1. Introduction and statement of the main results

Let \( \Gamma \) be a semigroup of \( d \times d \) nonsingular integer matrices, and consider the action of \( \Gamma \) on the torus \( T^d \). We assume throughout that the action is strongly irreducible: there is no subtorus invariant under a finite index subsemigroup of \( \Gamma \).

The strong irreducibility assumption in particular implies that \( \Gamma \) acts ergodically on \( T^d \) (equipped with the Lebesgue measure \( m \)). Therefore the \( \Gamma \)-orbit of Lebesgue almost every \( x \in T^d \) is dense and in an appropriate sense even becomes equidistributed. However, when \( \Gamma \) is cyclic, there is a set of full Hausdorff dimension of exceptional points \( x \) for which \( \Gamma \cdot x \) fails to be dense.

When \( \Gamma \) is bigger, the distribution of individual \( \Gamma \)-orbits can be expected to be much more restrictive. An important result in this direction is due to Furstenberg, who showed for \( d = 1 \) (in which case \( \Gamma \prec \mathbb{Z}^\times \) and in particular abelian) that if \( \Gamma \) is not virtually cyclic, \( \Gamma \cdot x \) is dense for all irrational \( x \in \mathbb{T} \), and moreover for any open \( U \subset \mathbb{T} \) there are only finitely many rational points whose \( \Gamma \)-orbits avoids \( U \). This has been extended by Berend \[1\] to actions of abelian semigroups of toral endomorphisms on \( T^d \). However, in both cases, while the orbit closure of individual orbits are very restricted, there is some flexibility on how such an orbit distributes; for example consider the orbit of \( x = \sum_{k=1}^{\infty} 2^{-k!} \in T \) under the semigroup \( \Gamma = \langle 2, 3 \rangle \).

In this paper we consider the action of semigroups \( \Gamma \) which satisfy the following three conditions:

\begin{itemize}
  \item[(\( \Gamma \)-0)] \( \Gamma \prec \text{SL}_d(\mathbb{R}) \),
  \item[(\( \Gamma \)-1)] \( \Gamma \) acts strongly irreducibly on \( \mathbb{R}^d \),
  \item[(\( \Gamma \)-2)] \( \Gamma \) contains a proximal element: there is some \( g \in \Gamma \) with a dominant eigenvalue which is a simple root of its characteristic polynomial.
\end{itemize}

Note that (\( \Gamma \)-1) is substantially stronger than the requirement we have already imposed that \( \Gamma \) acts strongly irreducibly on \( T^d \). In particular, for \( d > 1 \) an abelian semigroup never satisfies condition (\( \Gamma \)-1); indeed, the group generated by a semigroup satisfying (\( \Gamma \)-1) is nonamenable. Assumption (\( \Gamma \)-2) is a technical condition which is in particular satisfied when \( \Gamma \) is a Zariski dense semigroup of \( \text{SL}_d(\mathbb{Z}) \) \[16\].
While a substantial part of the argument works without assumption (Γ-0), without it simple counterexamples can be given to Theorem A below, similar to the example above of a nonequidistributed orbit for the semigroup \( \langle 2, 3 \rangle \).

Under these (and more general) conditions, R. Muchnik [27] and Y. Guivarc’h and A. Starkov [19] proved the analog of the theorems of H. Furstenberg and D. Berend, namely that for any \( x \in T^d \) with at least one irrational coordinate \( \Gamma \cdot x \) is dense, and moreover that there are only finitely many rational \( x \) whose orbits avoid a given open neighborhood in \( T^d \).

We study the quantitative distribution properties of \( \Gamma \)-orbits. Since \( \Gamma \) is not amenable, we do this by considering a random walk on \( \Gamma \cdot x \) corresponding to a probability measure \( \nu \) on \( \Gamma \). We will assume that \( \nu \) satisfies the moment condition
\[
(1.1) \quad \sum_{g \in \Gamma} \nu(g) \|g\|^{\epsilon} < \infty \quad \text{for some } \epsilon > 0.
\]

Given a probability measure \( \nu \) on \( \Gamma \) and a probability measure \( \mu \) on \( T^d \), the convolution \( \nu * \mu \in T^d \) is
\[
\nu * \mu = \sum_{g \in \Gamma} \nu(g) g * \mu.
\]

Furstenberg [14] has shown that under assumption (Γ-1) the top Liapunov exponent defined by
\[
\lambda_1(\nu) = \lim_{n \to \infty} \frac{1}{n} \log \|g_1 g_2 \cdots g_n\|, \quad \nu^{\otimes n} \text{-a.s.,}
\]

is positive. Assumption (Γ-2) guarantees that this Liapunov exponent is simple [16,17]. Our main theorem is the following:

**Theorem A.** Let \( \Gamma < SL_d(\mathbb{R}) \) satisfy (Γ-1) and (Γ-2) above, and let \( \nu \) be a probability measure supported on a set of generators of \( \Gamma \) satisfying (1.1). Then for any \( 0 < \lambda < \lambda_1(\nu) \) there is a constant \( C = C(\nu, \lambda) \) so that if for a point \( x \in T^d \) the measure \( \mu_n = \nu^{\otimes n} * \delta_x \) satisfies that for some \( a \in \mathbb{Z}^d \backslash \{0\} \)
\[
|\hat{\mu}_n(a)| > t > 0, \quad \text{with} \quad n > C \cdot \log \left( \frac{2 \|a\|}{t} \right),
\]
then \( x \) admits a rational approximation \( p/q \) for \( p \in \mathbb{Z}^d \) and \( q \in \mathbb{Z}_+ \) satisfying
\[
(1.2) \quad \left\| x - \frac{p}{q} \right\| < e^{-\lambda n} \quad \text{and} \quad |q| < \left( \frac{2 \|a\|}{t} \right)^C.
\]

This theorem has several corollaries:

**Corollary B.** Let \( \Gamma \) and \( \nu \) be as in Theorem A, and let \( x \in T^d \backslash (\mathbb{Q}/\mathbb{Z})^d \). Then the measures \( \mu_n = \nu^{\otimes n} * \delta_x \) converge to the Haar measure \( m \) on \( T^d \) in weak* topology.

This answers affirmatively a question of Guivarc’h in a private communication and should be contrasted with the example given above for the case of \( d = 1 \). We also have the following more quantitative equidistribution results:

**Corollary C.** Let \( \Gamma \) and \( \nu \) be as in Theorem A, and let \( x \in T^d \) and \( \mu_n = \nu^{\otimes n} * \delta_x \). Then there are \( c_1, c_2 \) depending only on \( \nu \) so that the following holds:

1. Assume \( x \) is Diophantine generic in the sense that for some \( M \) and \( Q \)
\[
(1.3) \quad \left\| x - \frac{p}{q} \right\| > q^{-M} \quad \text{for all integers } q \geq Q \text{ and } p \in \mathbb{Z}^d.
\]
Then for $n > c_1 \log Q$

$$\max_{b \in \mathbb{Z}^d, 0 < \|b\| < B} |\widehat{\mu}_n(b)| < Be^{-c_2n/M}.$$  

(2) Assume $x \notin (\mathbb{Q}/\mathbb{Z})^d$. Then there is a sequence $n_i \to \infty$ along which

$$\max_{b \in \mathbb{Z}^d, 0 < \|b\| < e^{c_2n_i}} |\widehat{\mu}_{n_i}(b)| < e^{c_2n_i}.$$

Our next corollary answers a question raised by Furstenberg in [12]. Recall that a measure $\mu$ is said to be $\nu$-stationary if $\nu \ast \mu = \mu$.

If the support of $\nu$ generates a semigroup $\Gamma$, any $\Gamma$-invariant probability measure is $\nu$-stationary for any probability measure $\nu$ on $\Gamma$, but the converse (even for a fixed $\nu$) is not true in general. Following Furstenberg ([12]), we say that an action $\Gamma \curvearrowright X$ is $\nu$-stiff if any $\nu$-stationary measure is $\Gamma$-invariant.

In his paper [12] Furstenberg shows that for carefully chosen $\nu$ on $\text{SL}_d(\mathbb{Z})$, namely probability measures $\nu$ so that the corresponding stationary measure on the boundary of $\text{SL}_d(\mathbb{R})$ is absolutely continuous with respect to Lebesgue, the action of $\text{SL}_d(\mathbb{Z})$ on $T^d$ is $\nu$-stiff. He then suggests that this should be true for any $\nu$ whose support generates $\text{SL}_d(\mathbb{Z})$. The following corollary of our main theorem confirms Furstenberg’s insight:

**Theorem D.** Let $\Gamma < \text{SL}_d(\mathbb{R})$ be a semigroup satisfying (Γ-1) and (Γ-2) above, and let $\nu$ be a probability measure supported on a set of generators of $\Gamma$ satisfying (1.1). Then any $\nu$-stationary measure $\mu$ on $T^d$ is a convex combination of the Haar measure on $T^d$ and atomic measures supported by rational points. In particular, for such $\nu$ the action of $\Gamma$ on $T^d$ is $\nu$-stiff.

The results of this paper have been announced in [6]. Since then an alternative, ergodic theoretic, approach to Theorem D was discovered by Y. Benoist and J. F. Quint [2]. This approach has the advantage of being more general; in particular, Benoist and Quint have been able to prove Theorem D without making the assumption (Γ-2). However their ergodic theoretic argument is not quantitative, certainly not in the sense of Theorem A. It also does not give equidistribution of $\nu^\ast n \ast \delta_x$ as in Corollary B.

2. Deduction of corollaries from Theorem A

In this short section, we deduce Corollaries E and C from Theorem A. The deduction of Theorem D from Theorem A, or more precisely from the closely related Proposition 3.1, is given at the beginning of the next section.

**Proof of Corollary E given Theorem A.** Let $x \in T^d \setminus (\mathbb{Q}/\mathbb{Z})^d$. Suppose that the measures $\mu_n = \nu^\ast n \ast \delta_x$ fail to converge to the Haar measure $m$. Then by Weyl’s equidistribution criterion it follows that for some $a \in T^d \setminus \{0\}$ and some sequence $n_i \to \infty$

$$|\widehat{\mu}_{n_i}(a)| > t > 0 \quad \text{for all } i.$$

It follows from Theorem A that there is a sequence of rational approximations $\frac{p_i}{q_i}$ tending to $x$ with $q_i$ uniformly bounded—which of course is only possible if $x$ is rational.

