J. Math. Anal. Appl. 459 (2018) 53–81

Contents lists available at ScienceDirect

Journal of Mathematical Analysis and Applications

www.elsevier.com/locate/jmaa

On the exponential large sieve inequality for sparse sequences modulo primes

Mei-Chu Chang [a], Bryce Kerr [b], Igor E. Shparlinski [b,*]

[a] Department of Mathematics, University of California, Riverside, CA 92521, USA
[b] Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history:
Received 31 July 2017
Available online 31 October 2017
Submitted by S. Tikhonov

Keywords:
Exponential sums
Sparse sequences
Large sieve

ABSTRACT

We complement the argument of M. Z. Garaev (2009) [9] with several other ideas to obtain a stronger version of the large sieve inequality with sparse exponential sequences of the form λ^{s_n}. In particular, we obtain a result which is non-trivial for monotonically increasing sequences $\mathcal{S} = \{s_n\}_{n=1}^{\infty}$ provided $s_n \leqslant n^{2+o(1)}$, whereas the original argument of M. Z. Garaev requires $s_n \leqslant n^{15/14+o(1)}$ in the same setting. We also give an application of our result to arithmetic properties of integers with almost all digits prescribed.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

The classical large sieve inequality, giving upper bounds on average values of various exponential and similar Dirichlet polynomials, such as

$$\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q} \left| \sum_{s=1}^{S} \alpha_s \exp\left(2\pi i a s/q\right) \right|^2 \quad \text{and} \quad \sum_{q=1}^{Q} \sum_{\substack{\chi \bmod q \\ \chi \text{ prim.}}} \left| \sum_{s=1}^{S} \alpha_s \chi(s) \right|^2,$$

with primitive multiplicative characters χ modulo q and arbitrary complex weights $\{\alpha_s\}_{n=1}^{S}$, has proved to be an extremely useful and versatile tool in analytic number theory and harmonic analysis, see, for example, [13,17,18].

Furthermore, if the weights α_s are supported only on elements of some sequence $\mathcal{S} = \{s_n\}_{n=1}^{T}$, which naturally occurs in many number theoretic applications, then the above sums can be written as

* Corresponding author.
E-mail addresses: mcc@math.ucr.edu (M.-C. Chang), bryce.kerr89@gmail.com (B. Kerr), igor.shparlinski@unsw.edu.au (I.E. Shparlinski).

https://doi.org/10.1016/j.jmaa.2017.10.070
0022-247X/© 2017 Elsevier Inc. All rights reserved.

$$\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_q\left(s_n\right) \right|^2 \quad \text{and} \quad \sum_{q=1}^{Q} \sum_{\substack{\chi \bmod q \\ \chi \text{ prim.}}} \left| \sum_{n \leqslant T} \gamma_n \chi(s_n) \right|^2, \tag{1.1}$$

where $\gamma_n = \alpha_{s_n}$ and

$$\mathbf{e}_q(z) = \exp(2\pi i z/q).$$

However, the power of general bounds rapidly diminishes when the sequence $\mathcal{S}$ becomes sparse.

Partially motivated by this phenomenon, and partially by applications to Mersenne numbers, Garaev and Shparlinski [10, Theorem 3.1] have introduced a modification of the large sieve, for both exponential and Dirichlet polynomials with arguments that contain exponentials from extremely sparse sequences.

In particular, in the setting of [10], the arguments of the exponentials and characters appearing in (1.1) contain exponential functions λ^{s_n} with elements of $\mathcal{S}$ rather than the elements of $\mathcal{S}$ themselves. In the case of exponential polynomials, Garaev [9] has introduced a new approach, which has led to a stronger version of the exponential large sieve inequality, improving some of the results of [10], see also [1, Lemma 2.11] and [22, Theorem 1] for several other bounds of this type. Furthermore, stronger versions of the exponential large sieve inequality for special sequences $\mathcal{S}$, such as T consecutive integers or the first T primes, can also be found in [1,10], with some applications given in [21].

Here we continue this direction and concentrate on the case of general sequences $\mathcal{S}$ without any arithmetic restriction. We introduce several new ideas which allow us to improve some results of Garaev [9]. For example, we make use of the bound of [15, Theorem 5.5] on exponential sums over small multiplicative subgroups modulo p, which hold for almost all primes p, see Lemma 3.2. We also make the method more flexible so it now applies to much sparser sequences $\mathcal{S}$ than in [9]. We believe these ideas may find more applications in similar problems.

More precisely, let us fix some integer $\lambda \geqslant 2$. For each prime number p, we let t_p denote the order of $\lambda \bmod p$. For real X and Δ we define the set

$$\mathcal{E}_\Delta(X) = \{p \leqslant X \ : \ t_p \geqslant \Delta\}.$$

Note that by a result of Erdős and Murty [8], see also (2.15), for $\Delta = X^{1/2}$, almost all primes $p \leqslant X$ belong to $\mathcal{E}_\Delta(X)$.

For integer T and two sequences of complex weights $\Gamma = \{\gamma_n\}_{n=1}^T$ and integers $\mathcal{S} = \{s_n\}_{n=1}^T$ we define the sums

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) = \sum_{p \in \mathcal{E}_\Delta(X)} \max_{\gcd(a,p)=1} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_p(a\lambda^{s_n}) \right|^2.$$

These sums majorize the ones considered by Garaev [9] where each term is divided by the divisor function $\tau(p-1)$ of $p-1$. Here we obtain a new bound of the sums $V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta)$ which in particular improves some bounds of Garaev [9].

The argument of Garaev [9] reduces the problem to bounding Gauss sums for which he uses the bound of Heath-Brown and Konyagin [12], that is, the admissible pair (2.1), which is defined below. In particular, for $V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/2})$ the result of Garaev [9] is nontrivial provided

$$S \leqslant X^{15/14+o(1)}. \tag{1.2}$$

Our results by-pass significantly the threshold (2.9) and allow us to replace 15/14 with any fixed $\vartheta < 2$.

Our improvement is based on a modification of the argument of Garaev [9] which allows us to use the bounds of short sums with exponential functions, given in [15, Theorem 5.5], see also Lemma 3.2 below. This alone allows us to extend the result of [9] to sparse sequences $\mathcal{S}$, roughly growing at most $s_n \leqslant n^{7/6-\varepsilon}$ for any fixed $\varepsilon > 0$ in the same scenario where the result of [9] limits the growth to $s_n \leqslant n^{15/14-\varepsilon}$. Furthermore, using bounds of exponential sums over small subgroups of finite fields, in particular that of Bourgain, Glibichuk and Konyagin [5] we relax the condition on $\mathcal{S}$ to $s_n \leqslant n^{3/2-\varepsilon}$.

Using a different argument which combines a bound of Bourgain and Chang [4] for Gauss sums modulo a product of two primes with a duality principle for bilinear forms, we obtain another, although less explicit bound which allows the elements to grow as fast as $s_n \leqslant n^{2-\varepsilon}$. Furthermore, for this result we do not need to limit the summation to primes from $\mathcal{E}_\Delta(X)$ but can consider all primes from $p \leqslant X$, in which case we denote

$$V_\lambda(\Gamma, \mathcal{S}; T, X) = \sum_{p \in X} \max_{\gcd(a,p)=1} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_p(a\lambda^{s_n}) \right|^2 .$$

We also give an application of our new estimate to investigating arithmetic properties of integers with almost all digits prescribed in some fixed base. To simplify the exposition, we only consider binary expansions (and hence we talk about bits rather than binary digits). Namely, for an integer $S \geqslant 1$, an S-bit integer a and a sequence of integers $\mathcal{S} = \{s_n\}_{n=1}^T$ with $0 \leqslant s_1 < \ldots < s_T \leqslant S$, we denote by $\mathcal{N}(a; \mathcal{S})$ the set of S-bit integers z whose bits on all positions $j = 1, \ldots, S$ (counted from the right) must agree with those of a except maybe when $j \in \mathcal{S}$.

We first recall that Bourgain [2,3] has recently obtained several very strong results about the distribution of prime numbers among the elements of $\mathcal{N}(a; \mathcal{S})$, see also [11]. However, in the setting of the strongest result in this direction from [3], the set $\mathcal{S}$ of "free" positions has to be very massive, namely its cardinality has to satisfy $T \geqslant (1 - \kappa)S$ for some small (and unspecified) absolute constant $\kappa > 0$. In the case of square-free numbers instead of prime numbers, a similar result has been obtained in [6] with any fixed $\kappa < 2/5$ (one can also find in [6] some results on the distribution of the value of the Euler function and quadratic non-residues in $\mathcal{N}(a; \mathcal{S})$). Here we address a problem at the other extreme, and relax the strength of arithmetic conditions on the elements from $\mathcal{N}(a; \mathcal{S})$ but instead consider much sparser sets $\mathcal{S}$ of available positions. In particular, we show that the product of the elements from $\mathcal{N}(a; \mathcal{S})$ contains significantly more prime divisors than a typical integer of comparable size.

2. Main results

Throughout the paper, the letter p always denotes a prime number.

As usual $A = O(B)$, $A \ll B$, $B \gg A$ are all equivalent to $|A| \leqslant c|B|$ for some *absolute* constant $c > 0$ (unless indicated otherwise), whereas $A = o(B)$ means that $A/B \to 0$.

We say that a pair (α, β) is *admissible* if for any prime p and any integer λ with $\gcd(\lambda, p) = 1$ we have

$$\max_{(a,p)=1} \left| \sum_{z=1}^{t} \mathbf{e}_p(a\lambda^z) \right| \leqslant t^\alpha p^{\beta + o(1)},$$

as $p \to \infty$, where t is the multiplicative order of λ modulo p.

Concerning admissible pairs, Korobov [16] has shown that the pair

$$(\alpha, \beta) = (0, 1/2),$$

is admissible. For shorter ranges of t, Korobov's bound has been improved by Heath-Brown and Konyagin [12] who show that the pairs

$$(\alpha, \beta) = (5/8, 1/8), \tag{2.1}$$

and

$$(\alpha, \beta) = (3/8, 1/4), \tag{2.2}$$

are admissible.

More recently Shkredov [19,20] has shown that the pair

$$(\alpha, \beta) = (1/2, 1/6), \tag{2.3}$$

is admissible, which improves on the pairs (2.1) and (2.2) in the medium range of t.

Furthermore, the truly remarkable result of Bourgain, Glibichuk and Konyagin [5] implies that for any $\zeta > 0$ there is some $\vartheta > 0$ that depends only on ζ such that

$$(1 - \vartheta, \zeta\vartheta), \tag{2.4}$$

is admissible.

Our first result is as follows.

