Large Sieve Inequality for Special Characters to Prime Square Moduli

Liangyi Zhao
United States Military Academy
In 1941, Yuri Vladimirovich Linnik originated the idea of large sieve. It is as follows. A set of real numbers \( \{x_k\} \) is said to be \( \delta \)-spaced modulo 1 if \( x_j - x_k \) is at least \( \delta \) away from any integer, for all \( j \neq k \).

**Theorem 1.** Let \( \{a_n\} \) be an arbitrary sequence of complex numbers, \( \{x_k\} \) be a set of real numbers which is \( \delta \)-spaced modulo 1, and \( M \in \mathbb{Z}, N \in \mathbb{N} \). Then we have

\[
\sum_{k} \left| \sum_{n=M+1}^{M+N} a_n e(x_k n) \right|^2 \ll (\delta^{-1} + N) \sum_{n=M+1}^{M+N} |a_n|^2,
\]

where the implied constant is absolute.
The above inequality is essentially the best possible. This theorem admits a corollary for multiplicative characters.

\[
\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\chi \mod q}^{\star} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2, \tag{1}
\]

where henceforth, \( \sum^{\star} \) runs over primitive characters modulo the specified modulus only which is a vital feature of the theorem.

We aim to have a result of the following kind.

\[
\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\chi \mod q^2}^{'} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll \Delta \sum_{n=M+1}^{M+N} |a_n|^2, \tag{2}
\]

where the \( \sum^{'} \) runs over some special Dirichlet characters, to be specified later.
In all of our investigations, we restrict our attention to prime square moduli only. The result can be generalized, but restricting the prime square moduli gives us great convenience in estimates, *id est* two prime squares are not co-prime if and only if they are the same.

The idea of studying character sums to prime-power moduli was started in a paper by A. G. Postnikov. He gave formulas on the decomposition of groups of characters of powerful moduli. P. X. Gallagher also studied characters of this type. H. Iwaniec expanded the Postnikov-Gallagher idea to composite moduli.
$G = (\mathbb{Z}/q^2\mathbb{Z})^*$ contains the subgroup $H = \{x \in G \mid x \equiv 1 \pmod{q}\}$, which is isomorphic to the additive group $\mathbb{Z}/q\mathbb{Z}$, with the isomorphism given by

$$H \rightarrow \mathbb{Z}/q\mathbb{Z} : x \mapsto \frac{x - 1}{q}.$$ 

Any Dirichlet character $\xi$ on $G$ induces an additive character on $H$. So for any $x \in H$,

$$\xi(x) = e\left[\frac{a(x-1)}{q^2}\right], \text{ for some } a \pmod{q}. \quad (3)$$

If $\xi' \pmod{q^2}$ is another character satisfying (3) with the same $a \pmod{q}$, then $\xi'\xi^{-1}$ is a character on $G$ that is trivial on $H$. Therefore, $\xi' = \xi\chi$ where $\chi$ is induced by a character on $(\mathbb{Z}/q\mathbb{Z})^*$. Let $G_a$ be the set of characters $\xi \pmod{q^2}$ satisfying (3), whose every element is obtained uniquely by multiplying a fixed character $\xi \in G_a$ by a character $\chi$ on $(\mathbb{Z}/q\mathbb{Z})^*$. 
The context in which we shall consider the sum in the left-hand side of (2) is with \( a = 1 \) in (3); \textit{Id est},

\[
\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\xi \in G_1} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2.
\]

The more general case with \( G_a \) is similar to that for \( G_1 \). Also note that the characters being summed are not necessarily primitive, a feature that the classical large sieve inequality, (1), does not possess.

Next, we observe the following.

\[
\frac{q}{\varphi(q)} \sum_{\xi \in G_1} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 = \frac{q}{\varphi(q)} \sum_{n} \sum_{n'} \bar{a}_n a_{n'} \xi(\bar{n}n') \sum_{\chi} \chi(\bar{n}n'),
\]
where $\xi$ is a fixed character in $G_1$ and $\chi$ runs over Dirichlet character of $(\mathbb{Z}/q\mathbb{Z})^*$. The inner-most sum vanishes unless $n \equiv n' \pmod{q}$, in which case it yields $\varphi(q)$ and

$$
\xi(\overline{nn'}) = e \left( \frac{\overline{nn'} - 1}{q} \right) = e \left( \frac{\overline{n}n' - n}{q} \right)
$$

by (3). Note that $\frac{n' - n}{q}$ is an integer. Hence, we have

$$
\frac{q}{\varphi(q)} \sum_{\xi \mod q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 = q \sum_{n} \sum_{n'} a_n a_{n'} e \left( \frac{\overline{nn'} - n}{q} \right),
$$

(4)

where henceforth $\sum_{\xi}^{(1)}$ denotes sum over characters $\xi \in G_1$. 
Trivially estimating the contribution of the above sum gives

$$\frac{q}{\varphi(q)} \sum_{\xi \mod q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 = [q + O(N)] \sum_{\gcd(n,q)=1} |a_n|^2. \quad (5)$$

Estimating thus gives that

$$\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\xi \mod q^2}^{(1)} \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^2 \ll (Q^2 + QN) \sum_n |a_n|^2. \quad (6)$$

Although (5) is obtained trivially, it is an asymptotic formula rather than simply an upper bound. The inequality (6) is of interest when $N \ll Q$. Moreover, in the light of (5), any improvement upon the exponent of $Q$ is not possible and improvement upon this trivial bound has to come from that on $N$. 
Our result is as follows. Throughout, \( q \) runs over prime numbers only.