□
Proof of Corollary A. We first prove assertion (1) of the corollary. Let $x$ be Diophantine generic in the sense of (1.3). Suppose that $|\hat{\mu}_n(b)| > t/B$ for some $b \in \mathbb{Z}^d$ with $0 < ||b|| < B$. Then as long as

$$t > \frac{1}{2} e^{-n/C}$$

for $C = C(\nu, \lambda_1/2)$ as in Theorem A by (1.2) there are $p \in \mathbb{Z}^d$, $q \in \mathbb{Z}_+$ so that

$$\left| x - \frac{p}{q} \right| < e^{-\lambda_1 n/2} \quad \text{and} \quad 1 < q < (2t^{-1})^C.$$ 

Chose $c_1$ so that $e^{-\lambda_1 n/2} < Q^{-2M}$ if $n \geq c_1 \log Q$; then if $q < Q$, we would have that $\left| x - \frac{p}{q} \right| < (Qq)^{-M}$ in contradiction to (1.3). It follows (using (1.3) once again) that if $n \geq c_1 \log Q$,

$$e^{-\lambda_1 n/2} > q^{-M} > C^t t^{-MC}.$$ 

From (2.1) and (2.2) we now conclude that

$$t \leq C^t \max(e^{-n/C}, e^{-\lambda_1 n/2MC}),$$

establishing Corollary A part(1).

Suppose now that for some $x \notin (Q/\mathbb{Z})^d$ part (2) of the corollary does not hold, i.e., that for every $n$ there is a $b_n \in \mathbb{Z}^d$ so that

$$|\hat{\mu}_n(b_n)| \geq e^{-c_2 n} \quad \text{and} \quad ||b_n|| < e^{c_2 n}.$$ 

Then by Theorem A as long as $2Cr < 1$ and $n$ is large enough, there is a sequence of rational points $\frac{p_n}{q_n}$ so that

$$\left| x - \frac{p_n}{q_n} \right| < e^{-\lambda_1 n/2} \quad \text{and} \quad |q_n| < 2Ce^{c_2 Cn}.$$ 

Since $x$ is irrational, the sequence $q_n$ is not eventually constant, so there are arbitrarily large $n$ for which $\frac{p_n}{q_n} \neq \frac{p_{n+1}}{q_{n+1}}$. But then (2.3) applied for both $n, n+1$ gives

$$2^{-2C} e^{-4C c_2} \leq (q_n q_{n+1})^{-1} \leq \left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| \leq 2e^{-\lambda_1 n/2},$$

which is a contradiction for large $n$ if $8C c_2 < \lambda_1$. \qed

3. Outline of the Proof

Given a positive integer $Q$, let

$$R_Q = \bigcup_{q \leq Q} \left\{ \left( \frac{p_1}{q}, \ldots, \frac{p_d}{q} \right) \in T^d : p_1, \ldots, p_d \in \{0, \ldots, q-1\} \right\}$$

denote the set of rational points on the torus with denominators $q \leq Q$. For $r > 0$ let $W_{Q,r} = \bigcup_{x \in R_Q} B_{x,r}$ denote the $r$-neighborhood of $R_Q$. We prove Theorem A by establishing the following:

**Proposition 3.1.** Let $\Gamma$ and $\nu$ be as in Theorem A $0 < \lambda < \lambda_1(\nu)$. Then for some constant $C$ depending on $\nu, \lambda$ the following holds: for any probability measure $\mu_0$ on $\mathbb{T}^d$, if $\mu_n = \nu^{*n} * \mu_0$ has a nontrivial Fourier coefficient $a \in \mathbb{Z}^d \setminus \{0\}$

$$|\hat{\mu}_n(a)| > t, \quad \text{with} \quad n > C \cdot \log(\frac{2 ||a||}{t}),$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
then

\[ \mu_0(W_{Q,e^{-\lambda n}}) > \left( \frac{t}{2} \right)^C \text{ where } Q = \left( \frac{2\|a\|}{t} \right)^C. \]

By specializing to the case of \( \mu_0 = \delta_x \), we get Theorem A since

\[ \delta_x(W_{Q,e^{-\lambda n}}) > 0 \iff \| x - \frac{p}{q} \| < e^{-\lambda n} \text{ for some } q \leq Q. \]

Note that somewhat surprisingly Theorem A then implies a sharper form of Proposition 3.1 with the estimate (3.2) on the mass of almost rational points replaced by the sharper estimate \( \mu_0(W_{Q,e^{-\lambda n}}) > C't. \) In the special case of \( \mu = \mu_0 = \mu_1 = \ldots \) a \( \nu \)-stationary probability measure, we can take \( n \) in Proposition 3.1 to be arbitrarily large and deduce that for appropriate constant \( C \)

\[ \mu(R_Q) \geq \left( \frac{t}{2} \right)^C \text{ for } Q = \left( \frac{2\|a\|}{t} \right)^C, \]

with \( a \) and \( t \) as in (3.1), giving a somewhat more quantitative version of Theorem A.

We sketch the proof of Proposition 3.1. The proof consists of two phases:

(Ph-1) First one starts with a lower bound on a single Fourier coefficient of the measure \( \mu_n = \nu^n * \mu \), namely \( |\hat{\mu}_n(a)| t \), and deduce from this that for an appropriately chosen \( m_1 < n \) the measure \( \mu_{n-m_1} \) has a rich set of Fourier coefficients which are larger than a fixed power of \( t/2 \).

(Ph-2) In the second phase, this information on the set of big Fourier coefficients of \( \mu_{n_1} \) for \( n_1 = n - m_1 \) is used to show that for another appropriately chosen \( m_2 < n_1 \) the measure \( \mu_{n_1-m_2} \) gives a significant (a fixed power of \( t/2 \)) mass to small balls around rational points with low denominator.

It is perhaps instructive to present a proof of a much simpler result with a somewhat similar structure:

**Proposition 3.2** ("Baby Case"). A probability measure \( \mu \) on \( \mathbb{T}^d \) which is \( \Gamma \)-invariant for \( \Gamma \) a finite index subgroup of \( \text{SL}_d(\mathbb{Z}) \) is a linear combination of Haar measure and a purely atomic \( \Gamma \)-invariant measure.

In this setting one can use the following simple argument by Marc Burger [9].

- Assume that the \( \Gamma \)-invariant probability measure \( \mu \) is not Haar measure. Then \( \mu \) has a nontrivial Fourier coefficient:

\[ |\hat{\mu}(a)| = t > 0 \quad \text{at some } a \in \mathbb{Z}^d \setminus \{0\}. \]

Since \( \hat{\mu}(a) = \hat{g} * \hat{\mu}(a) = \hat{\mu}(g^\ast a) \), it follows that \( |\hat{\mu}(b)| = t_0 > 0 \) for all \( b \in \Gamma^\ast a \). For \( \text{SL}_d(\mathbb{Z}) \) and its finite index subgroups, any orbit \( \Gamma^\ast a \subset \mathbb{Z}^d \setminus \{0\} \) has positive density in \( \mathbb{Z}^d \).

- By Wiener’s Lemma this implies that \( \mu \) has atoms. Indeed, evaluating \( \mu \times \mu(\Delta) = \mu * \hat{\mu}(\{0\}) \) (where \( \Delta \) is the diagonal in \( \mathbb{T}^d \times \mathbb{T}^d \) and the convolution \( \mu * \hat{\mu} \) is the image of \( \mu \times \mu \) under the projection \( (x,y) \mapsto x - y \)) in two ways, one gets the identity (cf. [28, I.7.13])

\[ \sum_{x \text{ atom of } \mu} \mu(\{x\})^2 = \lim_{n \to \infty} \frac{1}{|B_n|} \sum_{a \in B_n} |\hat{\mu}(a)|^2 \]
where \( B_n = \{ a \in \mathbb{Z}^d : \max_{1 \leq i \leq d} |a_i| \leq n \} \). It follows that any \( \Gamma \)-invariant probability measure \( \mu \) on \( \mathbb{T}^d \) can be presented as a linear combination of Haar measure and a purely atomic \( \Gamma \)-invariant measure.

In the context of Proposition 3.1 establishing the existence of enough “big” Fourier coefficients for \( \mu_n \), given that \( \mu_n \) had at least one significant Fourier coefficient is substantially more involved, and we get much less than positive density. Consequently, in the second phase of the proof we will start with a weaker type of information on \( \mu \) than in the simple proof sketched above.

3.A. Phase I: Large scale structure of the set of large Fourier coefficients.

Starting from some \( a_0 \in \mathbb{Z}^d \setminus \{0\} \) with \( |\hat{\mu}_n(a_0)| = t_0 > 0 \) for sufficiently large \( n \) depending on \( t_0, a_0 \), we shall prove that for \( t = t_0^p \) and any \( m_1 \) in the range \( C(1 + \log t_0) < m_1 < n \) (with \( p, C \) some constants depending on \( \Gamma, \nu \)) the set of \( t \)-“large” Fourier coefficients

\[
A_{n-m_1, t} = \{ a \in \mathbb{Z}^d : |\hat{\mu}_{n-m_1}(a)| > t \}
\]

is relatively “thick” in \( \mathbb{Z}^d \), in the following sense.

Let \( \mathcal{N}(E; M) \) denotes the covering number of \( E \subset \mathbb{Z}^d \) by \( M \)-balls. In the simple proof of Proposition 3.2 the proportion of “large” Fourier coefficients in any sufficiently large box was shown to be positive. In the context of Proposition 3.1 the most difficult part of the proof, which in precise form is given by Theorem 6.1 below, gives that there is a large \( N \) (with \( \frac{N}{\|a_0\|} \) bounded above and below by an exponential in \( m_1 \)) and an exponentially smaller \( M \) (more precisely, \( \frac{M}{\|a_0\|} \) will be in the range \( \left( \frac{N}{\|a_0\|} \right)^{1-\kappa_1} < \frac{M}{\|a_0\|} < \left( \frac{N}{\|a_0\|} \right)^{1-\kappa_2} \)) so that the number of \( M \)-balls needed to cover the intersection \( A_{n-m_1, t_0} \cap [-N, N]^d \) is large—namely

\[
\mathcal{N} \left( A_{n-m_1, t_0} \cap [-N, N]^d; M \right) > t_0^p \left( \frac{N}{M} \right)^d,
\]

where \( p, \kappa_1, \kappa_2 > 0 \) are constants depending only on \( \Gamma \) and \( \nu \). Thinking of \( t_0 \) as fixed (which is the case needed to establish Corollary 3.3), this gives a lower bound on the covering number that is a positive proportion of the trivial upper bound.