Theorem 2.1. *Suppose that for an admissible pair (α, β) and some positive numbers η and δ, we have*

$$\frac{\beta + \eta}{1 - \alpha} \leqslant \frac{1}{2} - \delta. \tag{2.5}$$

Suppose further that S, T and X are parameters satisfying

$$T^{1+1/(3-2\alpha)} \geqslant SX^{2\eta}. \tag{2.6}$$

Let $\Delta > 1$ and integer $k \geqslant 1$ satisfy

$$X \leqslant \left(\left(\frac{T}{SX^{2\eta}} \right)^{1/(3-2\alpha)} \Delta \right)^k. \tag{2.7}$$

Then for any sequence of complex numbers $\Gamma = \{\gamma_n\}_{n=1}^T$ with $|\gamma_n| \leqslant 1$ and integers $\mathcal{S} = \{s_n\}_{n=1}^T$ with $0 \leqslant s_1 < \ldots < s_T \leqslant S$ we have

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \leqslant \left(X + TX^{-\delta/(k^2+2)} + \left(S^{2-2\alpha} TX^{-2\eta} \right)^{1/(3-2\alpha)} \right) TX^{1+o(1)}.$$

We note that under (2.6) the condition (2.7) also follows from a simpler inequality

$$X \leqslant \left(T^{-1/(3-2\alpha)^2} \Delta \right)^k.$$

For comparison of Theorem 2.1 with the bound of Garaev [9], we take $T = X^{1+\varepsilon}$ for some small fixed $\varepsilon > 0$ and $\Delta = X^{1/2}$. Assuming the conditions of Theorem 2.1 are satisfied, we analyse each of the three terms

$$TX^2, \qquad T^2 X^{1-\delta/(k^2+2)}, \qquad S^{1-1/(3-2\alpha)} T^{1+1/(3-2\alpha)} X^{1-2\eta/(3-2\alpha)},$$

of its bound independently and compare them with the trivial bound T^2X. Note that we have discarded $X^{o(1)}$ as we aim to establish a power saving in our bound which does not affect this property.

First we notice that for the first term we obviously have

$$TX^2 = T^2X^{1-\varepsilon},$$

provided that X is large enough.

We next notice that the third term $T^2X^{1-\delta/(k^2+2)}$ is always nontrivial provided k is bounded.

For the second term, apart of $X^{o(1)}$ we have

$$S^{1-1/(3-2\alpha)}T^{1+1/(3-2\alpha)}X^{1-2\eta/(3-2\alpha)} = T^2X\Omega,$$

where

$$\begin{aligned}\Omega &= S^{2(1-\alpha)/(3-2\alpha)}T^{-2(1-\alpha)/(3-2\alpha)}X^{-2\eta/(3-2\alpha)}\\ &= \left(S^{1-\alpha}T^{-1-\alpha}X^{-\eta}\right)^{2/(3-2\alpha)}\\ &= \left(S^{1-\alpha}X^{-1-\alpha-\eta}\right)^{2/(3-2\alpha)}X^{-2(1-\alpha)\varepsilon/(3-2\alpha)} \leqslant X^{-2(1-\alpha)\varepsilon/(3-2\alpha)},\end{aligned}$$

provided

$$S \ll X^{1+\eta/(1-\alpha)}. \tag{2.8}$$

Garaev [9] uses the bound of Heath-Brown and Konyagin [12], that is, the admissible pair (2.1), to provide an estimate on $V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/2})$ which is nontrivial provided

$$S \leqslant X^{15/14+o(1)}. \tag{2.9}$$

For comparison with our bound, using the same pair (2.1) and considering the condition (2.5), we see that we may take

$$\eta = \frac{1}{16} - \frac{3}{8}\delta, \tag{2.10}$$

and the condition (2.8) becomes

$$S \leqslant X^{7/6-\delta}, \tag{2.11}$$

under which we have

$$V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/2}) \leqslant T^2X^{1-\kappa},$$

for some $\kappa > 0$ depending on δ and ε. In particular, by taking $\delta > 0$ sufficiently small we see that (2.11) by-passes the threshold (2.9) due to Garaev [9].

It remains to verify the conditions (2.6) and (2.7) are satisfied.

For (2.6), since $T \geqslant X$, recalling that $\alpha = 5/8$ it is enough to check that

$$S \leqslant X^{11/7-2\eta}. \tag{2.12}$$

Recalling (2.11) we see that it is enough to check that

$$\frac{11}{7} - 2\eta \geqslant \frac{7}{6} - \delta,$$

or

$$\eta \leqslant \frac{17}{84} + \frac{1}{2}\delta,$$

which is satisfied for the choice (2.10).

Next consider the condition (2.7). Again, we see that it is enough to check that

$$X \leqslant \left(\left(\frac{X^{1-2\eta}}{S}\right)^{1/(3-2\alpha)} \Delta\right)^k.$$

We first note that (2.10) and (2.11) imply that

$$\frac{X^{1-2\eta}}{S} \geqslant X^{-7/24}.$$

Recalling the choice of $\alpha = 5/8$ and $\Delta = X^{1/2}$, we see that the above inequality follows from

$$X \leqslant \left(\left(X^{-7/24}\right)^{4/7} \Delta\right)^k = \left(X^{-1/6+1/2}\right)^k = \left(X^{1/3}\right)^k,$$

and hence we may take $k = 3$ and produce a bound of the form

$$V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/2}) \leqslant X^{3-\kappa},$$

for some fixed $\kappa > 0$ provided (2.11) is satisfied (improving the trivial bound $X^{3+o(1)}$).

We next consider using the admissible pair (2.3) given by Shkredov. As before we take $T = X^{1+\varepsilon}$ for some small fixed ε and $\Delta = X^{1/2}$. Considering the condition (2.5), we may take

$$\eta = \frac{1}{12} - \frac{\delta}{2},$$

so that (2.8) becomes

$$S \leqslant X^{7/6-\delta}, \tag{2.13}$$

which is the same range produced by the admissible pair given by Heath-Brown and Konyagin. We next verify when the conditions (2.6) and (2.7). Considering (2.6), it is enough to check that

$$S \leqslant X^{8/6} = X^{8/6},$$

which is guaranteed by (2.13). Considering (2.7), we need

$$X \leqslant \left(\left(\frac{X^{1-2\eta}}{S}\right)^{1/(3-2\alpha)} \Delta\right)^k.$$

We first note that

$$\frac{X^{1-2\eta}}{S} \geqslant X^{-1/3},$$

hence recalling that $\Delta = X^{1/2}$, it is enough to check that

$$X \leqslant X^{k/6},$$

which is satisfied for $k = 6$.

Furthermore, let us fix some $\zeta > 0$ and consider the admissible pair given by (2.4). With the above choice of parameters $T = X^{1+\varepsilon}$ and $\Delta = X^{1/2}$, we see that we can take

$$\eta = \frac{\vartheta}{2} - \delta\vartheta - \zeta\vartheta,$$

and the condition (2.8) becomes

$$S \leqslant X^{3/2-\delta-\zeta}. \tag{2.14}$$

This produces a bound of the form

$$V_\lambda(\Gamma, \mathcal{S}; T, X, X^{1/2}) \leqslant X^{3-\kappa},$$

provided the inequalities (2.6) and (2.7) are satisfied. Considering (2.6), we have

$$SX^{2\eta} \leqslant X^{3/2+\vartheta} \leqslant X^{1+1/(1+2\vartheta)} \leqslant T^{1+1/(3-2(1-\vartheta))},$$

provided ϑ is sufficiently small, which we may assume.

Considering (2.7), we have

$$\left(\frac{T}{SX^{2\eta}}\right)^{1/(3-2\alpha)} \Delta \geqslant \left(\frac{X^{\delta+\zeta}}{X^{(1+2\vartheta)/2}}\right)^{1/(1+2\vartheta)} X^{1/2} = X^{(\delta+\zeta)/(1+2\vartheta)},$$

and hence (2.7) is satisfied by taking

$$k = \left\lfloor \frac{1+2\vartheta}{\delta+\zeta} \right\rfloor + 1.$$

Using a different method we can set $\Delta = 1$ and also extend the range of S for which we may obtain a nontrivial bound for $V_\lambda(\Gamma, \mathcal{S}; T, X)$ at the cost of making the power saving explicit.

Theorem 2.2. *There exists some absolute constant $\rho > 0$ such that*

$$V_\lambda(\Gamma, \mathcal{S}; T, X) \leqslant \left(X^{1-\rho}T^2 + X^{3/2}T^{3/2} + X^{3/4}T^{7/4}S^{1/4}\right) X^{o(1)}.$$

Comparing the bound of Theorem 2.2 with the trivial bound XT^2, we see that it is nontrivial provided

$$T > X^{1+\varepsilon} \quad \text{and} \quad S < X^{1+\varepsilon}T,$$

which on taking $T = X^{1+\varepsilon}$, we obtain a power saving in Theorem 2.2 provided $S \leqslant T^{2-\varepsilon}$.

For a sequence of points $\mathcal{A} = \{a_n\}_{n=1}^T$ we define the discrepancy D of $\mathcal{A}$ by

$$D = \sup_{0 \leqslant a \leqslant b \leqslant 1} \left| \frac{A(a,b)}{T} - (b-a) \right|,$$

where $A(a,b)$ denotes the number of points of $\mathcal{A}$ falling in the interval $[a,b] \in [0,1]$. Garaev [9] combines his bound for $V_\lambda(\Gamma, \mathcal{S}, T, X, \Delta)$ with a result of Erdős and Murty [8], which in particular implies that

$$\mathcal{E}_{X^{1/2},X} = (1+o(1))\frac{X}{\log X}, \qquad X \to \infty, \tag{2.15}$$

and the Erdős–Turán inequality (see for example [7]). This allows Garaev [9, Section 3] to show that for any $\varepsilon > 0$ there is some $\delta > 0$ such that for almost all primes $p \leqslant X$, the sequence

$$A(\lambda, p) = \left\{ \frac{\lambda^{s_n}}{p} \bmod 1 \right\}_{1 \leqslant n \leqslant T}, \tag{2.16}$$

with $T = \left\lceil X(\log X)^{2+\varepsilon} \right\rceil$, has discrepancy

$$D \leqslant (\log T)^{-\delta},$$

provided $S \leqslant X^{15/14+o(1)}$ as $X \to \infty$.

For comparison with our bound, Theorem 2.2 produces the following result. For any $\varepsilon > 0$ and almost all primes $p \leqslant X$, the sequence (2.16) with $T = \left\lceil X^{1+\varepsilon} \right\rceil$ has discrepancy

$$D \leqslant T^{-\delta},$$

provided that $S \leqslant X^{2-\varepsilon}$ as $X \to \infty$.

