_{r-1}$, $(q_i, q_j) = (q_i, q_r) = 1$,

$$\max_i q_i < N^{1/2}, \tag{5.10}$$

such that

$$q = Q_1 \cdots Q_{r-1} q_r \mid q_1^{m_1} \cdots q_{r-1}^{m_{r-1}} q_r, \tag{5.11}$$

with

$$m_s = 10\left[\frac{\log Q_s}{\log N}\right]. \tag{5.12}$$

Proof of Claim.

The validity of Assumption (1) follows from Theorem 12.16 in [IK], which gives a bound

$$\Big|\sum_{x\in I} \chi(x)\Big| < C^{r \log\log r} N^{1-\frac{c}{r^2 \log r}} \tag{5.13}$$

with $r = \frac{\log q}{log N}$, assuming that $q'^{100} < N$. This gives a nontrivial result provided $\log N \gtrsim (\log q)^{\frac{3}{4}+\epsilon}$.

To see Assumption (2), we first note that

$$\prod_{\nu_p > (\log N)^{3\kappa}} p < q^{(\log N)^{-3\kappa}} < e^{(\log N)^{1-\kappa}} < q'^{\frac{1}{100}}, \tag{5.14}$$

where ν_p is the exponent of p in the prime factorization of q.

From

$$\prod_{m=1}^{(\log N)^{3\kappa}} \Big(\prod_{\nu_p = m} p\Big) > q'^{\frac{99}{100}},$$

there exists $m \leq (\log N)^{3\kappa}$ such that

$$\prod_{\nu_p = m} p > (q')^{\frac{1}{2}(\log N)^{-3\kappa}} > e^{\frac{1}{200}(\log N)^{1-3\kappa}} > e^{(\log N)^{\frac{3}{4}}}.$$

Therefore, there exists q_r satisfies (5.6)-(5.8).

Write $q = Q\, q_r$, and

$$Q = \prod p_i^{\nu_i}, \quad \text{where } \upsilon_i := \nu_{pi} \text{ and } \nu_1 \geq \nu_2 \geq \cdots.$$

Let $Q' = \prod_{\nu_i \geq 1} p_i$ and factor

$$Q' = Q_1' \cdots Q_{r-1}' \text{ such that } Q_s' < N^{\frac{1}{5}} \text{ and } r = 1 + 10\left[\frac{\log Q'}{\log N}\right].$$

For each s, define $Q_s = \prod_{p|Q'_s} p^{\nu_p}$ and $q_s = \prod_{p|Q'_s} p^{\bar{\nu}_p}$ as follows

$$\bar{\nu}_p = \begin{cases} \left[\frac{\nu_p}{m_s}\right] + 1, & \text{if } \nu_p > m_s \\ 1, & \text{otherwise} \end{cases} \tag{5.15}$$

Denote

$$m_s = 10 \frac{\log Q_s}{\log N}.$$

It follows that $Q_s|(q_s)^{m_s}$ and $q_s < Q'_s Q_s^{\frac{2}{m_s}} < N^{\frac{1}{2}}$, which are (5.10)-(5.11).

Remark 5.1. Assumption (5.2) can be reformulated as

$$\left(3\,\frac{\log q}{\log q' N}\right)^{10^{\frac{\log Nq'}{\log N}}} < (\log N)^c. \tag{5.16}$$

Remark 5.2. Using (5.4), (5.16) and the inequality of arithmetic and geometric means, one can show that

$$\prod_{i=1}^{r-1} m_i < \left(\log q_0\right)^{\frac{1}{75}}. \tag{5.17}$$

Remark 5.3. It is easy to check that (5.2) and (5.7) imply

$$r < 10^{-3} \log\log q_0. \tag{5.18}$$

Remark 5.4. If $\log q' \leq \log N$, (5.16) becomes

$$\log N > (\log q)^{1-c},$$

which is similar to Theorem 12 in [IK].

Remark 5.5. If $q = q'$ (i.e. q is square free), condition (5.16) becomes

$$\frac{\log q}{\log\log q} < c \log N.$$

This is slightly better than Corollary 12.15 in [IK] and essentially optimal in view of the Graham-Ringrose argument.

6 The proof of Theorem 5.

The proof will use the technique from the previous sections. The following lemma is the technical part of the inductive step.