To prove the key estimate \( \| \cdot \| \), one starts with the identity

\[
\hat{\mu}_n(a_0) = \sum_g \nu^{*m}(g) \cdot \hat{\mu}_{n-m}(g^{\dagger}a_0)
\]

to conclude that if \( |\hat{\mu}_n(a_0)| > t_0 \), then

\[
\nu^{*m} \left\{ g \in \Gamma : |\hat{\mu}_{n-m}(g^{\dagger}a_0)| > \frac{t_0}{2} \right\} \geq \frac{t_0}{2}.
\]

In Proposition 6.2 below we deduce from \( \| \cdot \| \), using the quantitative theory of random matrix products, that once \( m_1 \) is larger than some absolute constant,

\[
\mathcal{N} \left( A_{n_1-t_1} \cap [-N_1, N_1]^d; M_1 \right) > \left( \frac{N_1}{M_1} \right)^{\alpha_1}.
\]

where \( n_1 = n - m_1, N_1 = \|a_0\| \exp(\frac{3}{2} \lambda n), M_1 = \|a_0\|, t_1 = t_0/2 \), with \( \lambda \) the top Lyapunov exponent corresponding to \( \nu \) (cf. Section 4).

\(^1\)There is nothing special about \( \frac{3}{2} \); any constant greater than 1 would do.
For our proof it is crucial to improve the estimate (3.6) to the much sharper density type estimate (3.7). Equation (3.6) is equivalent to having an $M_1$-separated subset $E \subset Z^d \cap [-N_1, N_1]^d$ of cardinality $|E| \geq (N_1/M_1)^{\alpha_1}$ so that for every $a \in E$ we have $|\hat{\mu}_{n_1}(a)| > t_1$; and decreasing the cardinality of $E$ by a constant factor, we may assume

\begin{equation}
|\sum_{a \in E} \hat{\mu}_{n_1}(a)| > \frac{t_1}{2} |E|.
\end{equation}

Similarly to the way we used the identity $\mu_n = \nu^{*m_1} * \mu_{n_1}$ in the proof of (3.6), equation (3.7) implies that (for any choice of $m < n_1$), for $\nu^m$-many $g \in \Gamma$, for many $e \in g^{t_1}E$ we have that $|\hat{\mu}_{n_1-m}(e)| > t_1/4$; indeed, if

\[ G = \left\{ g \in \Gamma : \left\{ e \in g^{t_1}E : |\hat{\mu}_{n_1-m}(e)| > \frac{t_1}{4} \right\} > \frac{t_1}{4} |E| \right\}, \]

then $\nu^m(G) \geq t_1/4$.

Our assumptions (Γ-0)–(Γ-2) on $\Gamma$ guarantee that the top Liapunov exponent for the random walk on $SL_d(\mathbb{Z})$ corresponding to $\nu$ is simple, which allows us to approximate $\nu^m$-typical $g$ by a composition of dilatation (by a factor $\sigma_1(g)$ in the range $e^{(\lambda - \epsilon)m} \leq \sigma_1(g) \leq e^{(\lambda + \epsilon)m}$), a rotation, and a rank one projection, say $\pi_g$. The theory of random matrix products also gives us control over the distribution on the direction of the null space of this projection. Therefore choosing $M_2$ appropriately, we cannot distinguish with resolution $M_2$ between the map $a \mapsto g^{t_1}a$ and this rank one transformation, e.g. in the sense that for any $E' \subset E$

\[ \mathcal{N}(g^{t_1}(E'); M_2) \approx \mathcal{N}(\sigma_1(g)g^{t_1}(E'); M_2). \]

As long as $m = m_2$ is sufficiently large (larger than some constant times $|\log t_1|$), this applies to most $g \in G$ so that we can view $g^{t_1}(E)$ as a rotated and dilated rank one (random) projection of $E$.

If $N_2, M_2, m_2$ are appropriately chosen, outside a set of $g \in \Gamma$ of negligible $\nu^m$-measure, $g^{t_1}([-N_1, N_1]^d)$ is contained in a rotated rectangular box of size $[-N_2, N_2] \times [-M_2, M_2] \times \cdots \times [-M_2, M_2]$. If $\alpha_2$ were very close to $d$ (say bigger than some $\alpha_{\text{high}}$), we could use a variant on the Marstrand Projection Theorem, or more precisely on an extension due to Falconer [13], to show that for many $g \in G$

\[ \mathcal{N}(g^{t_1}E; M_2) \gg t_1^p \left( \frac{N_2}{M_2} \right), \]

and moreover that a similar inequality (with possibly a different implied constant, still polynomial in $t_1$) holds for any subset $E' \subset E$ with $|E'| \geq t_1 |E|/4$. By definition of $G$, one obtains that

\[ \mathcal{N}(A_{n_2, t_1/4} \cap g^{t_1}([-N_1, N_1]^d); M_2) \gg t_1^p \left( \frac{N_2}{M_2} \right) \]

and with some further arguments employing the inherent additive structure of Fourier coefficients of probability measures, we get from this an estimate of the desired form

\[ \mathcal{N}(A_{n_2, t_1/4} \cap [-N_2, N_2]^d; M_2) \gg t_1^{p'} \left( \frac{N_2}{M_2} \right)^d \]

where $p' > p$ is some fixed power.

\footnote{Essentially, the Cauchy-Schwartz inequality.}
The argument sketched above is carried out in Section 6.C below, and the resulting proposition is given by Proposition 6.5 below. Unfortunately, we have little control over \( \alpha_1 \) which is determined by properties of the random walk corresponding to \( \nu \) on \( SL(d, \mathbb{R}) \). To handle the main case where \( \alpha_1 < \alpha_{\text{high}} \), we need to use arithmetic combinatorics: a projection result [5, Thm. 5] of the first author (based on techniques developed in the context of the Discretized Ring Conjecture [4]). Roughly stated, this theorem asserts that given a sufficiently rich set of lines \( D \subset \mathbb{R}^{d-1} \) and a (sufficiently nondegenerate) set \( E \subset [0, 1]^d \) of “dimension” \( \alpha \), there exist (many) lines \( \theta \in D \) so that the projection \( \pi_\theta(E) \) of \( E \) to \( \theta \) has “dimension” \( \alpha + \alpha_{\text{inc}} > \frac{\alpha + \alpha_{\text{inc}}}{d} \) for some fixed \( \alpha_{\text{inc}} > 0 \). This bootstrap step is the content of Proposition 6.3.

A complication in the proof of both Proposition 6.3 and Proposition 6.5 is that the two conditions (1)–(2) above on \( \mu \) guarantee in particular that \( \mu_{n-m} \) is granulated in the following sense (cf. Proposition 7.1): for some constants \( 1 < L_1 < L_2 \) and \( \kappa > 0 \) there is some \( \rho \in (L_2^{-m}, L_1^{-m}) \) and the finite set \( X \subset \mathbb{T}^d \) so that

\[
\mu \left( \bigcup_{x \in X} B_{x, \frac{1}{\rho}} \right) > t^{\rho'}.
\]

Using this harmonic analytic fact, the outcome of the first stage of the proof is that for \( m_1 \gg \log(||a||/t_0) \), the measure \( \mu_{n_1} = \mu_{n-m} \) is granulated in the following sense (cf. Proposition 7.1): for some constants \( 1 < L_1 < L_2 \) and \( \kappa > 0 \) there is some \( \rho \in (L_2^{-m}, L_1^{-m}) \) and the finite set \( X \subset \mathbb{T}^d \) so that

1. \( X \) is \( r = \rho^{1-\kappa} \)-separated,
2. \( \mu_{n_1} \left( \bigcup_{x \in X} B_{x, \rho} \right) > t^{\rho'} \).

This is not yet what we want. So we continue with the strategy of successively sacrificing some convolution powers of \( \nu \) (i.e., increasing \( m \) to \( m' > m \)) in exchange for more precise information on \( \mu_{n-m'} \).

The two conditions (1)–(2) above on \( \mu_{n-m} \) and \( X \) guarantee in particular that \( t^{O(1)} \) of the mass of \( \mu_{n-m} \) is concentrated in balls of radius \( \rho \) whose measure is rather large, namely \( \geq t^{O(1)} \rho^{1-\kappa} \).

Thanks to the separation condition, we can improve this estimate (cf. Proposition 7.2) and show that for appropriate \( m' \) (also \( \ll \log(||a||/t) \)) there is a set \( X' \) of cardinality at most that of \( X \) so that \( \mu_{n-m'} \left( \bigcup_{x \in X'} B_{x, \rho^N} \right) \geq t^{O(1)}N \) for an arbitrary \( N \).
At this stage we can rectify the unknown balls \( \{ B_{x,\rho}^n : x \in X' \} \) to be centered at rational points of controlled denominator. The reason for that is that as

\[
\mu_{n-m'}(B_{x,\rho}^n) = \sum_g \nu^g(\mu) \mu_{n-m'-\ell}(g^{-1}B_{x,\rho}^n),
\]

if \( \mu_{n-m'}(B_{x,\rho}^n) \) is big, for many \( g \) with \( \|g^{-1}\| \) of controllable size (roughly \( e^{-\lambda_d \ell} \), with \( \lambda_d \) the bottom Liapunov exponent of \( \nu \)), the measure of the “shifted” balls \( \mu_{n-m'-\ell}(g^{-1}B_{x,\rho}^n) \) has to be big—so many \( g \) in fact that as \( \mu_{n-m'-\ell} \) is a probability measure, there should be a lot of intersections between these shifted balls. These nontrivial intersections can be used to show that \( x \) is much closer to a rational of controlled denominator than what can be expected of a random point in \( T^d \). This rough scheme is carried out by Proposition 7.3.

Using the extra information obtained, one can proceed similarly to the first step mentioned above (i.e., Proposition 7.2) but with essentially no loss of mass (Proposition 7.4) and obtain the desired conclusion, i.e., Proposition 3.1.

4. Random matrix products

4.A. Notation. Let \( G \) be a topological group, in this paper the discrete group \( \Gamma \) or the torus \( T^d \). On the set \( \text{Prob}(G) \) of all probability measures on \( G \) (for \( G = T^d \) the measures are assumed to be Borel regular) one defines operations of convolution: \( \nu_1, \nu_2 \mapsto \nu_1 * \nu_2 \), and of a reflection \( \nu \mapsto \tilde{\nu} \), by pushing forward \( \nu_1 \times \nu_2 \) under the product map \( (g_1, g_2) \mapsto g_1 \cdot g_2 \) and pushing \( \nu \) by the inverse map \( g \mapsto g^{-1} \), respectively. For \( n \in \mathbb{N} \) we write \( \nu^n \) for the \( n \)th convolution power of \( \nu \) with itself. This should be distinguished from the product \( \nu \cdot \mu \) defined on \( G^n \).