We now give an application of Theorem 2.2 to the numbers with prescribed digits, namely to the integers from the set $\mathcal{N}(a; \mathcal{S})$, defined in Section 1. We denote by $\omega(k)$ the number of distinct prime divisors of an integer $k \geqslant 1$.

Theorem 2.3. *Let us fix some $\varepsilon > 0$. For any sequence of integers $\mathcal{S} = \{s_n\}_{n=1}^{T}$ with $0 \leqslant s_1 < \ldots < s_T \leqslant S$ with*

$$S \leqslant T^{2-\varepsilon},$$

and any S-bit integer a, letting

$$P(a; \mathcal{S}) = \prod_{z \in \mathcal{N}(a;\mathcal{S})} z,$$

we have

$$\omega\left(P(a; \mathcal{S})\right) \gg T^{1+\delta},$$

for some $\delta > 0$ which depends only on ε.

Considering Theorem 2.3, we first recall a classic result of Hardy and Ramanujan, which states that for any function $\psi(x) \to \infty$, the number of positive integers $n \leqslant x$ such that

$$|\omega(n) - \log\log n| > \psi(n)(\log\log n)^{1/2},$$

is $o(x)$, see, for example [13, Corollary 1.4]. Since we have

$$2^{2^T S} \ll P(a; \mathcal{S}) \ll 2^{2^T S},$$

an application of Theorem 2.3 gives

$$\omega(P(a;\mathcal{S})) \geqslant (\log\log P(a;\mathcal{S}))^{1+\delta},$$

for some $\delta > 0$. In particular, the above inequality implies that the product $P(a;\mathcal{S})$ has a much larger number of prime factors than one usually expects from an integer of similar size.

3. Preliminary results

We use Σ^* to indicate that the summation is taken over a reduced residue system. That is, for any function ψ and integer k, we have

$$\sideset{}{^*}\sum_{c \bmod k} \psi(c) = \sum_{\substack{c=1\\ \gcd(c,k)=1}}^{k} \psi(c).$$

We need the following simplified form of the large sieve inequality, see [13, Theorem 7.11].

Lemma 3.1. *For any $K \geqslant 1$ and increasing sequence of integers $\mathcal{S} = \{s_n\}_{n=1}^T$ with $\max_{s\in\mathcal{S}} s = S$ and any sequence of complex numbers $\Gamma = \{\gamma_n\}_{n=1}^T$ with $|\gamma_n| \leqslant 1$ we have*

$$\sum_{k\leqslant K} \sideset{}{^*}\sum_{c \bmod k} \left|\sum_{n\leqslant T} \gamma_n \mathbf{e}_k(cs_n)\right|^2 \ll (K^2+S)T.$$

The following is [15, Theorem 5.5].

Lemma 3.2. *For each integer t and prime $\ell \equiv 1 \bmod t$ we fix some element $g_{t,\ell}$ of multiplicative order t modulo ℓ. Then, for any fixed integer $k \geqslant 2$ and an arbitrary $U > 1$, the bound*

$$\max_{(a,\ell)=1} \left|\sum_{x=0}^{t-1} \mathbf{e}_\ell(ag_{t,\ell}^x)\right| \ll t\ell^{1/2k^2}(t^{-1/k} + U^{-1/k^2}),$$

holds for all primes $\ell \equiv 1 \bmod t$ except at most $U/\log U$ of them.

Lemma 3.3. *Let λ be a fixed integer. For any $Z > 0$ we have*

$$\#\{p \text{ prime} \ : \ \operatorname{ord}_p \lambda \leqslant Z \} \ll Z^2$$

where the implied constant may depend on λ.

Proof. If $\operatorname{ord}_p \lambda = y$ then $\lambda^y - 1 \equiv 0 \bmod p$. This implies that

$$\#\{p \text{ prime} \ : \ \operatorname{ord}_p \lambda < Z\} \leqslant \omega\left(\prod_{1\leqslant z\leqslant Z} (\lambda^z - 1)\right),$$

where as before, $\omega(k)$ denotes the number of distinct prime divisors of an integer $k \geqslant 1$. Hence,

$$\#\{p \text{ prime} \ : \ \operatorname{ord}_p \lambda < Z \} \ll \log \prod_{1\leqslant z\leqslant Z} (\lambda^z - 1) \leqslant \log\left(\lambda^{Z^2/2}\right) \ll Z^2,$$

which gives the desired result. □

The following is a special case of [4, Corollary 4.2].

Lemma 3.4. *Let p_1 and p_2 be primes and let $\mathcal{H}$ be a subgroup of $\mathbb{Z}_q^*$, where $q = p_1p_2$ such that*

$$\#\{\mathcal{H} \bmod p_\nu\} \geqslant q^\delta, \qquad \nu = 1, 2$$

for some fixed $\delta > 0$. Then

$$\max_{\gcd(a,q)=1} \left| \sum_{h\in\mathcal{H}} \mathbf{e}_q(ah) \right| \leqslant (\#\mathcal{H})^{1-\varrho},$$

for some $\varrho > 0$ which depends only on $\delta > 0$.

4. Proof of Theorem 2.1

4.1. Initial transformations

Let

$$\sigma_p(a) = \sum_{n\leqslant T} \gamma_n \, \mathbf{e}_p(a\lambda^{s_n}).$$

It is also convenient to define a_p as any integer $a \in \{1, \dots, p-1\}$ with

$$|\sigma_p(a_p)| = \max_{\gcd(a,p)=1} |\sigma_p(a)|, \tag{4.1}$$

so that

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) = \sum_{p\in\mathcal{E}_\Delta(X)} |\sigma_p(a_p)|^2.$$

However, it is more convenient to work with the sums where each term is divided by the divisor function $\tau(p-1)$. We define

$$W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) = \sum_{p\in\mathcal{E}_\Delta(X)} \frac{1}{\tau(p-1)} |\sigma_p(a)|^2,$$

and note the inequality $\tau(n) = n^{o(1)}$ implies that

$$V_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \leqslant W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) X^{o(1)}.$$

Hence it is enough to prove

$$W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \leqslant \left(X + \frac{S^{1-1/(3-2\alpha)} T^{1/(3-2\alpha)}}{X^{2\eta/(3-2\alpha)}} + \frac{T}{X^{\delta/(k^2+2)}} \right) T X^{1+o(1)}, \tag{4.2}$$

where $\alpha, \beta, \delta, \eta$ satisfy (2.5) and (α, β) is an admissible pair.

Fix some $p \leqslant X$ and consider $\sigma_p(a_p)$. Recalling that t_p denotes the order of $\lambda \mod p$, we split s_n into arithmetic progressions mod t_p. Using the orthogonality of exponential functions, we obtain

$$\sigma_p(a_p) = \sum_{x=1}^{t_p} \sum_{\substack{n\leqslant T\\ s_n\equiv x \bmod t_p}} \gamma_n\, \mathbf{e}_p(a_p\lambda^{s_n})$$
$$= \frac{1}{t_p}\sum_{x=1}^{t_p}\sum_{b=1}^{t_p}\sum_{n\leqslant T} \gamma_n\, \mathbf{e}_{t_p}(b(s_n-x))\, \mathbf{e}_p(a_p\lambda^x),$$

and hence

$$\sigma_p(a_p) = \frac{1}{t_p}\sum_{d\mid t_p}\sum_{x=1}^{t_p}\sum_{\substack{b=1\\ \gcd(b,t_p)=d}}^{t_p}\sum_{n\leqslant T} \gamma_n\, \mathbf{e}_{t_p}(b(s_n-x))\, \mathbf{e}_p(a_p\lambda^x)$$
$$= \frac{1}{t_p}\sum_{d\mid t_p}\sum_{x=1}^{t_p}\sum_{b \bmod (t_p/d)}^{*}\sum_{n\leqslant T} \gamma_n\, \mathbf{e}_{t_p/d}(b(s_n-x))\, \mathbf{e}_p(a_p\lambda^x).$$

Let $\xi > 0$ be a real parameter to be chosen later. We set

$$D_p = \xi t_p,$$

and partition summation over d according to D_p. This gives

$$|\sigma_p(a_p)| \leqslant |\sigma_{p,1}(a_p)| + |\sigma_{p,2}(a_p)|, \tag{4.3}$$

where

$$\sigma_{p,1}(a_p) = \frac{1}{t_p}\sum_{\substack{d\mid t_p\\ d\leqslant D_p}}\sum_{x=1}^{t_p}\sum_{b \bmod (t_p/d)}^{*}\sum_{n\leqslant T} \gamma_n\, \mathbf{e}_{t_p/d}(b(s_n-x))\, \mathbf{e}_p(a_p\lambda^x), \tag{4.4}$$

and

$$\sigma_{p,2}(a_p) = \frac{1}{t_p}\sum_{\substack{d\mid t_p\\ d> D_p}}\sum_{x=1}^{t_p}\sum_{b \bmod (t_p/d)}^{*}\sum_{n\leqslant T} \gamma_n\, \mathbf{e}_{t_p/d}(b(s_n-x))\, \mathbf{e}_p(a_p\lambda^x).$$

The equation (4.3) implies that

$$|\sigma_p(a_p)|^2 \ll |\sigma_{p,1}(a_p)|^2 + |\sigma_{p,2}(a_p)|^2,$$

which on averaging over $p \leqslant X$ gives

$$W_\lambda(\Gamma, \mathcal{S}; T, X, \Delta) \ll \Sigma_1 + \Sigma_2, \tag{4.5}$$

where

$$\Sigma_1 = \sum_{p\in\mathcal{E}_\Delta(X)} \frac{1}{\tau(p-1)}|\sigma_{p,1}(a_p)|^2,$$
$$\Sigma_2 = \sum_{p\in\mathcal{E}_\Delta(X)} \frac{1}{\tau(p-1)}|\sigma_{p,2}(a_p)|^2. \tag{4.6}$$

4.2. The sum Σ_1

To bound Σ_1 we use the argument of Garaev [9, Theorem 3.1]. Fix some $p \leqslant X$ and consider $\sigma_{p,1}(a_p)$. From (4.4) and the Cauchy–Schwarz inequality

$$|\sigma_{p,1}(a_p)|^2 = \left| \frac{1}{t_p} \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sum_{x=1}^{t_p} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b(s_n - x)) \, \mathbf{e}_p(a_p \lambda^x) \right|^2$$

$$\leqslant \frac{\tau(t_p)}{t_p} \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sum_{x=1}^{t_p} \left| \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b(s_n - x)) \right|^2 .$$