Lemma 6. *Assume*

(a). $q = q_1^m q'$, *where* $q' = q'' q_r$, *with* q_1, q'', q_r *mutually coprime.*

(b). $\chi = \chi_1 \chi'$, *with* $\chi_1 (\text{mod } q_1^m)$ *and* $\chi' (\text{mod } q')$.

(c). $f(x) = \prod_{\alpha=1}^{\beta} (x - a_\alpha)^{d_\alpha}$, $d = \sum |d_\alpha|$, *with* $a_\alpha \in \mathbb{Z}$ *distinct and* $d_\alpha \in \mathbb{Z} \backslash \{0\}$.

(d). $\bar{q} | q_r$ *such that for each* $p | \bar{q}$, $p > \sqrt{\log q}$ *and* f mod p *satisfies* $(*)$ (*i.e. has a simple zero or a simple pole*).

(e). I *an interval of length* N, $q_1^2 < N < q$, $1440 \cdot m^2 d < (\log N)^{\frac{1}{10}}$.

(f). $M \in \mathbb{Z}$, $\log N + \log \bar{q} < M < N^{\frac{1}{10}}$, $M < \bar{q}^{\,\tau}$.

Then

$$\frac{1}{N} \Big| \sum_{x \in I} \chi\big(f(x)\big) \Big| < M^{-1/12} + M^{\frac{1}{60}} \Big| \frac{1}{N} \sum_{x \in I} \chi'\big(f_1(x)\big) \Big|^{\frac{1}{60m^2}}, \tag{6.1}$$

where $f_1(x)$ *is of the form*

$$f_1(x) = \frac{\prod_{\nu=1}^{k} f(x + q_1 t_\nu)}{\prod_{\nu=k+1}^{2k} f(x + q_1 t_\nu)} = \prod_{\alpha'=1}^{\beta'} (x - b_{\alpha'})^{d_{\alpha'}} \tag{6.2}$$

with $b_{\alpha'}, d_{\alpha'} \in \mathbb{Z}$, $2k = 60m^2$ *and*

$$d_1 := \sum | \, d_{\alpha'} \, | \le 60 \; d \; m^2. \tag{6.3}$$

Furthermore, $(f_1, \bar{q})$ *is admissible.*

Proof. Take $t \in [1, M]$. Clearly,

$$\chi\big(f(x + tq_1)\big) = \chi_1\big(f(x)\big) \chi_1 \bigg(1 + \frac{f(x + tq_1) - f(x)}{f(x)}\bigg) \chi'\big(f(x + tq_1)\big). \tag{6.4}$$

Hence, as in the proof of Theorem 2,

$$\chi\big(f(x+tq_1)\big) = \chi_1\big(f(x)\big)\chi'\big(f(x+tq_1)\big)e_{q_1^m}\Big(\sum_{j=1}^{m-1} Q_j(x)\; q_1^j\; t^j\Big), \qquad (6.5)$$

where

$$Q_j(x) = \frac{1}{j!}\frac{d^j}{dt^j}\Big\{F\Big(\frac{f(x+t)-f(x)}{f(x)}\Big)\Big\}\Big|_{t=0} \qquad (6.6)$$

with

$$F(x) = \sum_{s=1}^{2m}(-1)^{s-1}\frac{1}{s}x^s \qquad \text{(up to a factor).} \qquad (6.7)$$

By the same technique as used in the proof of Theorem 4 (See (4.3)-(4.8)), after averaging and summing over $t \in M$ and $x \in I$, we remove the last factor in (6.5). Thus, our goal is to show that after $\underline{t} = (t_1, \cdots, t_{2k}) \in [1, M]^{2k}$ is chosen for (6.2) such that f_1 maximizes the character sum in (6.1) among all admissible $(f_1, \bar{q})$, the first term in (6.1) accounts for those $\underline{t}$ for which f_1 is not $\bar{q}$-admissible. The zeros or poles of $f_1(x)$ are of the form

$$b_{\alpha'} = a_\alpha - t_\nu q_1 \;\text{ with } t_\nu \in [1, M]. \qquad (6.8)$$