Similarly, if \( G \rightsquigarrow X \) is a continuous action on a topological space, for \( \nu \in \text{Prob}(G) \) and \( \mu \in \text{Prob}(X) \) the convolution \( \nu * \mu \in \text{Prob}(X) \) is the pushforward of \( \nu \times \mu \) under the action map \( G \times X \to X \). For \( \Gamma \rightsquigarrow T^d \) and \( \nu \in \text{Prob}(\Gamma) \), \( \mu \in \text{Prob}(T^d) \) we have

\[
\nu * \mu = \sum_{g \in \Gamma} \nu(g) \cdot g_* \mu, \quad \text{where} \quad g_* \mu(E) = \mu(g^{-1}E).
\]

For \( \mu \in \text{Prob}(T^d) \) the Fourier coefficients are

\[
\hat{\mu}(a) = \int_{T^d} e_a(x) \, d\mu(x) \quad \text{where} \quad e_a(x) = e^{2\pi i \langle a, x \rangle} \quad (a \in \mathbb{Z}^d, \ x \in T^d).
\]

The Fourier transform intertwines \( \Gamma \)-actions on \( T^d \) and on \( \mathbb{Z}^d = \hat{T}^d \) according to

\[
\hat{g_* \mu}(a) = \hat{\mu}(g^* a).
\]

In a metric space (such as \( \mathbb{Z}^d, \mathbb{R}^d, \mathbb{P}^{d-1}, T^d \)) we denote by \( B_{x,r} = \{ y : d(x, y) \leq r \} \) the closed \( r \)-ball around \( x \) and by \( \text{Nbd}_r(E) \) the (closed) \( r \)-neighborhood of a set \( E \). For a set \( E \) denote by

\[
\mathcal{N}(E; r) = \inf \left\{ n : \exists x_1, \ldots, x_n \text{ s.t. } E \subset \bigcup_{i=1}^n B_{x_i,r} \right\}
\]

the covering number of \( E \) by \( r \)-balls (these covering numbers will be used for finite subsets of \( \mathbb{Z}^d \) with a large \( r \) and for subsets of \( \mathbb{P}^{d-1} \) and \( T^d \) with small \( r > 0 \)).
Linear algebra. Throughout the paper we use the standard inner product \( \langle x, y \rangle = \sum_1^d x_i y_i \), the Euclidean norm \( \|x\|^2 = \langle x, x \rangle \) on \( \mathbb{R}^d \), and the operator norm \( \|g\| = \max \|gx\|/\|x\| \) on matrices \( g \in \text{GL}_d(\mathbb{R}) \). For \( x \in \mathbb{R}^d \setminus \{0\} \), \( \bar{x} = Rx \) denotes the corresponding point in the projective space \( \mathbb{P}^{d-1} \). We equip \( \mathbb{P}^{d-1} \) with the metric given by
\[
d_\mathbb{P}(\bar{x}, \bar{y}) = \sin (\angle(\bar{x}, \bar{y})) = \frac{\|x \wedge y\|}{\|x\| \cdot \|y\|}.
\]
For \( g \in \text{GL}_d(\mathbb{R}) \) denote by \( \sigma_1(g) \geq \sigma_2(g) \geq \cdots \geq \sigma_d(g) > 0 \) the singular values of \( g \). In the polar decomposition we have
\[
g = U \begin{pmatrix} \sigma_1(g) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_d(g) \end{pmatrix} V \text{ with } U, V \text{ orthogonal.}
\]
For \( g \in \text{GL}_d(\mathbb{R}) \) let \( \varrho(g) = \sigma_2(g)/\sigma_1(g) \). If \( \varrho(g) < 1 \), let
\[
\theta(g) = U\bar{e}_1 \in \mathbb{P}^{d-1}.
\]
This is the direction of the long axis of the \( g \) image of the round ball
\[
\{ x \in \mathbb{R}^d : \|x\| \leq 1 \}.
\]
Denote by \( H(g) \) the hyperplane of vectors with “shorter stretch”
\[
H(g) = \left\{ \bar{z} \in \mathbb{P}^{d-1} : V \bar{z} \in \text{Span}(e_2, \ldots, e_d) \right\}
\subset \left\{ \bar{z} \in \mathbb{P}^{d-1} : \|g\bar{z}\| \leq \sigma_2(g) \|\bar{z}\| \right\}.
\]
Note that \( \theta(g) \) describes the direction of the image of the “long vector”, under \( g : \mathbb{R}^d \to \mathbb{R}^d \), while \( H(g) \) refers to the source of the shorter ones. If \( \varrho(g) = 1 \), define \( \theta(g) \) and \( H(g) \) arbitrarily.

Lemma 4.1. For \( g \in \text{GL}_d(\mathbb{R}) \) with \( \varrho(g) < 1 \):

1. \( H(g) = \theta(g)^{1^+} \).
2. For any \( 0 \neq z \in \mathbb{R}^d \),
\[
\|g\| \cdot \|z\| \cdot d_\mathbb{P}(\bar{z}, H(g)) \leq \|g\| \cdot \|z\| \cdot (\varrho(g) + d_\mathbb{P}(\bar{z}, H(g))).
\]
3. \( d_\mathbb{P}(g\bar{z}, \theta(g)) < \varrho(g)/d_\mathbb{P}(\bar{z}, H(g)) \) for any \( 0 \neq z \in \mathbb{R}^d \).
4. If \( g = hk \) with \( \varrho(h) < 1 \) and \( 2\varrho(h) < \|g\|/\|h\| \|k\| \), then
\[
d_\mathbb{P}(\theta(h)) < 2\varrho(h) \cdot \frac{\|h\| \cdot \|k\|}{\|g\|}.
\]

Proof. (1) is immediate from the definitions.

(2) Write \( z = \|z\| \cdot (tx + sy) \) with \( \bar{x} \in H(g)^{1^+}, \bar{y} \in H(g), \|x\| = \|y\| = 1 \). Then
\[
|t| = d_\mathbb{P}(\bar{z}, H(g)), \text{ while}
\]
\[
\|z\| \cdot \|g\| \cdot |t| \leq \|g\| \|z\| \|tx + sy\| = \|z\| \sqrt{t^2 \|gx\|^2 + s^2 \|gy\|^2} \leq \|z\| \|\|t\|\|g\| + \|s\| \sigma_2(g)\|).
\]

(3) Assume \( \|z\| = 1 \) and write \( z = tx + sy \) as in (2). We have \( \theta(g) = g\bar{x} \) and
\[
\|g\| = \|gx\| \text{ and } \|g\| \geq \|g\| \cdot |t| \text{. Also } gx \wedge gz = gx \wedge (tx + sy) = s(gx \wedge gy).
\]
Hence
\[
d_\mathbb{P}(g\bar{z}, \theta(g)) = \frac{\|gz \wedge gx\|}{\|gz\| \cdot \|gx\|} \leq \frac{|s| \cdot \|gy\| \cdot \|gx\|}{\|g\| \cdot |t| \cdot \|gx\|} \leq \frac{\|gy\|}{\|g\| \cdot |t|}.
\]
Now (3) follows, because \( \|gy\| \leq \sigma_2(g) \) and \( |t| = d_\mathbb{P}(\bar{z}, H(g)) \).
The top Lyapunov exponent is simple: the following subadditive sequences:

\[ \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d \]

Thus \( d_z(\tilde{z}, H(h)) = |t| \). We have

\[ \|g\| = \|gx\| = \|hz\|, \quad \|z\| = \|kx\| \leq \|k\| \implies \frac{\|hz\|}{\|z\|} \geq \frac{\|g\|}{\|k\|}. \]

But \( \|hz\|^2 \leq \|z\|^2 (t^2 \sigma_1(h)^2 + \sigma_2(h)^2 s^2) \) because \( w \in H(h) \). Hence

\[ \frac{\|g\|}{\|h\| \cdot \|k\|} \leq \frac{\|hz\|}{\|h\| \cdot \|z\|} \leq \sqrt{t^2 + \rho(h)^2 s^2} \leq \sqrt{t^2 + \rho(h)^2}. \]

Denoting by \( c \) the left-hand side, we get \( d_z(\tilde{z}, H(h)) = |t| \geq \sqrt{c^2 - \rho(h)^2} \). Since \( \theta(g) = g\tilde{x} = h\tilde{z} \), estimate (3) gives

\[ d_z(\theta(g), \theta(h)) = d_z(h\tilde{z}, \theta(h)) \leq \frac{\rho(h)}{\sqrt{c^2 - \rho(h)^2}} \leq \frac{2\rho(h)}{c} \]

under the assumption \( 2\rho(h) < c \). \( \square \)

4.B. Random walks. Let \( \nu \) be a probability measure on \( \text{SL}_d(\mathbb{R}) \) such that

\[ \int \log \|g\| \, d\nu < \infty. \]

The Lyapunov exponents \( \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d \) of \( \nu \) are defined through the limits of the following subadditive sequences:

\[ \lambda_1 = \lim_{n \to \infty} \frac{1}{n} \log \|g\| \, d\nu^*(g), \quad \lambda_i = \lim_{n \to \infty} \frac{1}{n} \log \|g\| \, d\nu^*(g). \]

Equivalently, \( \lambda_i \) describes the asymptotic of \( \int n^{-1} \log \sigma_i(g) \, d\nu^*(g) \), where \( \sigma_i \) are the singular values; in particular, \( \sigma_1(g) = \|g\| \). The convergence holds not only on average, but also a.e. and in \( L^1 \) if \((g_1, g_2, \ldots)\) are chosen independently according to \( \nu \), then, using Kingman’s subadditive ergodic theorem, with probability one and in \( L^1(\nu^\infty) \) a long random product has polar decomposition

\[ g_n \cdots g_2g_1 = U \begin{pmatrix} e^{\lambda_1n + o(n)} \\ e^{\lambda_2n + o(n)} \\ \vdots \end{pmatrix} V \]

with \( U \) and \( V \) orthogonal.

Theorem 4.2 ([17, 16]). Let \( \nu \) be a probability measure on \( \text{SL}_d(\mathbb{R}) \) with (4.1) and so that the group \( \langle \text{supp}(\nu) \rangle \) satisfies conditions (\( \Gamma \)-0)–(\( \Gamma \)-2) of p. 231. Then the top Lyapunov exponent is simple:

\[ \lambda_1 > \lambda_2. \]

In particular, \( \lambda_1 > 0 \).