Expanding the square and interchanging summation gives

$$|\sigma_{p,1}(a_p)|^2 \leqslant \frac{\tau(t_p)}{t_p} \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b_1, b_2 \bmod (t_p/d)}$$

$$\sum_{n_1, n_2 \leqslant T} \gamma_{n_1} \overline{\gamma}_{n_2} \, \mathbf{e}_{t_p/d}(b_1 s_{n_1} - b_2 s_{n_2}) \sum_{x=1}^{t_p} \mathbf{e}_{t_p/d}(x(b_2 - b_1)).$$

By the orthogonality of exponential functions, the inner sum vanishes unless $b_1 = b_2$. Hence

$$|\sigma_{p,1}(a_p)|^2 \leqslant \tau(t_p) \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n_1, n_2 \leqslant T} \gamma_{n_1} \overline{\gamma}_{n_2} \, \mathbf{e}_{t_p/d}(b(s_{n_1} - s_{n_2}))$$

$$\leqslant \tau(p-1) \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b s_n) \right|^2 ,$$

where we have used the inequality

$$\tau(t_p) \leqslant \tau(p-1),$$

since $t_p \mid (p-1)$. Summing over $p \leqslant X$ we see that

$$\Sigma_1 \leqslant \sum_{p \leqslant X} \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b s_n) \right|^2 .$$

We define the sequence of numbers X_j for $1 \leqslant j \leqslant J$, where

$$J = \left\lceil \frac{\log(X/\Delta)}{\log 2} \right\rceil , \tag{4.7}$$

by

$$X_1 = \Delta, \qquad X_j = \min\{2X_{j-1}, X\}, \ 2 \leqslant j \leqslant J, \tag{4.8}$$

and partition the set of primes $p \leqslant X$ into the sets

$$\mathcal{R}_j = \{p \leqslant X \ : \ X_j \leqslant t_p < X_{j+1}\}. \tag{4.9}$$

Writing

$$\Sigma_{1,j} = \sum_{p \in \mathcal{R}_j} \sum_{\substack{d \mid t_p \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(bs_n) \right|^2,$$

we have

$$\Sigma_1 \ll \sum_{j=1}^{J} \Sigma_{1,j}. \tag{4.10}$$

For each integer r, we define the set $\mathcal{Q}(r)$ by

$$\mathcal{Q}(r) = \{p \leqslant X \ : \ t_p = r\}, \tag{4.11}$$

so that, replacing t_p with r for $p \in \mathcal{Q}(r)$, we obtain

$$\begin{aligned} \Sigma_{1,j} &\leqslant \sum_{X_j \leqslant r < 2X_j} \sum_{p \in \mathcal{Q}(r)} \sum_{\substack{d \mid r \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b \bmod (r/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{r/d}(bs_n) \right|^2 \\ &= \sum_{X_j \leqslant r < 2X_j} \#\mathcal{Q}(r) \sum_{\substack{d \mid r \\ d \leqslant D_p}} \sideset{}{^*}\sum_{b \bmod (r/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{r/d}(bs_n) \right|^2. \end{aligned}$$

For each prime $p \in \mathcal{Q}(r)$ we have $r \mid (p-1)$ and hence for $X_j \leqslant r < 2X_j$ we also have

$$\#\mathcal{Q}(r) \leqslant \frac{X}{r} \leqslant \frac{X}{X_j} \qquad \text{and} \qquad D_p < 2\xi X_j.$$

This implies that

$$\begin{aligned} \Sigma_{1,j} &\leqslant \frac{X}{X_j} \sum_{X_j \leqslant r < 2X_j} \sum_{\substack{d \mid r \\ d \leqslant 2\xi X_j}} \sideset{}{^*}\sum_{b \bmod (r/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{r/d}(bs_n) \right|^2 \\ &= \frac{X}{X_j} \sum_{d \leqslant 2\xi X_j} \sum_{\substack{X_j \leqslant r < 2X_j \\ d \mid r}} \sideset{}{^*}\sum_{b \bmod (r/d)} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{r/d}(bs_n) \right|^2, \end{aligned}$$

and hence

$$\Sigma_{1,j} \leqslant \frac{X}{X_j} \sum_{d \leqslant 2\xi X_j} F_j(d), \tag{4.12}$$

where $F_j(d)$ is given by

$$F_j(d) = \sum_{X_j/d \leqslant m < 2X_j/d} \sideset{}{^*}\sum_{b \bmod m} \left| \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_m(bs_n) \right|^2 .$$

An application of Lemma 3.1 gives

$$F_j(d) \ll \left(\frac{X_j^2}{d^2} + S \right) T,$$

which combined with (4.12) implies that

$$\Sigma_{1,j} \leqslant \frac{X}{X_j} \sum_{d \leqslant 2\xi X_j} \left(\frac{X_j^2}{d^2} + S \right) T \ll \frac{X}{X_j} \left(X_j^2 + 2\xi X_j S \right) T,$$

and hence by (4.10)

$$\Sigma_1 \ll \sum_{j=1}^{J} \frac{X}{X_j} \left(X_j^2 + \xi X_j S \right) T \ll X(X + \xi S \log X) T. \tag{4.13}$$

4.3. The sum Σ_2

Fix some $p \leqslant X$ and consider $\sigma_{p,2}(a_p)$. For each value of d in the outermost summation we split summation over x into arithmetic progressions mod t_p/d. Recalling that $\sigma_{p,2}(a_p)$ is given by

$$\sigma_{p,2}(a_p) = \frac{1}{t_p} \sum_{\substack{d \mid t_p \\ d > D_p}} \sum_{x=1}^{t_p} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b(s_n - x)) \, \mathbf{e}_p \left(a_p \lambda^x \right),$$

we see that

$$\sigma_{p,2}(a_p) = \frac{1}{t_p} \sum_{\substack{d \mid t_p \\ d > D_p}} \sum_{y=1}^{t_p/d} \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b(s_n - y)) \sum_{z=1}^{d} \mathbf{e}_p \left(a_p \lambda^y \lambda^{z t_p/d} \right),$$

and hence

$$\begin{aligned} |\sigma_{p,2}(a_p)| &\leqslant \frac{1}{t_p} \sum_{\substack{d \mid t_p \\ d > D_p}} \sum_{y=1}^{t_p/d} \left| \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b(s_n - y)) \right| \left| \sum_{z=1}^{d} \mathbf{e}_p \left(a_p \lambda^y \lambda^{z t_p/d} \right) \right| \\ &\leqslant \sum_{\substack{d \mid t_p \\ d > D_p}} \frac{1}{t_p} \sum_{y=1}^{t_p/d} \left| \sideset{}{^*}\sum_{b \bmod (t_p/d)} \sum_{n \leqslant T} \gamma_n \, \mathbf{e}_{t_p/d}(b(s_n - y)) \right| \left| \sum_{z=1}^{d} \mathbf{e}_p \left(f_{d,p} \lambda^{z t_p/d} \right) \right|, \end{aligned}$$

where $f_{d,p}$ is chosen to satisfy

$$\left| \sum_{z=1}^{d} \mathbf{e}_p \left(f_{d,p} \lambda^{z t_p/d} \right) \right| = \max_{\gcd(a,p)=1} \left| \sum_{z=1}^{d} \mathbf{e}_p \left(a \lambda^{z t_p/d} \right) \right|.$$

Let

$$U(p,d) = \frac{1}{t_p}\sum_{y=1}^{t_p/d}\left|\sum_{\substack{b=1\\ \gcd(b,t_p/d)=1}}^{t_p/d}\sum_{n\leqslant T}\gamma_n\,\mathbf{e}_{t_p/d}(b(s_n-y))\right|,$$

so that

$$|\sigma_{p,2}(a_p)| \leqslant \sum_{\substack{d\mid t_p\\ d>D_p}} U(p,d)\left|\sum_{z=1}^{d}\mathbf{e}_p(f_{d,p}\lambda^{zt_p/d})\right|. \tag{4.14}$$

We consider bounding the terms $U(p,d)$. By the Cauchy–Schwarz inequality

$$\begin{aligned} U(p,d)^2 &\leqslant \frac{1}{dt_p}\sum_{y=1}^{t_p/d}\left|\sum_{\substack{b=1\\ \gcd(b,t_p/d)=1}}^{t_p/d}\sum_{n\leqslant T}\gamma_n\,\mathbf{e}_{t_p/d}(b(s_n-y))\right|^2\\ &= \frac{1}{dt_p}\sum_{1\leqslant n_1,n_2\leqslant T}\sum_{\substack{b_1,b_2=1\\ \gcd(b_1b_2,t_p/d)=1}}^{t_p/d}\gamma_{n_1}\overline{\gamma}_{n_2}\,\mathbf{e}_{t_p/d}(b_1s_{n_1}-b_2s_{n_2})\sum_{y=1}^{t_p/d}\mathbf{e}_{t_p/d}(y(b_1-b_2)). \end{aligned}$$

Using the orthogonality of exponential functions again, we see that the last sums vanishes unless $b_1=b_2$. This gives

$$U(p,d)^2 \leqslant \frac{1}{d^2}\sum_{1\leqslant n_1,n_2\leqslant T}\sum_{\substack{b=1\\ \gcd(b,t_p/d)=1}}^{t_p/d}\gamma_{n_1}\overline{\gamma}_{n_2}\,\mathbf{e}_{t_p/d}(b(s_{n_1}-s_{n_2})).$$

After rearranging and extending the summation over b to the complete residue system modulo t_p/d, we derive

$$\begin{aligned} U(p,d)^2 &\leqslant \frac{1}{d^2}\sum_{\substack{b=1\\ \gcd(b,t_p/d)=1}}^{t_p/d}\sum_{1\leqslant n_1,n_2\leqslant T}\gamma_{n_1}\overline{\gamma}_{n_2}\,\mathbf{e}_{t_p/d}(b(s_{n_1}-s_{n_2}))\\ &= \frac{1}{d^2}\sum_{\substack{b=1\\ \gcd(b,t_p/d)=1}}^{t_p/d}\left|\sum_{1\leqslant n\leqslant T}\gamma_n\,\mathbf{e}_{t_p/d}(bs_n)\right|^2\\ &\leqslant \frac{1}{d^2}\sum_{b=1}^{t_p/d}\left|\sum_{1\leqslant n\leqslant T}\gamma_n\,\mathbf{e}_{t_p/d}(bs_n)\right|^2 = \frac{t_p}{d^3}V\left(t_p/d\right), \end{aligned}$$

where for an integer $r\geqslant 1$ we define

$$V(r) = \#\{(n_1,n_2)\in[1,T]^2\ :\ s_{n_1}\equiv s_{n_2} \bmod r\}. \tag{4.15}$$