Here, while applying Hölder, we take $k \in \mathbb{Z}^+$ satisfying

$$48kd < \big(\log N\big)^{\frac{1}{10}} \;\text{ and } k > 30 \qquad (6.9)$$

To count the set of bad $\underline{t}$, we fix $p|\bar{q}$. By assumption on f_1, we may also assume $d_1 = 1$ and $a_1 \neq a_\alpha \pmod p$ for any $\alpha > 1$. Recalling (6.8), assume that none of the $a_1 - t_\nu q_1, 1 \le \nu \le 2k$, is simple $\pmod p$. This means that for each ν there is a pair $(\alpha(\nu), \sigma(\nu))$ in $\{1, \ldots, \beta\} \times \{1, \ldots, 2k\}$ such that $\alpha(\nu) \neq 1$, $\sigma(\nu) \neq \nu$ and

$$a_1 - t_\nu q_1 \equiv a_{\alpha(\nu)} - t_{\sigma(\nu)} q_1 \pmod p. \qquad (6.10)$$

The important point is that $\sigma(\nu) \neq \nu$ for all ν, by assumption on a_1. One may therefore obtain a subset $S \subset \{1, \ldots, 2k\}$ with $|S| = k$ such that there exists $S_1 \subset S$ with $|S_1| = \frac{k}{2}$ and

$$S_1 = \{\nu \in S : \sigma(\nu) \notin S_1\} \qquad (6.11)$$

(The existence of S and S_1 satisfying this property is justified in Fact 6.1 following the proof of this lemma.)

Specifying the values of $t_{\nu'}$ for those $\nu' \in \mathcal{K} \setminus S_1$, equations (6.10) will determine the remaining values, after specification of $\alpha(\nu)$ and $\sigma(\nu)$. An easy count shows that

$$\begin{aligned} &\left|\{\pi_p(\underline{t}) : \ f_1(\text{mod } p) \ \text{ does not satisfy } (*) \ \}\right| \\ \leq &\binom{2k}{k} \binom{k}{\frac{k}{2}} \left(\frac{3}{2}\, k\right)^{\frac{k}{2}} \left(\frac{\beta}{2}\right)^{\frac{k}{2}} \big(M \wedge p\big)^{\frac{3k}{2}} < (48kd)^{\frac{k}{2}} \big(M \wedge p\big)^{\frac{3k}{2}}. \end{aligned} \tag{6.12}$$

The first factor counts the number of sets S, the second the number of sets S_1, and the third and the forth the numbers of maps $\sigma|_{S_1}$ and $\alpha|_{S_1}$.

Applying assumptions (d)-(f) to (6.12), we obtain

$$\left|\{\pi_p(\underline{t}) : \ f_1(\text{mod } p) \ \text{ does not satisfy } (*) \ \}\right| < \big(M \wedge p\big)^{\frac{8}{5}k}. \tag{6.13}$$

If $(f_1, \bar{q})$ is not admissible, there is some $Q|\bar{q}$, $Q > q_r^\tau > \bar{q}^{\,\tau}$ such that for each $p|Q$, f_1 is p-bad. As in the proof of Theorem 4, we distinguish several cases.

(a). *There is* $p|Q$ *with* $p > M$.

Hence, $\left|\{\underline{t} \in [1, M]^{2k} : f_1 \text{ is } p\text{-bad } \}\right| < M^{\frac{8}{5}k}$ and summing over p gives the contribution $M^{\frac{8}{5}k} \log \bar{q}$.

(a'). $\sqrt{M} < \max\limits_{p|Q} p < M$.

Then

$$\begin{aligned} &\left|\{\underline{t} \in [1, M]^{2k} : f_1 \text{ is } p\text{-bad } \}\right| \\ \leq &\Big(\frac{M}{p} + 1\Big)^{2k} \left|\{\pi_p(\underline{t}) : f_1 \text{ is } p\text{-bad } \}\right| \\ \leq &\Big(\frac{M}{p} + 1\Big)^{2k} p^{\frac{8}{5}k} < M^{2k} \Big(\frac{p}{32}\Big)^{-\frac{2}{5}k} < (4M)^{\frac{9}{5}k}. \end{aligned}$$

Summing over p gives the contribution $(4M)^{\frac{9}{5}k} \log \bar{q}$.