If \( \langle \text{supp}(\nu) \rangle \) is irreducible on \( \mathbb{R}^d \), then (18) for any fixed \( x \in \mathbb{R}^d \setminus \{0\} \) for \( \nu^\infty \)-a.e. sequence \((g_1, g_2, \ldots)\)

\[ \frac{1}{n} \log \|g_n \cdots g_1x\| = \lambda_1. \]

If, furthermore, \( \lambda_1 > \lambda_2 \), then, denoting \( h_n = g_n \cdots g_1 \), the angle \( d_z(h_n\tilde{x}, \theta(h_n)) \to 0 \) a.s.
We shall need exponential estimates for various rates of convergence in the above stated limits. Such estimates are known under an assumption slightly stronger than (4.1), namely:

\( (4.2) \quad \int ||g||^\nu \, d\nu(g) < \infty \quad \text{for some} \quad \epsilon > 0. \)

**Theorem 4.3** (Large deviations). Let \( \nu \in \text{Prob}(\text{SL}_d(\mathbb{R})) \) satisfy (4.2). Then for any \( \omega > 0 \) there are \( \rho = \rho(\omega) > 0 \) and \( m_0(\omega) \) so that for \( m \geq m_0(\omega) \)

\[
\nu^* \left\{ g : \left| \lambda_i - \frac{1}{m} \log \frac{|gx|}{|x|} \right| > \omega \right\} < e^{-\rho \cdot m} \quad \forall x \in \mathbb{R}^{d-1} \setminus \{0\},
\]

\[
\nu^* \left\{ g : \left| \lambda_i - \frac{1}{m} \log \sigma_i(g) \right| > \omega \right\} < e^{-\rho \cdot m} \quad (i = 1, \ldots, d).
\]

**Proof.** The first inequality follows from [3, Thm. V.6.1] and the remarks following the proof regarding uniformity in \( x \); the second inequality is [3, Thm. V.6.2]. \( \square \)

**Theorem 4.4** (Exponential estimates). Let \( \nu \in \text{Prob}(\text{SL}_d(\mathbb{R})) \) satisfy (4.2) and conditions (\( \Gamma \)-0)-(\( \Gamma \)-2) of p. 231. Then for some \( c_1, c_2 > 0 \) and \( m_0 \in \mathbb{N} \) so that for all \( x, y \in \mathbb{P}^{d-1} \) each of the following subsets of \( \Gamma \)

1. \( \{ g \in \Gamma : d_{\langle X \rangle} (gx, gy) > e^{-c_1 \cdot m} \} \),
2. \( \{ g \in \Gamma : d_{\langle X \rangle} (gx, gy^{-1}) > e^{-c_1 \cdot m} \} \),
3. \( \{ g \in \Gamma : d_{\langle X \rangle} (gx, \theta(g)) < e^{-c_1 \cdot m} \} \)

has \( \nu^* \)-probability \( > 1 - e^{-c_2 \cdot m} \) for \( m \geq m_0 \).

**Proof.** Set \( c_1 = (\lambda_1 - \lambda_2)/2 \).

We first establish (3). Fix \( \bar{x} \in \mathbb{P}^{d-1} \). By Theorem 4.3 there is \( \rho_1 > 0 \) and \( m_1 \) so that for \( m > m_1 \), with \( \nu^* \)-probability \( > 1 - e^{-\rho_1 \cdot m} \)

\( (4.3) \quad \max \left\{ \lambda_1 - \frac{1}{m} \log ||g||, \lambda_2 - \frac{1}{m} \log \sigma_2(g), \lambda_3 - \frac{1}{m} \log \frac{|gx|}{|x|} \right\} < \frac{\lambda_1 - \lambda_2}{12}. \)

Let us show that for some \( m_2 (m_2 > m_1) \) for all \( m > m_2 \) these properties imply

\( (4.4) \quad d_{\langle X \rangle} (\bar{x}, H(g)) > e^{-\lambda_1 - \lambda_2 \cdot m}. \)

Indeed, in the notation of Lemma 4.1 the inequalities in (4.3) imply that

\[
\varrho(g) = \frac{\sigma_2(g)}{\sigma_1(g)} < e^{-\frac{5(\lambda_1 - \lambda_2)}{6} \cdot m}.
\]

Hence by (2) of Lemma 4.1 (4.3) yields

\[
d_{\langle X \rangle} (\bar{x}, H(g)) \geq \frac{|gx|}{||g|| \cdot ||x||} - \varrho(g) \]

\[
> e^{-2(\lambda_1 - \lambda_2) \cdot m} - e^{-\frac{5(\lambda_1 - \lambda_2)}{6} \cdot m},
\]

and (4.4) follows for large \( m \). Using Lemma 4.1(3),

\[
d_{\langle X \rangle} (g\bar{x}, \theta(g)) \leq \frac{\varrho(g)}{d_{\langle X \rangle} (\bar{x}, H(g))} < e^{-\frac{5(\lambda_1 - \lambda_2)}{6} \cdot m} \cdot e^{\lambda_1 - \lambda_2 \cdot m} = e^{-\frac{\lambda_1 - \lambda_2}{6} \cdot m}.
\]

This proves (3).

We now turn to the proof of assertion (2). This also relies on Theorem 4.3 but applied to the random walk corresponding to the measure \( \tilde{\nu} \) defined by \( \tilde{\nu}(g) = \frac{\varrho(g)}{d_{\langle X \rangle} (\bar{x}, H(g))} \).
\(\nu(g^{tr})\). The measure \(\tilde{\nu}\) also satisfies conditions (1.2) and conditions (1\(\Gamma\))-0,\(\Gamma\)-2 above and moreover has the same Liapunov exponents as \(\nu\). Thus inequalities (1.3) hold with \(\tilde{\nu}^{sm}\)-probability exceeding \(1 - e^{-\rho_2 \cdot m}\) for large \(m\). Since \(\theta(g)^\perp = H(g^{tr})\), we have for \(\bar{x}, \bar{y} \in \mathbb{P}^{d-1}\)

\[
\begin{align*}
    d_{\perp}(\bar{x}, y^\perp) & \geq d_{\perp}(\theta(g), y^\perp) - d_{\perp}(\bar{x}, \theta(g)) \\
    &= d_{\perp}(\bar{y}, H(g^{tr})) - d_{\perp}(\bar{x}, \theta(g)).
\end{align*}
\]

Using (4.4) for \(\tilde{\nu}\) and part (3) for \(\nu\), it follows that for large \(m\)

\[
d_{\perp}(\bar{x}, y^\perp) > e^{-\lambda_1 - \lambda_2 \cdot m} - e^{-\lambda_1 - \lambda_2 \cdot m} > e^{-\lambda_1 - \lambda_2 \cdot m}
\]

holds with \(\nu^{sm}\)-probability > \(1 - e^{-\rho_2 \cdot m} - e^{-\rho_1 \cdot m}\). Thus taking \(c_2 = \min(\rho_1, \rho_2)/2\) and \(m_0\) large enough, we deduce (2). Assertion (1) is a trivial consequence of (2). \(\Box\)

4.C. Some further estimates. In this subsection we shall establish some basic estimates that will be used in the following sections.

We shall need a variant of Theorem 4.4 where \(c_1 > 0\) may vary.

Lemma 4.5 (Basic estimate of distribution of directions). There exist \(\tau > 0\) and \(m_0\) so that for any \(r\) in the range

\[e^{-m} < r < e^{-m_0},\]

for any \(\bar{x}, \bar{y} \in \mathbb{P}^{d-1}\)

\[
\nu^{sm}\left\{ g : d_{\perp}(\bar{x}, \bar{y}) < r \right\} < r^\tau,
\]

\[
\nu^{sm}\left\{ g : d_{\perp}(\theta(g), \bar{y}) < r \right\} < r^\tau.
\]

Proof. Let \(c_1, c_2\) be as in Theorem 4.4. Since \(c_1\) can be replaced by any larger value, we may assume \(c_1 \geq 2\) and pick \(0 < r < c_2/c_1\). Given \(r > 0\), let \(k = \left[ c_1^{-1} \cdot \log(1/r) \right]\); in particular \(k < m\). By choosing \(m_0\) large enough, we may ensure that Theorem 4.4 holds for \(\nu^{sk}\). Viewing \(\nu^{sm}\)-random element \(g = g_m \cdots g_1\) as a product \(g = h_2 \cdot h_1\) of a \(\nu^{sk}\)-random element \(h_1\) followed by a \(\nu^{sm-k}\)-random element \(h_2\), we estimate

\[
\begin{align*}
    \nu^{sm}\left\{ g : d_{\perp}(\bar{x}, \bar{y}) < r \right\} & \leq \nu^{sm}\left\{ g : d_{\perp}(\bar{x}, \bar{y}) < e^{-c_1 \cdot k} \right\} \\
    &= \int\nu^{sk}\left\{ h_1 : d_{\perp}(h_1 \bar{x}, h_2^{tr}(\bar{y})) < e^{-c_1 \cdot k} \right\} d\nu^{sm-k}(h_2) \\
    &< \int e^{-c_2 \cdot k} d\nu^{sm-k}(h_2) = e^{-c_2 \cdot k} < e^{c_2} \cdot r^{c_2} < r^\tau
\end{align*}
\]

provided \(r\) is small enough.

For the second estimate, fix an auxiliary \(\bar{x} \in \mathbb{P}^{d-1}\), and let \(k = \left[ c_1^{-1} \cdot \log(1/r) \right]\) as before. We can assume \(m_0 + 1 \leq k < m\) and \(r + e^{-c_1 \cdot m} < 2r < e^{-c_1 \cdot (k-1)}\). Since

\[
d_{\perp}(\theta(g), \bar{y}) \geq d_{\perp}(\bar{x}, \bar{y}) - d_{\perp}(\theta(g), \bar{x}),
\]

we have

\[
\begin{align*}
    \nu^{sm}\left\{ g : d_{\perp}(\theta(g), \bar{y}) < r \right\} & \leq \nu^{sm}\left\{ g : d_{\perp}(\theta(g), \bar{x}) > e^{-c_1 \cdot m} \right\} \\
    &+ \nu^{sm}\left\{ g : d_{\perp}(\theta(g), \bar{y}) < r + e^{-c_1 \cdot m} < e^{-c_1 \cdot (k-1)} \right\} \\
    &< e^{-c_2 \cdot m} + e^{-c_2 \cdot (k-1)} \leq 2e^{-c_2 \cdot (k-1)} < r^\tau
\end{align*}
\]

assuming \(r\) is small enough (guaranteed by taking \(m_0\) large). \(\Box\)
Given a set \( F = \{\vec{x}_1, \ldots, \vec{x}_d\} \subset \mathbb{P}^{d-1} \), a quantitative measure of the extent to which these lines are in general position is given by the volume spanned by unit vectors in these directions:

\[
\operatorname{vol}(\vec{x}_1, \ldots, \vec{x}_d) = \frac{|x_1 \wedge \cdots \wedge x_d|}{\|x_1\| \cdots \|x_d\|}.
\]

This quantity is symmetric in the arguments but can be computed as

\[
\operatorname{vol}(\vec{x}_1, \ldots, \vec{x}_d) = \prod_{i=2}^{d} d_{\perp} (x_i, \text{Span}(x_1, \ldots, x_{i-1})).
\]

Hence, denoting

\[
u(\vec{x}_1, \ldots, \vec{x}_d) = \min_{1 \leq j \leq d} d_{\perp} (x_j, \text{Span}(x_1, \ldots, \hat{x}_j, \ldots, x_d)),
\]

we have

\[
u(\vec{x}_1, \ldots, \vec{x}_d)^d \leq \operatorname{vol}(\vec{x}_1, \ldots, \vec{x}_d) \leq \nu(\vec{x}_1, \ldots, \vec{x}_d).
\]

**Lemma 4.6** (General position). For some \( p < \infty, c_0 \) and \( s_0 > 0 \) depending on \( \nu \), one has

\[
(\nu^m)^d \{ \vec{g} \in \Gamma^d : \operatorname{vol}(\theta(g_1), \ldots, \theta(g_d)) > s^p \} > 1 - s
\]

and

\[
(\nu^m)^d \{ \vec{g} \in \Gamma^d : \operatorname{vol}(\theta(g_1^t), \ldots, \theta(g_d^t)) > s^p \} > 1 - s
\]

for \( e^{-cm} < s < s_0 \).