Substituting this in (4.14) gives

$$|\sigma_{p,2}(a_p)| \leqslant t_p^{1/2}\sum_{\substack{d\mid t_p\\ d>D_p}}\frac{1}{d^{3/2}}V\left(t_p/d\right)^{1/2}\left|\sum_{z=1}^{d}\mathbf{e}_p\left(f_{d,p}\lambda^{zt_p/d}\right)\right|.$$

Summing over $p \leqslant X$ gives

$$\Sigma_2 \leqslant \sum_{p\in\mathcal{E}_\Delta(X)} \frac{t_p}{\tau(p-1)} \left(\sum_{\substack{d|t_p \\ d>D_p}} \frac{1}{d^{3/2}} V\left(t_p/d\right)^{1/2} \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zt_p/d}\right)\right| \right)^2,$$

which by the Cauchy–Schwarz inequality implies that

$$\begin{aligned}\Sigma_2 &\leqslant \sum_{p\in\mathcal{E}_\Delta(X)} \frac{t_p\tau(t_p)}{\tau(p-1)} \sum_{\substack{d|t_p \\ d>D_p}} \frac{1}{d^3} V\left(t_p/d\right) \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zt_p/d}\right)\right|^2 \\ &\leqslant \sum_{p\in\mathcal{E}_\Delta(X)} t_p \sum_{\substack{d|t_p \\ d>D_p}} \frac{1}{d^3} V\left(t_p/d\right) \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zt_p/d}\right)\right|^2.\end{aligned}$$

At this point our strategy is to rearrange summation so we may apply Lemma 3.2. We define the sequence X_j as in (4.8), we let $\mathcal{Q}(r)$ be given by (4.11) and for each integer r we define the following subsets $S_i(r)$ of $\mathcal{Q}(r)$

$$\mathcal{S}_i(r) = \{p \ : \ 2^i \leqslant p \leqslant 2^{i+1} \text{ and } t_p = r\}.$$

Writing

$$\Sigma_{2,i,j} = \sum_{X_j\leqslant r\leqslant X_{j+1}} r \sum_{p\in\mathcal{S}_i(r)} \sum_{\substack{d|r \\ d>D_p}} \frac{1}{d^3} V\left(r/d\right) \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right)\right|^2,$$

the above implies that

$$\Sigma_2 \leqslant \sum_{i=1}^{J} \sum_{j:X_j\ll 2^i} \Sigma_{2,i,j}.$$

To further transform the sums $\Sigma_{2,i,j}$, define the numbers Z_j by

$$Z_j = \xi X_j, \qquad j = 1,\dots,J, \tag{4.16}$$

so that

$$\Sigma_{2,i,j} \ll X_j \sum_{X_j\leqslant r\leqslant X_{j+1}} \sum_{p\in\mathcal{S}_i(r)} \sum_{\substack{d|r \\ d>Z_j}} \frac{1}{d^3} V\left(r/d\right) \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right)\right|^2.$$

After interchanging summation, we arrive at

$$\Sigma_{2,i,j} \ll X_j \sum_{Z_j<d\leqslant X_{j+1}} \frac{1}{d^3} \sum_{\substack{X_j\leqslant r\leqslant X_{j+1} \\ d|r}} V\left(r/d\right) \sum_{p\in\mathcal{S}_i(r)} \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right)\right|^2. \tag{4.17}$$

Let ρ be a parameter to be chosen later. We now partition summation over i and j in Σ_2 as follows

$$\Sigma_2 \leqslant \Sigma_2^{\leqslant} + \Sigma_2^{\geqslant}, \tag{4.18}$$

where

$$\Sigma_2^{\leqslant} = \sum_{i=1}^{J} \sum_{j:X_j \leqslant 2^{i\rho}} \Sigma_{2,i,j} \qquad \text{and} \qquad \Sigma_2^{\geqslant} = \sum_{i=1}^{J} \sum_{j:2^{i\rho} \leqslant X_j \ll 2^i} \Sigma_{2,i,j}.$$

To estimate $\Sigma_2^{\leqslant}$, we first fix some j with $X_j \leqslant 2^{i\rho}$. Considering the inner summation over p, we partition $\mathcal{S}_i(r)$ according to Lemma 3.2. Let

$$U_i(r) = \frac{2^{i(1-1/(k^2+2))}}{r^{1-2/(k^2+2)}},$$

and for integer k we define the sets $S_i^{(1)}(r)$ and $S_i^{(2)}(r)$ by

$$\mathcal{S}_i^{(1)}(r) = \Bigg\{ p \in \mathcal{S}_i(r) \ : \ \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right) \right| \leqslant d2^{i/2k^2} \left(d^{-1/k} + U_i(r)^{-1/k^2} \right) \Bigg\},$$

$$\mathcal{S}_i^{(2)}(r) = \mathcal{S}_i(r) \setminus \mathcal{S}_i^{(1)}(r).$$

Lemma 3.2 implies that

$$\#\mathcal{S}_i^{(2)}(r) \ll \frac{U_i(r)}{\log U_i(r)}.$$

Considering $\mathcal{S}_i^{(1)}(r)$ and using the fact that $r \mid p-1$ for $p \in \mathcal{S}_i(r)$ gives

$$\#\mathcal{S}_i^{(1)}(r) \leqslant \#\mathcal{S}_i(r) \ll \frac{2^i}{r}, \tag{4.19}$$

which implies that

$$\sum_{p \in \mathcal{S}_i(r)} \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right) \right|^2 \ll d^2 \left(\frac{2^{i(1+1/k^2)}}{r} (d^{-2/k} + U_i(r)^{-2/k^2}) + \frac{U_i(r)}{\log U_i(r)} \right).$$

Recalling the choice of $U_i(r)$ we see that

$$\sum_{p \in \mathcal{S}_i(r)} \left| \sum_{z=1}^{d} \mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right) \right|^2 \ll \frac{d^2 2^{i(1-1/(k^2+2))}}{r^{1-2/(k^2+2)}} + \frac{d^{2-2/k} 2^{i(1+1/k^2)}}{r},$$

which on assuming that

$$X \leqslant (\xi\Delta)^k, \tag{4.20}$$

simplifies to

$$\sum_{p\in\mathcal{S}_i(r)}\left|\sum_{z=1}^{d}\mathbf{e}_p\left(f_{d,p}\lambda^{zr/d}\right)\right|^2 \ll \frac{d^2 2^{i(1-1/(k^2+2))}}{r^{1-2/(k^2+2)}}. \tag{4.21}$$

Hence considering $\Sigma_{2,i,j}$, we have

$$\begin{aligned}\Sigma_{2,i,j} &\ll X_j 2^{i(1-1/(k^2+2))}\sum_{Z_j<d\leqslant X_{j+1}}\frac{1}{d}\sum_{\substack{X_j\leqslant r\leqslant X_{j+1}\\ d|r}}\frac{V(r/d)}{r^{1-2/(k^2+2)}}\\ &\ll X_j 2^{i(1-1/(k^2+2))}\sum_{Z_j<d\leqslant X_{j+1}}\frac{1}{d^{2-2/(k^2+2)}}\sum_{X_j/d\leqslant r\leqslant X_{j+1}/d}\frac{V(r)}{r^{1-2/(k^2+2)}},\end{aligned}$$

after the change of variable $r\to dr$. Writing

$$W_j(d)=\sum_{X_j/d\leqslant r\leqslant X_{j+1}/d}\frac{V(r)}{r^{1-2/(k^2+2)}},$$

the above implies

$$\Sigma_{2,i,j}\ll X_j 2^{i(1-1/(k^2+2))}\sum_{Z_j<d\leqslant X_{j+1}}\frac{W_j(d)}{d^{2-2/(k^2+2)}}. \tag{4.22}$$

Considering the sum $W_j(d)$ and recalling the definition of $V(r)$ given by (4.15), we have

$$\begin{aligned}W_j(d) &= \sum_{X_j/d\leqslant r\leqslant X_{j+1}/d}\ \sum_{\substack{1\leqslant n_1,n_2\leqslant T\\ s_{n_1}\equiv s_{n_2} \bmod r}}\frac{1}{r^{1-2/(k^2+2)}}\\ &\ll \left(\frac{d}{X_j}\right)^{1-2/(k^2+2)}\sum_{1\leqslant n_1,n_2\leqslant T}\ \sum_{\substack{X_j/d\leqslant r\leqslant X_{j+1}/d\\ s_{n_1}\equiv s_{n_2} \bmod r}}1.\end{aligned}$$

Considering the last sum on the right, we have

$$\sum_{1\leqslant n_1,n_2\leqslant T}\ \sum_{\substack{X_j/d\leqslant r\leqslant X_{j+1}/d\\ s_{n_1}\equiv s_{n_2} \bmod r}}1\ll\frac{TX^j}{d}+\sum_{1\leqslant n_1<n_2\leqslant T}\ \sum_{\substack{X_j/d\leqslant r\leqslant X_{j+1}/d\\ s_{n_1}\equiv s_{n_2} \bmod r}}1.$$

Since the term

$$\sum_{\substack{X_j/d\leqslant r\leqslant X_{j+1}/d\\ s_{n_1}\equiv s_{n_2} \bmod r}}1,$$

is bounded by the number of divisors of $s_{n_2}-s_{n_1}$, we see that

$$\sum_{\substack{X_j/d\leqslant r\leqslant X_{j+1}/d\\ s_{n_1}\equiv s_{n_2} \bmod r}}1=S^{o(1)},$$

and hence

$$\sum_{1\leqslant n_1,n_2\leqslant T}\sum_{\substack{X_j/d\leqslant r\leqslant X_{j+1}/d\\ s_{n_1}\equiv s_{n_2} \bmod r}} 1 \ll \left(\frac{X_j}{d}+TS^{o(1)}\right)T, \tag{4.23}$$

which gives

$$W_j(d)\leqslant \left(\frac{d}{X_j}\right)^{1-2/(k^2+2)}\left(\frac{X_j}{d}+TS^{o(1)}\right)T.$$

Substituting the above into (4.22) we get

$$\begin{aligned}\Sigma_{2,i,j} &\ll X_j^{1+2/(k^2+2)}2^{i(1-1/(k^2+2))}T\sum_{Z_j<d\leqslant X_{j+1}}\frac{1}{d^2}\\ &\quad + X_j^{2/(k^2+2)}2^{i(1-1/(k^2+2))}T^2S^{o(1)}\sum_{Z_j<d\leqslant X_{j+1}}\frac{1}{d},\end{aligned}$$

which simplifies to

$$\begin{aligned}\Sigma_{2,i,j} &\leqslant \frac{X_j^{1+2/(k^2+2)}2^{i(1-1/(k^2+2))}T}{Z_j}+X_j^{2/(k^2+2)}2^{i(1-1/(k^2+2))}T^2(SX)^{o(1)}\\ &\leqslant X_j^{2/(k^2+2)}2^{i(1-1/(k^2+2))}\left(\frac{1}{\xi}+T\right)T(SX)^{o(1)},\end{aligned}$$

on recalling the choice of Z_j given by (4.16).