(b). $\max\limits_{p|Q} p \leq \sqrt{M}$ *and* $Q > M$.

Take $Q_1|Q$ such that $\sqrt{M} < Q_1 < M$. Then

$$\begin{aligned} &\big|\{\underline{t} \in [1, M]^{2k} : f_1 \text{ is } p\text{-bad for each } p|Q_1\}\big| \\ \leq &\Big(\frac{M}{Q_1} + 1\Big)^{2k} \big|\{\pi_{Q_1}(\underline{t}) : f_1 \text{ is } p\text{-bad for each } p|Q_1\}\big| \\ \leq &\Big(\frac{M}{Q_1} + 1\Big)^{2k} \prod_{p|Q_1} p^{\frac{8}{5}k} < M^{2k}\Big(\frac{Q_1}{32}\Big)^{-\frac{1}{5}k} < (4M)^{\frac{9}{5}k}. \end{aligned}$$

Summing over Q_1 gives the contribution $(4M)^{\frac{9}{5}k+1}$.

Summing up cases (a)-(b) and recalling assumption (f), we conclude that

$$\begin{aligned} &\big|\{\underline{t} \in [1, M]^{2k} : (f_1, \bar{q}) \text{ is not admissible }\}\big| \\ < &M^{2k}\big(M^{-\frac{k}{6}} + \bar{q}^{\,\frac{-\tau k}{5}}\big) \end{aligned} \tag{6.14}$$

Taking $d = m - 1$ in (4.8), by assumption (f), we show that

$$\begin{aligned} &\frac{1}{N}\Big|\sum_{x\in I} \chi\big(f(x)\big)\Big| \\ < &O(\theta) + O\Big(\frac{q_1 M}{N}\Big) + \Big[M^{-\frac{k}{6}} + \Big(\frac{M^{m-1}}{\theta}\Big)^m \frac{1}{N}\Big|\sum_{x\in I} \chi'\big(f_1(x)\big)\Big|\Big]^{\frac{1}{2k}}. \end{aligned} \tag{6.15}$$

We obtain (6.1) by letting $\theta = \frac{1}{M}$ in (6.15). □

Fact 6.1. *Let $\mathcal{K} = \{1, \cdots, 2k\}$ and $\sigma : \mathcal{K} \to \mathcal{K}$ be a function such that $\sigma(\nu) \neq \nu$ for all $\nu \in \mathcal{K}$. Then there exist subsets $S_1 \subset S \subset \mathcal{K}$ with $|S_1| = \frac{k}{2}$, $|S| = k$ and $\sigma(\nu) \notin S_1$ for any $\nu \in S_1$.*

Proof. Since the subset of elements of $\mathcal{K}$ with more than one pre-image of σ has size $\leq k$, there exist $S \subset \mathcal{K}$ with $|S| = k$, and every $\nu \in S$ has at most one pre-image. Therefore, σ^{-1} makes sense on S. To construct $S_1 \subset S$, we choose ν_i for S_1 inductively, such that $\nu_i \notin \{\nu_1, \ldots, \nu_{i-1}, \sigma(\nu_1), \ldots, \sigma(\nu_{i-1}), \sigma^{-1}(\nu_1), \ldots, \sigma^{-1}(\nu_{i-1})\}$ and $\sigma(\nu_i) \notin S_1$. □

Proof of Theorem 5.

Choose a sequence $M_1 < M_2 < \cdots < M_{r-1}$ of M values and iterate (6.1) in Lemma 6.

Since

$$\prod_{p<\sqrt{\log q}} p < e^{\sqrt{\log q}},$$

we use trivial bound for small p and we may assume Assumption (d). In order to satisfy Assumption (e), we assume

$$1440 \cdot 60^{r-1} \prod_{i=1}^{r} (m_i^2) < \big(\log N\big)^{\frac{1}{10}}, \tag{6.16}$$

which follows from (5.17) and (5.18).