**Proof.** Let \( r = d^{-1} \cdot s^{1/\tau} \). Given any arbitrary \( g_1 \in \Gamma \), the \( \nu^m \)-probability that

\[
d_{\perp} (\theta(h), \theta(g_1)) > r
\]

is at least \( 1 - r^\tau \) (Theorem 4.4). For the same reason, given any \( g_1, g_2 \),

\[
\nu^m \{ h : d_{\perp} (\theta(h), \theta(g_1) \oplus \theta(g_2)) > r \} > 1 - r^\tau.
\]

Continuing this argument, we deduce that the set

\[
\{ \vec{g} \in \Gamma^d : d_{\perp} (\theta(g_1), \theta(g_1) \oplus \cdots \oplus \theta(g_{i-1})) > r \text{, } i = 2, \ldots, d\}
\]

has \( (\nu^m)^d \)-measure at least

\[
(1 - r^\tau)^{d-1} > 1 - (d - 1) r^\tau > 1 - s.
\]

On the other hand every \( d \)-tuple in the set above has

\[
\operatorname{vol}(\theta(g_1), \ldots, \theta(g_d)) > r^d.
\]

If \( p \) is large enough, \( s^p < r^d = d^{-d} s^d / \tau \).

To deduce the second estimate, one may apply the same arguments to the random walk generated by \( \tilde{\nu} \), with \( \tilde{\nu} \) the transpose to \( \nu \) as in the proof of Theorem 4.4. \( \square \)
5. Two notions of coarse dimension

Given a subset \( \hat{A} \) of \( B_{0,1} \subset \mathbb{R}^d \), there are several ways one can try to estimate its dimension, or more precisely, in our case, its dimension at scale \( r \). One simple way is via covering numbers: we can consider \( \hat{A} \) to be of “coarse dimension” \( \geq \alpha \) at scale \( r \) if \( \mathcal{N}(\hat{A};r) \geq r^{-\alpha} \). Another, more restrictive, definition of “coarse dimension \( \geq \alpha \)” is via the following:

**Definition 5.1.** A measure \( \rho \) on a set \( B \) is said to be \((C,\alpha)\)-regular at scale \( r \) on \( B \) if for any \( x \in A \), \( s \geq r \)

\[
\rho(B_{x,s}) < C \left( \frac{s}{\text{diam } B} \right)^\alpha.
\]

A set \( B \) is said to be \((C,\alpha)\)-regular at scale \( r \) if the corresponding uniform measure \( \rho = \frac{1}{|B|} \sum_{x \in B} \delta_x \) is \((C,\alpha)\)-regular at scale \( r \).

Thus another plausible definition of “coarse dimension” of a finite set \( A \) would be that \( A \) supports some probability measure \( \rho \) which is \((C,\alpha)\)-regular at scale \( r \) on \( A \) for some absolute constant \( C \).

The following lemma allows us to relate the two notions:

**Lemma 5.2.** For any \( \epsilon > 0 \) there are constants \( C_{\epsilon}, C_{\epsilon}' > 0 \) such that for every \( s, \alpha \) with \( 2\epsilon < s < \alpha \) and \( r < 1 \), if \( \hat{A} \subset B_{0,1} \subset \mathbb{R}^d \) satisfies

\[
\mathcal{N}(\hat{A};r) \geq r^{-\alpha},
\]

then there is a point \( x \in B_{0,1} \) and a probability measure \( \rho \) supported on \( \hat{A} \cap B_{x,r^\beta} \) which is \((C_{\epsilon},\alpha-s)\)-regular on \( B_{x,C_{\epsilon}'r^\beta} \) at scale \( r \) for \( \beta = \frac{d-\alpha+\epsilon}{d-\alpha+s-\epsilon} \).

**Proof.** Let \( T \) be a large integer (which will eventually be determined by \( \epsilon \)), and let \( k_1 = \lceil -\log_2(r)/T \rceil \). Without loss of generality we shall assume that every cube of size \( 2^{-k_1T} \) intersects \( \hat{A} \) in at most one point.

Denote \( S_0 = \{(x_1,\ldots,x_d) \in \mathbb{R}^d : \exists \ell \leq d, x_i \in Z + [0,2^{-T})\} \), \( S_k = 2^{-k} \cdot S \), and

\[
S = S_0 \cup \cdots \cup S_{k_1}.
\]

The density of each \( S_k \) in \( \mathbb{R}^d \) is less than \( d2^{-T} \), so the density of \( S \) is no more than

\[
1 - (1 - d2^{-T})^{k_1 + 1}.
\]

Hence there is a translate \( \hat{A} + \xi \) of \( \hat{A} \) so that

\[
\left| (\hat{A} + \xi) \setminus S \right| \geq (1 - d2^{-T})^{k_1 + 1} \left| \hat{A} \right| \geq C(1)r^{-\alpha + \epsilon/2}
\]

as long as \( T \) is large enough (depending only on \( d, \epsilon \)) for some constant \( C(1) \) (depending on \( d, T, \) and \( \epsilon \)).

Let \( A_0 = (\hat{A} + \xi) \setminus S \). We shall call a cube of the form

\[
Q = \left[ \frac{n_1}{2kT}, \frac{n_1 + 1}{2kT} \right) \times \cdots \times \left[ \frac{n_d}{2kT}, \frac{n_d + 1}{2kT} \right)
\]

for \((n_1,\ldots,n_d) \in \mathbb{Z}^d \) a \( 2^{-kT} \)-cube. By definition of \( A_0 \), for any \( 0 \leq k \leq k_1 \) and any two distinct \( 2^{-kT} \)-cubes \( Q_1, Q_2 \) intersecting \( A_0 \), the distance between \( Q_1 \cap \hat{A}_0 \) and \( Q_2 \cap \hat{A}_0 \) is at least \( 2^{-(k+1)T} \) (this is precisely the purpose of removing points of \( S \) from an appropriate shift of \( \hat{A} \)).
It will be convenient to start by extracting from $\tilde{A}_0$ a large subset $\tilde{A}_1$ with tree-structure (similar to but simpler than that used in [4,5]). By this we mean that there are integers $R_1, \ldots, R_k$ with $1 \leq R_k \leq 2^T$ so that if $A_k$ denotes the collection of $2^{-kT}$-cubes intersecting $\tilde{A}_1$, then for each $0 \leq k < k_1$, each $2^{-kT}$-cube $Q \in A_k$ contains precisely $R_{k+1}$ cubes in $A_{k+1}$. By successively trimming the set $A_0$, we will show that if $T$ is large enough (also depending only on $\epsilon$), one can find such a subset $A_1 \subset A_0$ with tree-structure so that $|\tilde{A}_1| \geq C(2)^{-\alpha+\epsilon}$.

Indeed, to obtain this trimmed set $\tilde{A}_1$, start by throwing away all $2^{-k_1T}$-cubes not intersecting $A_0$. Then consider all $2^{-(k_1-1)T}$ cubes intersecting $A_0$, and find $R_k$, so that the number of these cubes containing between $R_k$ and $2R_k$ of the $2^{-kT}$-cubes is maximized. Throw away all points of $\tilde{A}_0$ which are not contained in such a $2^{-(k_1-1)T}$-cube. Suppose $Q$ is one of the remaining $2^{-(k_1-1)T}$-cubes and that exactly $n_Q$ of the $2^{dT}$ possible $2^{-kT}$-subcubes in $Q$ have nonempty intersection with $\tilde{A}_0$. We throw away all points of $\tilde{A}_0$ in $n_Q - R_k$ of these $2^{-kT}$-subcubes so that precisely $R_k$ subcubes with nonempty intersection with $\tilde{A}_0$ remain in $Q$. Note that the number of points of $\tilde{A}_0$ that are contained in this collection of remaining $2^{-(k_1-1)T}$-cubes is at least $|\tilde{A}_0|/(2dT)$.

Now consider all $2^{-(k_1-2)T}$-cubes intersecting the surviving set, and choose $R_{k_1-1}$ in a similar way, etc. At the end of $k_1$ steps of this type we get a set $A_1$ with tree structure as above and

\begin{equation}
|\tilde{A}_1| \geq (2dT)^{-k_1} |\tilde{A}_0| \geq C(2)^{-\alpha+\epsilon}
\end{equation}

if $T$ is large enough for a suitably chosen constant $C(2)$ (depending on $T$ but not on $r$).

Since each $2^{-kT}$-cube contains at most one point of $\tilde{A}_1$, we have that

\[ \sum_{\ell=1}^{k_1} \log_2 R_\ell = \log_2 |\tilde{A}_1|; \]

hence by (5.1)

\begin{equation}
\sum_{\ell=1}^{k_1} \log_2 R_\ell \geq -(\alpha - \epsilon)T(k_1 - 1).
\end{equation}

Set

\[ M_i = \min_{i < k \leq k_1} \frac{1}{k - i} \sum_{\ell=i+1}^{k} \log_2 R_\ell. \]

Let $1 \leq k_2 < k_1$ be the smallest integer for which $M_{k_2} > (\alpha - s + \epsilon)T$ if such exists; otherwise set $k_2 = k_1$. Then a standard covering argument gives that there is some $k_2 \leq k \leq k_1$ so that

\begin{equation}
\sum_{\ell=1}^{k} \log_2 R_\ell \leq k(\alpha - s + \epsilon)T;
\end{equation}

hence using (5.3) for $\ell \leq k$ and the bound $R_\ell \leq 2^{dT}$ for $\ell > k$, we get the inequality

\[ k_2(\alpha - s + \epsilon)T + (k_1 - k_2)dT \geq \sum_{\ell=1}^{k_1} \log_2 R_\ell \geq (\alpha - \epsilon)T(k_1 - 1) \]
Lemma 5.3. Let $\beta$ be a $(C, \alpha)$-regular probability measure at scale $r$ on $B \subset \mathbb{R}^d$. Then for any $\epsilon > 0$ there is an $r$-separated subset $A \subset \text{supp}(\rho)$ so that the uniform measure on $A$ (i.e., $\mu_A = \frac{1}{|A|} \sum_{a \in A} \delta_a$) is $(C, \alpha - \epsilon)$-regular at scale $r$ on $B$.