**Theorem 2 (Zhao).** Suppose \( Q, N \in \mathbb{N}, M \in \mathbb{Z} \) and \( \{a_n\} \) be a sequence of complex numbers. We have

\[
\sum_{q=1}^{Q} \frac{q}{\varphi(q)} \sum_{\xi \text{ mod } q^2}^{(1)} \left. \left| \sum_{n=M+1}^{M+N} a_n \xi(n) \right|^{2} \right. 
\ll Q^\epsilon \left( NQ^2 + N^4Q^2 + N^3Q^{11/8} \right) \sum_{n=M+1}^{M+N} |a_n|^2,
\]

with any \( \epsilon > 0 \) and the implied constant depends on \( \epsilon \) alone.
Theorem 3 (Weil). For any $c \in \mathbb{N}$, $m$ and $n$, we have

$$\left| \sum_{ad \equiv 1 \mod c} e\left( \frac{ma + nd}{c} \right) \right| \leq \left[ \gcd(m, n, c) \right]^{1/2} c^{1/2} \tau(c),$$

where $\tau(c)$ is the divisor function.

**Proof.** This is deduced from the celebrated Riemann hypothesis for curves over finite fields proved by A. Weil.

**Proof.** (Sketch) It suffices to consider $q \in (Q/2, Q]$. The size of th sum resulted from breaking the left-hand side of (7) into dyadic intervals is majorized by $QT(N, Q)$, with

$$T(N, Q) = \sum_{Q/2 < q \leq Q} \frac{1}{\varphi(q)} \sum_{1}^{(1)} \sum_{n=M+1}^{M+N} a_n \xi(n) \left| \sum_{\xi \mod q^2} \right|^2.$$
It is said that an analytic number theorist is someone who is good at using Cauchy’s inequality. Hence after expanding applying Cauchy’s inequality twice, we get

\[ T^4(N, Q) \leq \left( \sum_n |a_n|^2 \right)^4 Q \sum_{q} \sum_{q_1} \sum_{q_2} \sum_{l_1} \sum_{l_2} \sum_{l'} \sum_{l''} \left\{ \sum_n \right\}, \quad (8) \]

where the inner-most sum is

\[ \sum_n e \left[ \frac{(n - l'q)l_1}{q_1} - \frac{nl'}{q} - \frac{(n - l''q)l_2}{q_2} + \frac{nl''}{q} \right], \]

which is an incomplete Kloosterman type sum and may be completed by Fourier techniques.
It suffices to estimate a sum of the following form

\[
\sum_{N \leq n \leq N_1} e \left[ \frac{(n - l'q)l_1}{q_1} - \frac{n}{q} - \frac{(n - l''q)l_2}{q_2} + \frac{n}{q} \right],
\]

(9)

where \( N < N_1 \leq 2N \). Our sum may be written as

\[
\frac{1}{q_1q_2q} \sum_{a \mod q_1q_2q} \sum_{n} e \left( \frac{an}{q_1q_2q} \right) \sum_{x \mod q_1q_2q} e \left[ f(x) - \frac{ax}{q_1q_2q} \right],
\]

(10)

where \( f(x) \) is the amplitude in (9) and the range of summation for \( n \) is the same as before. The main contribution will come from the part where \( a \equiv 0 \pmod{q_1q_2q} \). That part in (10) is the following

\[
\frac{N}{q_1q_2q} \sum_{x \mod q_1q_2q} e [f(x)].
\]

(11)
The other parts will have small contributions, but they are nevertheless

\[ \ll \sum_{0 < |a| \leq q_1 q_2 q / 2} \frac{1}{|a|} \left| \sum_{x \mod q_1 q_2 q} e \left[ f(x) - \frac{ax}{q_1 q_2 q} \right] \right| \]  \hspace{1cm} (12)\]

The sum in (11) is a Ramanujan type sum while the one in (12) is a Kloosterman type sum and may be estimated via Weil’s bound. This will give the $N^{3/4}Q^{11/8}$ in (7).

The other terms in (7) come from the contribution of (11) which is a Ramanujan type sum, and estimates for such sums are well-known. The assumption that $q$’s are primes provides convenience in the estimates here. \hfill \Box
The asymptotic formula of (5) is useful when $N \ll Q$. Theorem 2 is better than (5) when $Q^{\frac{3}{2}+\epsilon} \ll N$. We would certainly hope to have a result that is useful whenever (5) is not, *id est* whenever $Q \ll N$. However, since we already have to resort to the strength of Weil bound for our present result, any desire for improvement is perhaps too greedy.