By (6.1) and iteration, $\frac{1}{N}\big|\sum_{x=1}^{N} \chi(x)\big|$ is bounded by

$$\begin{aligned} M_1^{-\frac{1}{12}} + M_1^{\frac{1}{60}} M_2^{-\frac{1}{12\cdot 60 m_1^2}} + M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} M_3^{-\frac{1}{12\cdot 60^2 m_1^2 m_2^2}} + \cdots \\ + M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} \cdots M_{r-2}^{\frac{1}{60^{r-2} m_1^2 \cdots m_{r-3}^2}} M_{r-1}^{-\frac{1}{12\cdot 60^{r-2} m_1^2 \cdots m_{r-2}^2}} \\ + M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} \cdots M_{r-1}^{\frac{1}{60^{r-1} m_1^2 \cdots m_{r-2}^2}} \mathcal{S}^{\frac{1}{60^{r-1} m_1^2 \cdots m_{r-1}^2}}, \end{aligned} \tag{6.17}$$

where $\mathcal{S}$ is of the form

$$\mathcal{S} = \frac{1}{N}\Big|\sum_{x=1}^{N} \chi_r(g(x))\Big|, \tag{6.18}$$

with χ_r primitive modulo q_r, and

$$g(x) = \prod_{\alpha=1}^{\beta} (x-a_\alpha)^{d_\alpha}, a_\alpha, d_\alpha \in \mathbb{Z},$$

$$d = \sum \mid d_\alpha \mid < 60^r m_1^2 \dots m_r^2, \tag{6.19}$$

and $(g, \bar{q})$ admissible for some $\bar{q}|q_r$, $\bar{q} > \sqrt{q_r}$.

Take M_s, for $s = 1, \cdots, r-1$ such that

$$\begin{aligned} M_1^{-\frac{1}{12}} &= M^{-1} \\ M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} \cdots M_{s-1}^{\frac{1}{60^{s-1} m_1^2 \cdots m_{s-2}^2}} M_s^{-\frac{1}{12\cdot 60^{s-1} m_1^2 \cdots m_{s-1}^2}} &= M_1^{-\frac{1}{12}} \end{aligned} \tag{6.20}$$

to ensure that each of the $r-1$ fist terms in (6.17) is bounded by $\frac{1}{M}$.

One checks recursively that

$$M_s < M^{6^{s-1}\cdot 12^s m_1^2 \cdots m_{s-1}^2} \tag{6.21}$$

and hence (6.17) implies

$$\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| < \frac{r-1}{M} + M^{(\frac{6}{5})^{r-1}-1}\mathcal{S}^{\frac{1}{60^{r-1}m_1^2\cdots m_{r-1}^2}}. \tag{6.22}$$

In order to satisfy the last condition in Assumption (f) of Lemma 6, we impose

$$M^{(6\cdot 12)^r m_1^2\cdots m_{r-1}^2} < q_r^{\tau} = q_r^{\frac{10}{\log\log q_r}}. \tag{6.23}$$

The above holds, if we take

$$M = e^{(\log q_r)^{9/10}}, \tag{6.24}$$

and assume

$$\sum_{i=1}^{r-1}\log m_i < \frac{1}{40}\log\log q_r. \tag{6.25}$$

(Clearly, this follows from (5.17).)

We will prove the theorem by distinguishing two cases in the next section.

7 The two cases.

To finish the proof of Theorem 5, we need to bound $\mathcal{S}$ in (6.22).

Case 1. $m=1$.

Since $(g,\bar{q})$ is admissible and $\bar{q}$ is square free, $\mathcal{S}$ may be bounded by Remark 3.2.

$$\mathcal{S} < \bar{q}^{\,-\frac{3}{10}}q_r^{\frac{3}{10}\tau} < q_r^{-\frac{1}{7}}, \tag{7.1}$$

and by (6.22)

$$\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| < \frac{r-1}{M} + M^{(\frac{6}{5})^{r-1}-1}q_r^{-\frac{1}{7\cdot 60^{r-1}m_1^2\cdots m_{r-1}^2}} < \frac{r}{M}. \tag{7.2}$$

The last inequality is by Remark 5.2 and (6.23).

Now we obtain (5.3) by combining (6.24), (7.2) and (5.18). □

We state the above case as a proposition for its own interest.

Proposition 7. *Assume* $q = q_1^{m_1} \dots q_{r-1}^{m_{r-1}} q_r$ *with* $(q_i, q_j) = 1$ *for* $i \neq j$, q_r *square free and*

$$\prod_{i=1}^{r-1} m_i < \Big(\log q_r\Big)^{\frac{1}{75}}. \tag{7.3}$$

Factor $\chi = \chi_1 \dots \chi_r$, *where* $\chi_i (\bmod\ q_i^{m_i})$ *is arbitrary for* $i < r$, *and primitive for* $i = r$.