We now assume that

$$\xi\geqslant\frac{1}{T}. \tag{4.24}$$

Without loss of generality, we can also assume that $S=X^{O(1)}$ and thus $(SX)^{o(1)}=X^{o(1)}$. Hence, the above bounds further simplify to

$$\Sigma_{2,i,j}\leqslant T^2X_j^{2/(k^2+2)}2^{i(1-1/(k^2+2))}X^{o(1)}.$$

Summing over i and j with $X_j\leqslant 2^{i\rho}$ we arrive at

$$\Sigma_2^{\leqslant}\leqslant T^2X^{o(1)}\sum_{i=1}^{J}\sum_{j:X_j\leqslant 2^{i\rho}}X_j^{2/(k^2+2)}2^{i(1-1/(k^2+2))},$$

and hence

$$\Sigma_2^{\leqslant}\leqslant T^2X^{1-(1-2\rho)/(k^2+2)}X^{o(1)}. \tag{4.25}$$

We next consider $\Sigma_2^{\geqslant}$. We begin our treatment of $\Sigma_2^{\geqslant}$ in a similar fashion to $\Sigma_2^{\leqslant}$. In particular, we use (4.17) and the assumption that (α,β) is admissible to obtain

$$\Sigma_{2,i,j}\leqslant 2^{i(2\beta+o(1))}X_j\sum_{X_j\leqslant r\leqslant X_{j+1}}\#\mathcal{S}_{i,j}(r)\sum_{\substack{d\mid r\\ d>Z_j}}\frac{1}{d^{3-2\alpha}}V\left(r/d\right), \tag{4.26}$$

as $i\to\infty$.

Using (4.19) and then rearranging the order of summation, the above reduces to

$$\Sigma_{2,i,j} \leqslant 2^{i(1+2\beta+o(1))} \sum_{X_j \leqslant r \leqslant X_{j+1}} \sum_{\substack{d|r \\ d>Z_j}} \frac{1}{d^{3-2\alpha}} V(r/d)$$
$$\leqslant 2^{i(1+2\beta+o(1))} \sum_{Z_j < d \leqslant X_{j+1}} \frac{1}{d^{3-2\alpha}} W_j(d),$$

where

$$W_j(d) = \sum_{X_j/d \leqslant r \leqslant X_{j+1}/d} V(r).$$

We see from the definition (4.15) that

$$W_j(d) = \sum_{1 \leqslant n_1, n_2 \leqslant T} \sum_{\substack{X_j/d \leqslant r \leqslant X_{j+1}/d \\ s_{n_1} \equiv s_{n_2} \bmod r}} 1 \leqslant \left(\frac{X_j}{d} + TS^{o(1)} \right) T,$$

and hence

$$\Sigma_{2,i,j} \leqslant 2^{i(1+2\beta+o(1))} T \left(X_j \sum_{Z_j < d \leqslant X_{j+1}} \frac{1}{d^{4-2a}} + TS^{o(1)} \sum_{Z_j \leqslant d \leqslant X_{j+1}} \frac{1}{d^{3-2\alpha}} \right)$$
$$\leqslant 2^{i(1+2\beta+o(1))} T \left(\frac{X_j}{Z_j^{3-2\alpha}} + \frac{TS^{o(1)}}{Z_j^{2-2a}} \right).$$

Since obviously $S \leqslant X^{O(1)}$, we can replace both $2^{o(i)}$ and $S^{o(1)}$ with $X^{o(1)}$. Recalling the choice of Z_j and the assumption (4.24), we get

$$\Sigma_{2,i,j} \ll \frac{2^{i(1+2\beta)} T}{\xi^{2(1-\alpha)} X_j^{2(1-\alpha)}} \left(\xi^{-1} + T \right) X^{o(1)} \leqslant \frac{2^{i(1+2\beta)} T^2}{\xi^{2(1-\alpha)} X_j^{2(1-\alpha)}} X^{o(1)}.$$

This implies that

$$\Sigma_2^{\geqslant} \leqslant \frac{1}{\xi^{2(1-\alpha)}} T^2 X^{o(1)} \sum_{i=1}^{J} \sum_{j: 2^{i\rho} \leqslant X_j \leqslant 2^i} \frac{2^{i(1+2\beta)}}{X_j^{2(1-\alpha)}}$$
$$\leqslant T^2 \frac{X^{1+2(\beta+\eta-\rho(1-\alpha))}}{\xi^{2(1-\alpha)}} X^{o(1)}. \tag{4.27}$$

Substituting the bounds (4.25) and (4.27) in (4.18), we see that

$$\Sigma_2 \leqslant \left(\frac{1}{X^{(1-2\rho)/(k^2+2)}} + \frac{X^{2(\beta-\rho(1-\alpha))}}{\xi^{2(1-\alpha)}} \right) T^2 X^{1+o(1)}. \tag{4.28}$$

4.4. Concluding the proof

Substituting (4.13) and (4.28) in (4.5), gives

$$W_\lambda(\Gamma,\mathcal{S};T,X,\Delta)\left(X+\xi S+\frac{T}{X^{(1-2\rho)/(k^2+2)}}+\frac{TX^{2(\beta-\rho(1-\alpha))}}{\xi^{2(1-\alpha)}}\right)TX^{1+o(1)}.$$

Let $\eta>0$ be a parameter and make the substitution

$$\rho=\frac{\beta+\eta}{1-\alpha}.$$

The above transforms into

$$W_\lambda(\Gamma,\mathcal{S};T,X,\Delta)\left(X+\xi S+\frac{T}{X^{(1-2(\beta+\eta)/(1-\alpha))/(k^2+2)}}+\frac{T}{\xi^{2(1-\alpha)}X^{2\eta}}\right)TX^{1+o(1)}.$$

Next we choose

$$\xi=\left(\frac{T}{SX^{2\eta}}\right)^{1/(3-2\alpha)},$$

to balance the second and fourth terms. This gives

$$W_\lambda(\Gamma,\mathcal{S};T,X,\Delta)\leqslant\left(X+\frac{S^{1-1/(3-2\alpha)}T^{1/(3-2\alpha)}}{X^{2\eta/(3-2\alpha)}}+\frac{T}{X^{(1-2(\beta+\eta)/(1-\alpha))/(k^2+2)}}\right)TX^{1+o(1)}.$$

We now note that the assumption (2.5) implies that

$$W_\lambda(\Gamma,\mathcal{S};T,X,\Delta)\left(X+\left(S^{2-2\alpha}TX^{-2\eta}\right)^{1/(3-2\alpha)}+\frac{T}{X^{\delta/(k^2+2)}}\right)TX^{1+o(1)},$$

which is the desired bound.

Finally, to complete the proof, it remains to note that (4.20) is satisfied by the assumption (2.7) and (4.24) is satisfied by (2.6).

5. Proof of Theorem 2.2

5.1. Initial transformations

As before, for each prime p we define the number a_p by (4.1). Taking $Z=X^{1/4}$ in Lemma 3.3 and recalling that t_p denotes the order of λ mod p, we have

$$V_\lambda(\Gamma,\mathcal{S};T,X)\leqslant X^{1/2}T^2+V_\lambda(\Gamma,\mathcal{S};T,X,X^{1/4})=X^{1/2}T^2+\sum_{p\in\mathcal{E}_{X^{1/4}}(X)}|\sigma_p(a_p)|^2. \tag{5.1}$$

We define the sequence of numbers X_j, as in (4.8) with $\Delta=X^{1/4}$. We also define the sets $\mathcal{R}_j$ as in (4.9) for $j=1,\dots,J$ with J given by (4.7).

Hence, partitioning summation over p in (5.1) according to $\mathcal{R}_j$ gives,

$$V_\lambda(\Gamma,\mathcal{S};T,X)\ll X^{1/2}T^2+\sum_{j=1}^{J}W_j,$$

where

$$W_j=\sum_{p\in\mathcal{R}_j}|\sigma_p(a_p)|^2.$$

We define the number Y by

$$Y = \frac{X^{3/4}S^{1/4}}{T^{1/4}}, \tag{5.2}$$

and let I be the largest integer j with $X_j \leqslant Y$ (since $S \geqslant T$ we obviously have $Y \geqslant X^{3/4} > X^{1/4}$ so I is correctly defined).

We now further partition the summation over j and re-write (5.1) as

$$V_\lambda(\Gamma, \mathcal{S}; T, X) \leqslant X^{1/2}T^2 + W^{\leqslant} + W^{\geqslant}, \tag{5.3}$$

where

$$W^{\leqslant} = \sum_{j=1}^{I} W_j \qquad \text{and} \qquad W^{\geqslant} = \sum_{j=I+1}^{J} W_j. \tag{5.4}$$

5.2. The sum $W^{\leqslant}$

We fix some j with $X^{1/4} \leqslant X_j < Y$. Considering W_j, we define the sets

$$\mathcal{V}_j(r) = \{p \in \mathcal{R}_j \ : \ t_p = r\}, \tag{5.5}$$

so that

$$W_j = \sum_{X_j < r \leqslant 2X_j} U_{j,r}, \tag{5.6}$$

where $U_{j,r}$ is given by

$$U_{j,r} = \sum_{p \in \mathcal{V}_j(r)} |\sigma_p(a_p)|^2.$$

For each $p \in \mathcal{V}_j(r)$ we define the complex number $c_{j,r,p}$ by

$$c_{j,r,p} = \frac{\overline{\sigma}_p(a_p)}{\left(\sum_{p \in \mathcal{V}_j(r)} |\sigma_p(a_p)|^2\right)^{1/2}},$$

so that

$$\sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 = 1, \tag{5.7}$$

and writing

$$U^*_{j,r} = \sum_{p \in \mathcal{V}_j(r)} \sum_{1 \leqslant n \leqslant T} c_{j,r,p}\gamma_n \, \mathbf{e}_p(a_p\lambda^{s_n}),$$

we see that

$$|U^*_{j,r}| = U^{1/2}_{j,r}. \tag{5.8}$$

We have

$$U_{j,r}^* = \sum_{0 \leqslant x < r} \sum_{p \in \mathcal{V}_j(r)} b_r(x) c_{j,r,p}\, \mathbf{e}_p(a_p \lambda^x),$$

where

$$b_r(x) = \sum_{\substack{1 \leqslant n \leqslant T \\ s_n \equiv x \bmod r}} \gamma_n, \tag{5.9}$$

and hence by the Cauchy–Schwarz inequality

$$|U_{j,r}^*|^2 \leqslant \sum_{0 \leqslant x < r} |b_r(x)|^2 \sum_{0 \leqslant x < r} \left| \sum_{p \in \mathcal{V}_j(r)} c_{j,r,p}\, \mathbf{e}_p(a_p \lambda^x) \right|^2.$$