Proof. For simplicity of notation, we may assume without loss of generality that diam $B = 1$. We may also assume that $r = 10^{-K}$ and that $\rho(Q) < 10^{-\alpha k}$ for every $10^{-k}$-cube $Q$ of the form

\begin{equation}
Q = \left[ \frac{n_1}{10^k}, \frac{n_1 + 1}{10^k} \right) \times \cdots \times \left[ \frac{n_d}{10^k}, \frac{n_d + 1}{10^k} \right), \quad n_1, \ldots, n_d \in \mathbb{Z},
\end{equation}

where $k \in \{k_0, \ldots, K\}$. Let $L = \lceil 10^{\alpha K} \rceil$, and let $\{a_1, \ldots, a_L\}$ be chosen randomly and independently with distribution $\rho$.

Fix an integer $k \leq K$ and denote $p = 10^{-(\alpha - \epsilon)k}$, $N = 10Lp$. The probability that a given $10^{-k}$-cube $Q$ contains $n > N$ points from $\{a_1, \ldots, a_L\}$ is given by the tail of the binomial distribution:

$$
\sum_{n > N} \binom{L}{n} p^n (1 - p)^{L-n} < \sum_{n > N} \frac{L(L-1) \cdots (L-n+1)}{n!} \cdot p^n < \sum_{n > N} \left( \frac{3}{10} \right)^n < 10^{-\frac{1}{2}N}.
$$

Since $N/2 = 5Lp > 10^{\alpha K} \cdot 10^{-(\alpha - \epsilon)k} = 10^{\alpha (K-k) + k/2} \geq 10^{k/2} > 2dk$ for $k > k_\epsilon$, it follows that the probability that one or more of the $10^{dk}$ cubes $Q$ of size $10^{-k}$ has more than $L \cdot 10^{-(\alpha - \epsilon)k} > N$ points is less than

$$
10^{dk} \cdot 10^{-\frac{1}{2}N} < 10^{dk} \cdot 10^{-2dk} = 10^{-dk}.
$$

Hence with probability exceeding $1 - \sum_{k=1}^{\infty} 10^{-dk} > 0$, the set $A_0 = \{a_1, \ldots, a_L\}$ has the property that for each $k \in \{k_1, \ldots, K\}$ and every $10^{-k}$-cube $Q$

$$
\frac{|A \cap Q|}{|A|} < 10^{-(\alpha - \epsilon)k}.
$$

Even though each $10^{-K}$-cube as above (cf. (5.4)) contains at most one point of $A_0$, the set $A_0$ may not quite be $10^{-K}$-separated since points in adjacent cubes can be arbitrarily close; but since each $10^{-K}$-cube is adjacent to at most $3^d - 1$ other
10^−K-cubes, there is a 10^−K-separated subset A ⊂ A_0 with |A| ≥ |A_0|/(3^d - 1). This set A satisfies the conditions of the lemma.

Closely related to the notion of \((C, \alpha)\)-regular measures introduced in Definition 5.1 is the notion of \(\alpha\)-energy of a measure \(\rho\), denoted by \(E_\alpha(\rho)\), which we define for a compactly supported measure \(\rho\) on \(\mathbb{R}^d\) and \(\alpha < d\) by

\[
E_\alpha(\rho) = \int_{\mathbb{R}^d} \int_{\mathbb{R}^d} \frac{dp(x) dp(y)}{|x-y|^\alpha}.
\]

If \(\rho\) is \((C, \alpha + \epsilon)\)-regular on a set \(B\) at all scales, then

\[
E_\alpha(\rho) = \alpha \int_B \frac{d\mu(x) dr}{(\text{diam} B)^\alpha} \leq C(\text{diam} B)^{-\alpha - \epsilon \alpha^{-1}}.
\]

The energy \(E_\alpha(\rho)\) can also be given in terms of the Fourier transform of \(\rho\), up to an implicit constant that tends to \(\infty\) as \(\alpha \to d\) (cf. [26, 12.12]):

\[
(5.5) \quad E_\alpha(\rho) \asymp \int_{\mathbb{R}^d} |\hat{\rho}(\xi)|^2 (1 + |\xi|)^{\alpha - d} d\xi.
\]

If \(E_\alpha(\rho) < \infty\), then any set of positive \(\rho\) measure has Hausdorff dimension \(\geq \alpha\) (for this and further information about \(\alpha\)-energy, see [26]).

A simple way to adapt this notion to our “coarse” setup, where we do not care about the details of how \(\rho\) behaves at scales smaller than \(r\), is to smooth it by convolving with an appropriate kernel. Let \(\Phi\) be a fixed radially symmetric nonnegative smooth function on \(\mathbb{R}^d\) with \(\|\Phi\|_1 = 1\) supported on \(B_{0,1}\), and set for \(r > 0\)

\[
\Phi_r(x) = r^{-d} \Phi(r^{-1}x).
\]

Then instead of using the possibly atomic measure \(\rho\), we can consider its smoothed version \(\rho' = \rho * \Phi_r\). In particular, if \(\rho\) is \((C, \alpha + \epsilon)\)-regular at scale \(r\) on a subset \(B \subset \mathbb{R}^d\), then

\[
E_\alpha(\rho * \Phi_r) \ll C(\text{diam} B)^{-\alpha - \epsilon \alpha^{-1}}
\]

with the implicit parameter depending only on \(d\) and the choice of \(\Phi\).

6. Structure of the set of \(t\)-large Fourier coefficients

Fix some probability measure \(\mu_0 \in \text{Prob}(\mathbb{T}^d)\) and consider the sequence

\[
\mu_n = \nu * n * \mu_0
\]

and the following sets of “large” coefficients

\[
A_{t,n} = \{b \in \mathbb{Z}^d : |\tilde{\mu}_n(b)| > t\}.
\]

Our goal in this section is to obtain the following result:

**Theorem 6.1.** There exist constants \(\kappa_1 > \kappa_2 > 0, L_2 > L_1 > 1, p, C < \infty\) depending on \(\nu\) only, so that if for some \(t_0 \in (0, 1/2)\)

\[
|\tilde{\mu}_{n_0}(a_0)| \geq t_0,
\]

then for \(n_0 > m > C \log(2|a_0|/t_0)\) one has

\[
\mathcal{N}\left( A^{N}_{t_0, n_0 - m} \cap B_{0,N} ; M \right) > t_0^p \cdot \left( \frac{N}{M} \right)^d.
\]
for some \( N \) in the range \( L^{n_1}_1 < \frac{N}{\|a_0\|} < L^{n_2}_1 \) and \( M \) in the range \( \left( \frac{N}{\|a_0\|} \right)^{1-\kappa_1} < M < \left( \frac{N}{\|a_0\|} \right)^{1-\kappa_2} \).

The proof of Theorem 6.1 involves the following steps.

**Proposition 6.2** (Initial dimension). There exist \( \alpha_{ini}, C_1 > 0 \) depending only on \( \nu \) so that for any measure \( \mu_0 \) on \( \mathbb{T}^d \), if \( \mu_n = \nu^n * \mu_0 \) satisfies
\[
|\hat{\mu}_n(a_0)| > t_0
\]
for \( n = n_0, t_0 \in (0, 1/2) \), then for any integer \( m \) with
\[
n_0 > m \geq C_1 \log \frac{1}{t_0}
\]
it holds that
\[
N \left( A_{t_0/2, n_0 - m} \cap B_{0,N}; M \right) \geq \left( \frac{N}{M} \right)^{\alpha_{ini}}
\]
for \( N = \exp(3\lambda_1 m/2) \|a_0\|, M = \|a_0\| \).

**Proposition 6.3** (Improving the large scale dimension). Given \( \alpha_{ini} > 0 \) and \( \alpha_{high} < d \), there exist \( \alpha_{inc}, c_2, C > 0 \) (depending on \( \nu \)) so that if for some \( t \in (0, 1/2) \), \( 1 \leq M < N \) with
\[
\log(\frac{N}{M}) > c_2 \log(\frac{2}{t}) \quad \text{and} \quad n \geq c_2 \log \frac{N}{M}
\]
it holds that
\[
N \left( A_t, n \cap B_{0,N}; M \right) > \left( \frac{N}{M} \right)^{\alpha} \quad \text{for some} \quad \alpha_{ini} \leq \alpha \leq \alpha_{high},
\]
then there are \( m, M', N' \) with \( M' \geq M \),
\[
m \leq c_2 \log \frac{N}{M'}, \quad N' \leq N \left( \frac{N}{M} \right)^{c_2}, \quad \frac{N'}{M'} \geq \left( \frac{N}{M} \right)^{1/c_2},
\]
so that
\[
N \left( A_{t', n - m} \cap B_{0,N'}; M' \right) > \left( \frac{N'}{M'} \right)^{\alpha + \alpha_{inc}}
\]
for \( t' = Ct^{4d} \).

Iterating this proposition we obtain:

**Corollary 6.4** (of Proposition 6.3). Given \( \alpha_{ini} > 0 \) and \( \alpha_{high} < d \), there exist \( c_3, C_3 > 0 \) so that if for some \( t \in (0, 1/2) \), \( 1 \leq M < N \) with \( \log(N/M) > c_3 \log(1/t) \), and \( n \geq c_3 \log(N/M) \) it holds that
\[
N \left( A_t, n \cap B_{0,N}; M \right) > \left( \frac{N}{M} \right)^{\alpha_{ini}}
\]
then there are \( m, M', N' \) with \( M' \geq M \),
\[
m \leq c_3 \log \frac{N}{M'}, \quad N' \leq N \left( \frac{N}{M} \right)^{c_3}, \quad \frac{N'}{M'} \geq \left( \frac{N}{M} \right)^{1/c_3},
\]
so that
\[
N(A_{t',n-m} \cap B_{0,N'}; M') > \left( \frac{N'}{M'} \right)^{\alpha_{\text{high}}}
\]
for \( t' = t^{C_3} \).