We further assume

(i). *For all* $p | q_r, p > \sqrt{\log q}$.

(ii). *For all* i, $q_i^2 < N < q$.

(iii). $r < 10^{-3} \log\log q_r$.

Then

$$\Big| \sum_{x \in I} \chi(x) \Big| < N e^{-(\log q_r)^{4/5}}, \tag{7.4}$$

where I *is an interval of size* N.

Case 2. $m > 1$.

In this situation, we follow the analysis in the proof of Lemma 6. (Particularly, see (6.4)-(6.7).) To bound $\mathcal{S}$ in (6.17), We will use Postnikov and Vinogradov rather than Weil. Recall

$$\mathcal{S} = \frac{1}{N} \Big| \sum_{n=1}^{N} \chi_r(f(n)) \Big|,$$

with χ_r primitive modulo q_r, and

$$f(x) = \prod_{\alpha=1}^{\beta} (x - a_\alpha)^{d_\alpha} \quad \text{with } d =< 60^r m_1^2 \dots m_r^2.$$

Write $n \in [1, N]$ as $n = x + tq_0$, with $1 \le x \le q_0$ and $1 \le t \le \frac{N}{q_0}$. Then as in (6.4) and (6.6),

$$\begin{aligned} N \cdot \mathcal{S} &= \sum_{x=1}^{q_0} \sum_{t=1}^{N/q_0} \chi_r\big(f(x)\big) e_{q_0^m}\Big(\sum_{j=1}^{m-1} Q_j(x) q_0^j t^j\Big) \\ &\le \sum_{x=1}^{q_0} \Big| \sum_{t=1}^{N/q_0} e_{q_0^m}\Big(\sum_{j=1}^{m-1} Q_j(x) q_0^j t^j\Big)\Big|. \end{aligned} \tag{7.5}$$

We assume that $f(x)$ satisfies the following property.

For each prime divisor p of q_0, there is α such that $|d_\alpha| = 1$ and $\prod_{\beta\neq\alpha}(a_\alpha - a_\beta)$ relative prime to p.

This will provide some information on the coefficients Q_j in (6.5). Assume $\alpha = 1$ in $f(x)$ and $a_\alpha = 0$ (which we may). Thus 0 is a simple zero or pole of f; replacing f by $\frac{1}{f}$ (which we may by replacement of χ by $\bar{\chi}$), we can assume

$$f(x) = xg(x) = x \prod_{a_\alpha \neq 0} (x - a_\alpha)^{d_\alpha} \qquad \mathrm{mod}\ p \tag{7.6}$$

with $g(0)$ defined and non-vanishing (mod p).

From (6.6), (6.7), and (7.6), we have

$$j! Q_j(x) = \sum_s (-1)^{s-1} \frac{1}{s(xg(x))^s} \frac{d^j}{dt^j}\big[\big((x+t)g(x+t) - xg(x)\big)^s\big]\Big|_{t=0}. \tag{7.7}$$

Clearly only the terms $s \le j$ contribute and Q_j has a pole at 0 of order j,

$$C \cdot Q_j(x) = \frac{1}{x^j} + \frac{A_j(x)}{B_j(x)} \tag{7.8}$$

with $A_j(x), B_j(x) \in \mathbb{Z}[X]$ and $B_j(x) = x^k \hat{B}_j(x), k < j, \hat{B}_j(0) \neq 0$ and hence

$$\hat{B}_j(0) \neq 0 (\mathrm{mod}\ p) \tag{7.9}$$

since $B_j(x)$ is a product of monomials of the form $x - a_\alpha$ and $a_\alpha \neq 0(\mathrm{mod}\ p)$ for $\alpha \neq 1$. Thus

$$C \cdot Q_j(x) = \frac{P_j(x)}{x^j \hat{B}_j(x)} \tag{7.10}$$

where $P_j(x) \in \mathbb{Z}[X]$ is of degree at most dj, $P_j(0) \neq 0 \pmod p$. It follows that