Expanding the square and interchanging summation gives

$$|U_{j,r}^*|^2 \leqslant \sum_{0 \leqslant x < r} |b_r(x)|^2 \sum_{p_1, p_2 \in \mathcal{V}_j(r)} |c_{j,r,p_1}||c_{j,r,p_2}| \left| \sum_{0 \leqslant x < r} \mathbf{e}_{p_1 p_2}((a_{p_1} p_2 - a_{p_2} p_1)\lambda^x) \right|,$$

which implies that

$$\begin{aligned} |U_{j,r}^*|^2 \leqslant\ & r \sum_{0 \leqslant x < r} |b_r(x)|^2 \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 \\ & + \sum_{0 \leqslant x < r} |b_r(x)|^2 \sum_{\substack{p_1, p_2 \in \mathcal{V}_j(r) \\ p_1 \neq p_2}} |c_{j,r,p_1}||c_{j,r,p_2}| \max_{(a, p_1 p_2) = 1} \left| \sum_{0 \leqslant x < r} \mathbf{e}_{p_1 p_2}(a \lambda^x) \right|. \end{aligned}$$

Since

$$t_{p_1} = t_{p_2} = r,$$

the set

$$H = \{\ \lambda^x \bmod p_1 p_2\ :\ 0 \leqslant x < r\ \},$$

is a subgroup of $\mathbb{Z}_{p_1 p_2}^*$ and from the inequalities

$$r \geqslant X^{1/4} > (p_1 p_2)^{1/8},$$

we see that the conditions of Lemma 3.4 are satisfied. An application of Lemma 3.4 gives

$$|U_{j,r}^*|^2 \leqslant r \sum_{0 \leqslant x < r} |b_r(x)|^2 \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 + \sum_{0 \leqslant x < r} |b_r(x)|^2 \left(\sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}| \right)^2 r^{1-\varrho},$$

which by the Cauchy–Schwarz inequality implies that

$$|U_{j,r}^*|^2 \leqslant \sum_{0 \leqslant x < r} |b_r(x)|^2 \sum_{p \in \mathcal{V}_j(r)} |c_{j,r,p}|^2 \left(r + |\mathcal{V}_j(r)| r^{1-\varrho} \right),$$

and hence by (5.7)

$$|U_{j,r}^*|^2 \leqslant \sum_{0\leqslant x<r} |b_r(x)|^2 \left(r + |\mathcal{V}_j(r)| r^{1-\varrho}\right).$$

Since

$$|\mathcal{V}_j(r)| \leqslant \frac{X}{r}, \tag{5.10}$$

we get

$$|U_{j,r}^*|^2 \leqslant \left(r + \frac{X}{r^\varrho}\right) \sum_{0\leqslant x<r} |b_r(x)|^2. \tag{5.11}$$

Recalling (5.9) and the assumption each $|\gamma_n| \leqslant 1$, we see that

$$\sum_{0\leqslant x<r} |b_r(x)|^2 = \sum_{1\leqslant n_1,n_2\leqslant T} \gamma_{n_1}\overline{\gamma}_{n_2} \sum_{\substack{0\leqslant x<r \\ s_{n_1}\equiv x \bmod r \\ s_{n_2}\equiv x \bmod r}} 1 = V(r),$$

where $V(r)$ is defined by (4.15). By (5.11) we have

$$|U_{j,r}^*|^2 \leqslant V(r)\left(r + \frac{X}{r^\varrho}\right),$$

and hence by (5.8)

$$|U_{j,r}| \leqslant V(r)\left(r + \frac{X}{r^\varrho}\right).$$

Combining the above with (5.6) gives

$$W_j \leqslant \sum_{X_j<r\leqslant 2X_j} V(r)\left(X_j + \frac{X}{X_j^\varrho}\right). \tag{5.12}$$

As in the proof of Theorem 2.1, see (4.23), we have

$$\sum_{X_j<r\leqslant 2X_j} V(r) \ll X_j T + \sum_{\substack{1\leqslant n_1,n_2\leqslant T \\ n_1\neq n_2}} \sum_{\substack{X_j<r\leqslant 2X_j \\ s_{n_1}\equiv s_{n_2} \bmod r}} 1 \leqslant (X_j + TS^{o(1)})T \leqslant T^{2+o(1)},$$

where we have used the assumption $S \leqslant T^2$ and $T > X$ as otherwise Theorem 2.2 is trivial. Substituting the above into (5.12) gives

$$W_j \leqslant \left(X_j + \frac{X}{X_j^\varrho}\right) T^{2+o(1)},$$

and hence by (5.4)

$$W^{\leqslant} \leqslant \left(Y + XX_1^{-\varrho}\right) T^{2+o(1)} \leqslant \left(Y + X^{1-\varrho/4}\right) T^{2+o(1)}. \tag{5.13}$$

5.3. The sum $W^{\geqslant}$

We fix some j with $Y \leqslant X_j \leqslant X$ and arrange W_j as follows

$$W_j = \sum_{p\in\mathcal{R}_j} |\sigma_p(a_p)|^2 \leqslant T \sum_{p\in\mathcal{R}_j} |\sigma_p(a_p)|\,,$$

and hence there exists some sequence of complex numbers $c_{j,p}$ with $|c_{j,p}| = 1$ such that

$$W_j \leqslant T \sum_{p\in\mathcal{R}_j} \sum_{1\leqslant n\leqslant T} c_{j,p}\gamma_n\, \mathbf{e}_p(a_p\lambda^{s_n}).$$

An application of the Cauchy–Schwarz inequality gives

$$W_j^2 \leqslant T^3 \sum_{1\leqslant n\leqslant T} \left|\sum_{p\in\mathcal{R}_j} c_{j,p}\, \mathbf{e}_p(a_p\lambda^{s_n})\right|^2.$$

Since the sequence s_n is increasing and bounded by S, we see that

$$W_j^2 \leqslant T^3 \sum_{1\leqslant s\leqslant S} \left|\sum_{p\in\mathcal{R}_j} c_{j,p}\, \mathbf{e}_p(a_p\lambda^{s})\right|^2 \ll \frac{T^3}{S} \sum_{-S\leqslant r,s\leqslant S} \left|\sum_{p\in\mathcal{R}_j} c_{j,p}\, \mathbf{e}_p(a_p\lambda^{r+s})\right|^2,$$

so that writing

$$\mathbf{W}_j = \sum_{-S\leqslant r,s\leqslant S} \left|\sum_{p\in\mathcal{R}_j} c_{j,p}\, \mathbf{e}_p(a_p\lambda^{r+s})\right|^2,$$

the above implies

$$W_j^2 \leqslant \frac{T^3}{S}\mathbf{W}_j. \tag{5.14}$$

Considering $\mathbf{W}_j$, expanding the square and interchanging summation gives

$$\begin{aligned}\mathbf{W}_j &\leqslant \sum_{p_1,p_2\in\mathcal{R}_j} \left|\sum_{-S\leqslant r,s\leqslant S} \mathbf{e}_{p_1p_2}((a_{p_1}p_2 - a_{p_2}p_1)\lambda^{r+s})\right| \\ &\leqslant S^2|\mathcal{R}_j| + \sum_{\substack{p_1,p_2\in\mathcal{R}_j\\ p_1\neq p_2}} \sum_{-S\leqslant r\leqslant S} \left|\sum_{-S\leqslant s\leqslant S} \mathbf{e}_{p_1p_2}(a_{p_1p_2}\lambda^{r+s})\right|,\end{aligned}$$

for some integers $a_{p_1p_2}$ with $\gcd(a_{p_1p_2}, p_1p_2) = 1$. By (5.5) and (5.10)

$$|\mathcal{R}_j| = \sum_{X_j<r\leqslant 2X_j} |\mathcal{V}_j(r)| \ll X,$$

and hence

$$\mathbf{W}_j \ll S^2X + \sum_{\substack{p_1,p_2\in\mathcal{R}_j\\ p_1\neq p_2}} Z(p_1,p_2), \tag{5.15}$$

where

$$Z(p_1,p_2) = \sum_{-S\leqslant r\leqslant S}\left|\sum_{-S\leqslant s\leqslant S}\mathbf{e}_{p_1p_2}(a_{p_1p_2}\lambda^{r+s})\right|.$$

Considering $Z(p_1,p_2)$, by the Cauchy–Schwarz inequality, we have

$$\begin{aligned} Z(p_1,p_2)^2 &\ll S\sum_{-S\leqslant r\leqslant S}\left|\sum_{-S\leqslant s\leqslant S}\mathbf{e}_{p_1p_2}(a_{p_1p_2}\lambda^r\lambda^s)\right|^2\\ &\ll S\left(1+\frac{S}{\operatorname{ord}_{p_1p_2}(\lambda)}\right)\sum_{u \bmod p_1p_2}\left|\sum_{-S\leqslant s\leqslant S}\mathbf{e}_{p_1p_2}(a_{p_1p_2}u\lambda^s)\right|^2. \end{aligned}$$

Now, since

$$\begin{aligned} \sum_{u \bmod p_1p_2}\left|\sum_{-S\leqslant s\leqslant S}\mathbf{e}_{p_1p_2}(a_{p_1p_2}u\lambda^s)\right|^2 &= \sum_{-S\leqslant s_1,s_2\leqslant S}\sum_{u \bmod p_1p_2}\mathbf{e}_{p_1p_2}(a_{p_1p_2}u(\lambda^{s_1}-\lambda^{s_2}))\\ &\ll p_1p_2S\left(1+\frac{S}{\operatorname{ord}_{p_1p_1}(\lambda)}\right), \end{aligned}$$

we see that

$$Z(p_1,p_2)^2 \ll p_1p_2S^2\left(1+\frac{S}{\operatorname{ord}_{p_1p_1}(\lambda)}\right)^2 \leqslant X^2S^2\left(1+\frac{S}{\operatorname{ord}_{p_1p_2}(\lambda)}\right)^2.$$