$$\big|\{1 \leq x \leq p : Q_j(x) \equiv 0 \pmod p\}\big| \leq dj. \tag{7.11}$$

and

$$\big|\{1 \leq x \leq q_0 : Q_j(x) \equiv 0 \pmod{\bar{q}_0}\}\big| \leq (dj)^{\omega(\bar{q}_0)} \frac{q_0}{\bar{q}_0}. \tag{7.12}$$

whenever $\bar{q}_0 | q_0$. Taking $j = m-1$ and fixing x, we will apply Vinogradov's lemma ([Ga], Lemma 4) to bound

$$\Big| \sum_{t=1}^{N/q_0} e_{q_0^m} \Big(\sum_{j=1}^{m-1} Q_j(x) q_0^j t^j \Big) \Big|.$$

Lemma (Vinogradov). *Let $f(t) = a_1 t + \cdots + a_k t^k \in \mathbb{R}[t], k \geq 2$ and $P \in \mathbb{Z}_+$ large.*
Assume a_k rational, $a_k = \frac{a}{b}, (a,b) = 1$ such that

$$2 < P \leq b \leq P^{k-1} \tag{7.13}$$

Then

$$\Big| \sum_{n \in I} e(f(n)) \Big| < C^{k (\log k)^2} P^{1 - \frac{c}{k^2 \log k}} \tag{7.14}$$

for any interval I of size P (c, C are constants).

Write $Q_{m-1}(x) \equiv \bar{q}_0 \bar{a} \in \mathbb{Z} (\mathrm{mod}\ q_0^{m_0})$, $\bar{q}_0 | q_0$ and $(\bar{a}, q_0) = 1$.

If $\bar{q}_0 \leq \sqrt{q_0}$, then the coefficient of t^{m-1} in (7.5) is $a_{m-1} = \frac{Q_{m-1}(x)}{q_0^m} q_0^{m-1} = \frac{\bar{a}}{\bar{\bar{q}}_0}$, with $\bar{\bar{q}}_0 = \frac{q_0}{\bar{q}_0} > \sqrt{q_0}$.

Applying (7.14) with $P = q_0$ gives

$$\Big| \sum_{t=1}^{N/q_0} e_{q_0^m} \Big(\sum_{j=1}^{m-1} Q_j(x) q_0^j t^j \Big) \Big| < N\ C^{m (\log m)^2} q_0^{-\frac{c}{m^2 (\log m)}}. \tag{7.15}$$

It remains to estimate the contribution of those $1 \leq x \leq q_0$ such that $Q_j(x) \equiv 0$ in $\mathbb{Z}/\bar{q}_0\mathbb{Z}$ for some $\bar{q}_0 > \sqrt{q_0}$. This number is by (7.12) at most

$$\sum_{\substack{\bar{q}_0 | q_0 \\ \bar{q}_0 > \sqrt{q_0}}} (dm)^{\omega(\bar{q}_0)} \frac{q_0}{\bar{q}_0} < 2^{\omega(q_0)} (dm)^{\omega(q_0)} \sqrt{q_0} < (2dm)^{\frac{2 \log q_0}{\log \log N}} \sqrt{q_0} \tag{7.16}$$

since all prime divisors of q_0 are at least $(\log N)^{\frac{1}{2}}$. Note that the degree d of $f(x)$ is bounded by (6.19). Applying (5.8) and (5.17), we have

$$dm < 60^r \big(\log q_r\big)^{\frac{2}{75}} \big(\log N\big)^{3\kappa} < \big(\log N\big)^{15\kappa}. \tag{7.17}$$

In particular, (7.17) will ensure that (7.16) is bounded by $q_0^{3/4}$ and hence

$$\Big|\sum_{x=1}^{N} \chi(f(x))\Big| < C^{m(\log m)^2} q_0^{-\frac{c}{m^2(\log m)}} N. \tag{7.18}$$

This gives a bound on $\mathcal{S}$ in (6.22). $\square$

8 Applications.

Following Goldmakher's argument [G] (based on work of Granville and Soundararajan [GS]), and applying Theorem 5 instead of the character sum estimates developed by Graham-Ringrose [GR] and Iwaniec [I], we obtain the following improvement of the Pólya and Vinogradov bound.