Since $t_{p_1}, t_{p_2} \geqslant X_j$, we have

$$\operatorname{ord}_{p_1p_2}(\lambda) = \operatorname{lcm}(t_{p_1},t_{p_2}) = \frac{t_{p_1}t_{p_2}}{\gcd(t_{p_1},t_{p_2})} \geqslant \frac{X_j^2}{\gcd(p_1-1,p_2-1)},$$

which implies

$$Z(p_1,p_2)^2 \leqslant X^2S^2\left(1+\frac{\gcd(p_1-1,p_2-1)S}{X_j^2}\right)^2,$$

which after substituting the above in (5.15) gives

$$\mathbf{W}_j \ll S^2X + XS\sum_{\substack{p_1,p_2\in\mathcal{R}_j\\ p_1\neq p_2}} 1 + \frac{XS^2}{X_j^2}\sum_{\substack{p_1,p_2\in\mathcal{R}_j\\ p_1\neq p_2}}\gcd(p_1-1,p_2-1).$$

We have

$$\sum_{\substack{p_1,p_2\in\mathcal{R}_j\\ p_1\neq p_2}} 1 \leqslant |\mathcal{R}_j|^2 \ll X^2,$$

and

$$\sum_{\substack{p_1,p_2\in\mathcal{R}_j\\ p_1\neq p_2}} \gcd(p_1-1,p_2-1) \ll \sum_{1\leqslant x_1<x_2\leqslant X} \gcd(x_1,x_2) = \sum_{1\leqslant d\leqslant X} d \sum_{\substack{1\leqslant x_1<x_2\leqslant X/d\\ (x_1,x_2)=1}} 1 \ll X^{2+o(1)},$$

so that

$$\mathbf{W}_j \ll S^2X + SX^3 + \frac{S^2X^{3+o(1)}}{X_j^2}.$$

Combining the above with (5.14) gives

$$W_j^2 \ll SXT^3 + X^3T^3 + \frac{SX^{3+o(1)}T^3}{X_j^2},$$

which simplifies to

$$W_j \leqslant X^{3/2}T^{3/2}\left(1+\frac{S^{1/2}}{X_j}\right)X^{o(1)},$$

since we may assume $S \leqslant X^{2+o(1)}$. By (5.4) we have

$$W^{\geqslant} \ll X^{3/2}T^{3/2}\left(1+\frac{S^{1/2}}{Y}\right)X^{o(1)}. \tag{5.16}$$

5.4. Concluding the proof

Substituting (5.13) and (5.16) in (5.3) we derive

$$V_\lambda(\Gamma,\mathcal{S};T,X) \leqslant X^{1/2}T^2 + \left(Y+X^{1-\varrho}\right)T^{2+o(1)} + X^{3/2}T^{3/2}\left(1+\frac{S^{1/2}}{Y}\right)X^{o(1)}.$$

Recalling the choice of Y in (5.2) the above simplifies to

$$V_\lambda(\Gamma,\mathcal{S};T,X) \leqslant \left(X^{1/2}T^2 + X^{1-\varrho/4}T^2 + X^{3/2}T^{3/2} + X^{3/4}T^{7/4}S^{1/4}\right)X^{o(1)},$$

and the result follows with $\rho = \varrho/4$ (as clearly $\varrho \leqslant 1$ and thus $\rho < 1/2$).

6. Proof of Theorem 2.3

First we note that without loss of generality we may assume the binary digits of a are zeros on all positions $j \in \mathcal{S}$.

For a prime p, let $N_p(a;\mathcal{S})$ be the number of $z \in \mathcal{N}(a;\mathcal{S})$ with $p \mid z$. One can easily see that $N_p(a;\mathcal{S})$ is the number of solutions to the congruence

$$a + \sum_{n=1}^{T} d_n 2^{s_n} \equiv 0 \bmod p, \qquad d_n \in \{0,1\},\ n = 1,\dots,T.$$

We now proceed similarly to the proof of [15, Theorem 18.1]. Using the orthogonality of exponential functions, we write

$$\begin{aligned} N_p(a;\mathcal{S}) &= \frac{1}{p}\sum_{b=0}^{p-1}\sum_{(d_1,\dots,d_T)\in\{0,1\}^T} \mathbf{e}_p\left(b\left(\sum_{n=1}^{T} d_n 2^{s_n}+a\right)\right) \\ &= 2^T p^{-1} + \frac{1}{p}\sum_{b=1}^{p-1}\sum_{(d_1,\dots,d_T)\in\{0,1\}^T} \mathbf{e}_p\left(b\left(\sum_{n=1}^{T} d_j 2^{s_n}+a\right)\right) \\ &= 2^T p^{-1} + \frac{1}{p}\sum_{b=1}^{p-1} \mathbf{e}_p(ab)\prod_{n=1}^{T}\left(1+\mathbf{e}_p\left(b2^{s_n}\right)\right). \end{aligned}$$

Therefore,

$$\left|N_{n,p}(a) - 2^T p^{-1}\right| \leqslant Q_p, \tag{6.1}$$

where

$$Q_p = \max_{b=1,\dots,p-1}\left|\prod_{n=1}^{T}\left(1+\mathbf{e}_p\left(b2^{s_n}\right)\right)\right|.$$

Using [15, Equation (18.2)] we write

$$Q_p \leqslant \exp\left(O(M_p\log(T/M_p+1))\right), \tag{6.2}$$

where

$$M_p = \max_{\gcd(b,p)=1}\left|\sum_{n\leqslant T}\mathbf{e}_p(a\lambda^{s_n})\right|.$$

Now, by Theorem 2.2 if we fix some $\varepsilon_0 > 0$, then there is some $\kappa > 0$ such that if

$$X = T^{1/(1+\varepsilon_0)}, \quad \Delta = X^{1/2} \qquad \text{and} \qquad S \leqslant X^{2-\varepsilon_0},$$

then we have

$$\sum_{p\in\mathcal{E}_\Delta(X)} M_p^2 \leqslant T^2 X^{1-\kappa}.$$

Since $S \leqslant T^{2-\varepsilon}$, to satisfy the above conditions, it is enough to define ε_0 by the equation

$$\frac{2-\varepsilon_0}{1+\varepsilon_0} = 2-\varepsilon$$

or, more explicitly,

$$\varepsilon_0 = \frac{\varepsilon}{3-\varepsilon}.$$

Combining this with (2.15), we see that for all but $o(X/\log X)$ primes $p \leqslant X$ we have $M_p \leqslant TX^{-\kappa/3}$. For each of these primes p, a combination of (6.1) and (6.2) implies that $N_p(a;\mathcal{S}) > 0$ (provided that p is large enough), which concludes the proof.

7. Possible improvements

We note that one can get an improvement of Theorem 2.1 by using a combination of different admissible pairs depending on the range of d in our treatment of the sum (4.17) in and thus making the choice of α and β in (4.26) dependent on i and j.

In particular, one can use the admissible pairs (2.1), (2.2), (2.3) and (2.4) as well the admissible pairs given by Konyagin [14] and Shteinikov [23] for small values of d in (4.17).

Acknowledgments

This work was partially supported by the NSF Grant DMS 1600154 (for M.-C. C.) and by the ARC Grant DP170100786 (for I. S.).

References

[1] W.D. Banks, M.Z. Garaev, F. Luca, I.E. Shparlinski, Uniform distribution of fractional parts related to pseudoprimes, Canad. J. Math. 61 (2009) 481–502.
[2] J. Bourgain, Prescribing the binary digits of primes, Israel J. Math. 194 (2013) 935–955.
[3] J. Bourgain, Prescribing the binary digits of primes, II, Israel J. Math. 206 (2015) 165–182.
[4] J. Bourgain, M.-C. Chang, Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors, Geom. Funct. Anal. 16 (2006) 327–366.
[5] J. Bourgain, A.A. Glibichuk, S.V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, J. Lond. Math. Soc. 73 (2006) 380–398.
[6] R. Dietmann, C. Elsholtz, I.E. Shparlinski, Prescribing the binary digits of squarefree numbers and quadratic residues, Trans. Amer. Math. Soc. 369 (12) (2017) 8369–8388.
[7] M. Drmota, R. Tichy, Sequences, Discrepancies and Applications, Lecture Notes in Mathematics, vol. 1651, Springer-Verlag, New York, 2000.
[8] P. Erdős, M.R. Murty, On the order of a mod p, in: Number Theory, in: CRM Proc. Lecture Notes, vol. 19, American Mathematical Society, Providence, PI, 1999, pp. 87–97.
[9] M.Z. Garaev, The large sieve inequality for the exponential sequence $\lambda^{O(n^{15/14+o(1)})}$ modulo primes, Canad. J. Math. 61 (2009) 336–350.
[10] M.Z. Garaev, I.E. Shparlinski, The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes, Int. Math. Res. Not. 39 (2005) 2391–2408.
[11] G. Harman, I. Katai, Primes with preassigned digits II, Acta Arith. 133 (2008) 171–184.
[12] D.R. Heath-Brown, S.V. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Quart. J. Mech. 51 (2000) 221–235.
[13] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc., Providence, RI, 2004.
[14] S.V. Konyagin, Bounds of exponential sums over subgroups and Gauss sums, in: Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications, Moscow Lomonosov State Univ., Moscow, 2002, pp. 86–114 (in Russian).
[15] S.V. Konyagin, I.E. Shparlinski, Character Sums with Exponential Functions and Their Applications, Cambridge Univ. Press, Cambridge, 1999.
[16] N.M. Korobov, On the distribution of digits in periodic fractions, Mat. Sb. 89 (1972) 654–670 (in Russian).
[17] E. Kowalski, The Large Sieve and Its Applications: Arithmetic Geometry, Random Walks and Discrete Groups, Cambridge Tracts in Math., vol. 175, Cambridge Univ. Press, Cambridge, 2008.
[18] O. Ramaré, Arithmetical Aspects of the Large Sieve Inequality, Harish-Chandra Research Institute Lecture Notes, vol. 1, Hindustan Book Agency, New Delhi, 2009.
[19] I.D. Shkredov, Some new inequalities in additive combinatorics, Mosc. J. Comb. Number Theory 3 (2013) 237–288.
[20] I.D. Shkredov, On exponential sums over multiplicative subgroups of medium size, Finite Fields Appl. 30 (2014) 72–87.
[21] I.E. Shparlinski, Exponential sums and prime divisors of sparse integers, Period. Math. Hungar. 57 (2008) 93–99.
[22] I.E. Shparlinski, Bilinear sums with exponential functions, Proc. Amer. Math. Soc. 137 (2009) 2217–2224.
[23] Y.N. Shteinikov, Estimates of trigonometric sums over subgroups and some of their applications, Mat. Zametki 98 (2015) 606–625 (in Russian).