Theorem 8. Let χ be a multiplicative character with modulus q, and let p be the largest prime divisor of q, $q' = \prod_{p|q} p$ and $K = \frac{\log q}{\log q'}$. Let $M = (\log q)^{\frac{9}{10}} + (\log 2K)\frac{\log q'}{\log\log q'} + \log p$. Then

$$\Big|\sum_{n<x} \chi(n)\Big| \ll \sqrt{q}\sqrt{\log q}\sqrt{M}. \tag{8.1}$$

Remark 8.1. If q is square free, then the bound in (8.1) becomes

$$\sqrt{q}\left\{\sqrt{\log q}\sqrt{\log p} + \frac{\log q}{\sqrt{\log\log q}}\right\}.$$

This slightly improves on the corollary to Theorem 1 in Goldmakher's paper [G].

Repeating the argument in deducing Theorem 4 from Theorem 3, we obtain the following mixed character sum estimate from the proof of Theorem 5.

Theorem 9. *Under the assumptions of Theorem 5,*

$$\Big|\sum_{x\in I}\chi(x)e^{if(x)}\Big| < Ne^{-\sqrt{\log N}} \tag{8.2}$$

for $f(x)\in\mathbb{R}[X]$ *of degree at most* $(\log N)^c$.

Corollary 10. *Assume* N *satisfies*

$$q > N > \max_{p|q} p^{10^3}$$

and q *satisfies*

$$\log N > (\log qT)^{1-c} + C\log\Big(2\frac{\log q}{\log q'}\Big)\,\frac{\log q'}{\log\log q}\ . \tag{8.3}$$

Then for χ *non-principal, we have*

$$\Big|\sum_{n\in I}\chi(n)n^{it}\Big| < Ne^{-\sqrt{\log N}} \tag{8.4}$$

Following [Ga] and [I], (See in particular, Lemma 11 in [I]), this implies

Theorem 11. *Let* χ *be a non-principal character* (mod q), p *the largest prime divisor of* q *and* $q' = \prod_{p|q} p$.

Let

$$\theta = c\min\Big(\frac{1}{\log p}, \frac{\log\log q}{(\log q')(\log 2\frac{\log q}{\log q'})}.\frac{1}{(\log qT)^{1-c'}}\Big). \tag{8.5}$$

If $L(s,\chi), s=\rho+it$, *has a zero for* $\rho > 1-\theta, |t| < T$, *it has to be unique, simple and real. Moreover* χ *is real.*

It follows in particular that $\theta\cdot\log QT\to\infty$, if $\frac{\log p}{\log q}\to 0$.

This allows us to state Corollary 12.

Acknowledgement. The author would like to thank I. Shparlinski for helpful comments and the mathematics department of University of California at Berkeley for hospitality.

References

[C1] M.-C. Chang, *An Estimate of Incomplete Mixed Character Sums* , Duke Math. J. 145, No. 3 (2008), 409–442.

[Ga] P.X. Gallagher, *Primes in progressions to prime-power modulus*, Invent. Math. 16 (1972), 191-201.

[Go] L. Goldmakher, *Character sums to smooth moduli are small*, Can J. Math. 62 (2010), 1099.

[GR] S.W. Graham, C.J. Ringrose, *Lower bounds for least quadratic non-residues*, In: Analytic number theory (Allerton Park, IL, 1989), Progr. Math., 85, Birkhauser, Boston, MA, (1990), 269-309.

[GS] A. Granville, K. Soundararajan, *Large Character Sums: Pretentious Characters and the Plya-Vinogradov Theorem*, J. Amer. Math. Soc. 20 (2007), 357-384.

[HB1] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64, no. 2 (1992), 265338.

[HB2] D. R. Heath-Brown, *Siegel zeros and the least prime in an arithmetic progression*, Quart. J. Math. Oxford Ser. (2), 41 (1990), 405-418.

[IK] H. Iwaniec, E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence RI, (2004).

[I] H. Iwaniec, *On zeros of Dirichlets L series*, Invent. Math. 23 (1974), 97-104.

[P] A.G. Postnikov, *On Dirichlet L-series with the character modulus equal to the power of a prime number*, J. Indian Math. Soc. (N.S.) 20 (1956), 217-226.