**Proposition 6.5** (High dimension to positive density at large scales). There exist \( \alpha_{\text{high}}, c_4, \kappa_4 > 0 \) depending only on \( \nu \) and \( q_4 \) depending on \( d \) with the following properties. Assume that for some \( t \in (0, 1/2) \), \( 1 \leq M < N \) with \( \log(N/M) > c_4 \log(1/t) \), and \( n \geq c_4 \log(N/M) \) it holds that
\[
N(A_{t,n} \cap B_{0,N}; M) > \left( \frac{N}{M} \right)^{\alpha_{\text{high}}}
\]
Then there are \( m, M', N' \) with \( M' \geq M \),
\[
m \leq c_4 \log \frac{N}{M}, \quad N' \leq N \left( \frac{N}{M} \right)^{c_4}, \quad N' \geq \left( \frac{N}{M} \right)^{1/c_4},
\]
such that
\[
N(A_{t_1,n-m} \cap B_{0,N'; M'}) > c_4^{-1} t_1^{\kappa_4} \left( \frac{N'}{M'} \right)^d
\]
for \( t_1 = c_4^{-1} t^{q_4} \).

Let us deduce Theorem 6.1 from the above propositions.

**Proof.** Suppose \( |\hat{\mu}_{n_0}(a_0)| \geq t_0 \). Then by Proposition 6.2 there are \( \alpha_{\text{ini}}, c_1 \) so that
\[
N(A_{t_0/2,n_0-m_1} \cap B_{0,N_1}; M_1) \geq (N_1/M_1)^{\alpha_{\text{ini}}}
\]
for \( N_1 = \exp(3\lambda_1 m_1/2) \| a_0 \| \), \( M_1 = \| a_0 \| \) provided \( n_0 \geq m_1 \geq C_1(1 + |\log t_0|) \).

Let \( \alpha_{\text{high}} < d \) be as in Proposition 6.5 and let \( c_3, C_3 \) be as in Corollary 6.4 for the already chosen values of \( \alpha_{\text{ini}}, \alpha_{\text{high}} \). Then if
\[
\log \frac{N_1}{M_1} = \frac{3m_1 \lambda_1}{2} > c_3(1 + \log \frac{2}{t_0}),
\]
\[
n_0 - m_1 > c_3 \log \frac{N_1}{M_1},
\]
there are \( m_2 \leq c_3 \log \frac{N_1}{M_1} \) and \( N_2, M_2 \) with
\[
N_2 < N_1 \left( \frac{N_1}{M_1} \right)^{c_3}, \quad N_2 \geq \left( \frac{N_1}{M_1} \right)^{1/c_3}
\]
so that
\[
N(A_{t_1,n_0-m_1-m_2} \cap B_{0,N_2}; M_2) > \left( \frac{N_2}{M_2} \right)^{\alpha_{\text{high}}}
\]
with \( t_2 = (t_0/2)^{C_3} \).

As long as
\[
\log \frac{N_2}{M_2} > c_4 \log \frac{2}{t_2}
\]
and
\[
n_0 - m_1 - m_2 \geq c_4 \log \frac{N_2}{M_2},
\]
we can apply Proposition 6.5 and conclude that for some \( N_3, M_3 \) with
\[
m_3 \leq c_4 \log \frac{N_2}{M_2}, \quad N_3 \leq N_2 \left( \frac{N_2}{M_2} \right)^{c_4}, \quad N_3 \geq \left( \frac{N_2}{M_2} \right)^{1/c_4}
\]
we have that
\[
\mathcal{N}(A_{t_3,n_0-m_1-m_2-m_3} \cap B_{0,N_3};M_3) > c_4^{-1} t_3^{c_4} \left( \frac{N_2}{M_3} \right)^d
\]
with \( t_3 = (t_2)^{q_4} \), proving the theorem.

\[\Box\]

6. A. Initial dimension and regularity: Proof of Proposition 6.2

**Proof of Proposition 6.2.** Let \( \omega = \lambda_1/4 \), and let \( C_1 > 2 \) be a large constant to be determined later. For any fixed \( m > C_1 (1 + |\log(t_0)|) \) set
\[
N = e^{(\lambda_1 + 2\omega)m} \|a_0\|, \quad R = e^{(\lambda_1 - 2\omega)m} \|a_0\|.
\]

Let \( t' = \frac{t_0}{2} \) and \( n' = n_0 - m \). Consider the following sets:
\[
\begin{align*}
G_{\text{len}} &= \left\{ g \in \Gamma : e^{(\lambda_1 - \omega)m} < \|g\| = \|g^{tr}\| < e^{(\lambda_1 + \omega)m} \right\}, \\
G_{\text{stat}} &= \left\{ g \in \Gamma : \|\mu_{t'}(g^{tr}a_0)\| \geq t' \right\}, \\
G_{\text{ang}} &= \left\{ g \in \Gamma : d_\perp(\bar{a}_0, H(g)) > \min \left( \epsilon^{-\rho_0}(t_0), \left( \frac{t_0}{8} \right)^{1/\tau} \right) \right\}, \\
G &= G_{\text{len}} \cap G_{\text{stat}} \cap G_{\text{ang}},
\end{align*}
\]

where \( \tau \) and \( m_0 \) are as in Lemma 4.5 and we recall that
\[
d_\perp(\bar{a}_0, H(g)) = d_\perp(\theta(g), a_0^\perp).
\]

By Theorem 4.3 there is \( \rho_0 > 0 \) so that (assuming \( m > m_0 \))

\[
\nu^m(G_{\text{len}}) > 1 - e^{-\rho_0 m}.
\]

Our choice of \( C_1 \) should guarantee \( m > m_0, e^{-\rho_0 m} < \frac{t_0}{8}, m > m_0, \) and \( e^{-\tau m} < \frac{t_0}{8} \).

There exists \( m_1 \) so that for \( m > m_1 \) Lemma 4.5 gives

\[
\nu^m(G_{\text{ang}}) > 1 - \frac{t_0}{8}.
\]

Finally, the fact that \( \mu_{n_0} = \nu^m * \mu_{n'} \) gives

\[
\nu^m(G_{\text{stat}}) > \frac{t_0}{2}.
\]

Therefore
\[
\nu^m(G) > \frac{t_0}{2} - \frac{t_0}{8} - \frac{t_0}{8} = \frac{t_0}{4}.
\]

Since \( \|g^{tr}\| = \|g\| \) and \( d_\perp(\bar{x}, H(g^{tr})) = d_\perp(\theta(g), \bar{x}^\perp) \), by Lemma 4.1(2) every \( g \in G \subset G_{\text{ang}} \cap G_{\text{len}} \) has
\[
\|g^{tr}a_0\| \geq \|g^{tr}\| \cdot \|a_0\| \cdot d_\perp(\bar{a}, H(g^{tr})) > e^{(\lambda_1 - \omega)m} \|a_0\| \cdot \left( \frac{t_0}{8} \right)^{1/\tau}.
\]
If \( m > (\omega \cdot \tau)^{-1} \cdot \log(8/t_0) \), which is true for large \( C_1 \), then the right-hand side above is bigger than \( R \). It is also clear that \( \|g^{tr}a_0\| < N \) if \( g \in \mathcal{G}_{len} \). For \( g \in \mathcal{G}_{stat} \) it also holds that \( g^{tr}a_0 \in A_{\nu', \nu'} \). Therefore for \( g \in \mathcal{G} \subset \mathcal{G}_{len} \cap \mathcal{G}_{stat} \),

\[
g^{tr}a_0 \in A := A_{\nu', \nu'} \cap (B_0,N \setminus B_{0,R}) = \{ R < \|b\| \leq N : |\mu_{\nu'}(b)| > t' \}.
\]

Let \( D \) be the projection of \( A \) to \( \mathbb{P}^{d-1} \). Then

\[
\nu^{*m} \{ g : g^{tr}a_0 \in D \} \geq \frac{t_0}{4}
\]

and

\[
\mathcal{N} \left( D; e^{-(\lambda_1 - 2\omega)m} \right) \leq \mathcal{N}(A; \|a_0\|).
\]

It follows that

\[
\nu^{*m} \{ g : g^{tr}a_0 \in D \} \leq \mathcal{N} \left( D; e^{-(\lambda_1 - 2\omega)m} \right) \cdot \max_{g \in \mathbb{P}^{d-1}} \nu^{*m} \left\{ g : d_\mathcal{L}(g^{tr}a_0, \bar{g}) < e^{-(\lambda_1 - 2\omega)m} \right\} \leq \mathcal{N} \left( D; e^{-(\lambda_1 - 2\omega)m} \right) e^{-\tau'm}
\]

for some \( \tau' > 0 \) depending only on \( \nu \). It follows that

\[
\mathcal{N}(A; \|a_0\|) \geq \frac{t_0}{4} e^{\tau'm} \geq e^{\tau'm/2}
\]

if \( C_1 \) is large enough. \( \square \)

6.B. Bootstrap of large scale dimension: Proof of Proposition [6.3] A central step in the proof of Theorem [5] is the bootstrap procedure, which allows us to increase the large-scale “dimension” of the set of large Fourier coefficients from \( \alpha \) to \( \alpha + \alpha_{inc} \). In order to show this, we employ the following projection theorem due to the first author which implicitly can be found in [4] and is proved explicitly in [3].

**Theorem 6.6** ([5 Thm. 5]). For any \( \alpha_0, \kappa > 0 \) and \( d \geq 2 \) there are \( \alpha_\Delta, \epsilon_0, r_0, \tau_0 > 0 \) such that the following holds for \( 0 < r < r_0 \) and \( \alpha_0 < \alpha < d - \alpha_0 \): Let \( \eta \) be a probability measure on \( \mathbb{P}^{d-1} \) s.t.

\[
(6.11) \quad \max_y \eta(V(y^{\perp}, \rho)) < \rho^\kappa \quad \text{if} \quad r < \rho < r^{\tau_0}.
\]

Let \( E \subset [0,1]^d \) be an \( r \)-separated set with \( |E| > r^{-\alpha} \) and a nonconcentration property

\[
\max_x |E \cap B_x, \rho| < \rho^\kappa|E| \quad \text{if} \quad r < \rho < r^{\tau_0}.
\]

Then there exist \( D \subset \mathbb{P}^{d-1} \) and \( E' \subset E \) with

\[
\eta(D) > 1 - r^{-\alpha}, \quad |E'| > r^\alpha|E|
\]

so that

\[
\mathcal{N}(\pi_\theta(E''); r) > r^{-(\alpha + \alpha_\Delta)/d}
\]

whenever \( \theta \in D \) and \( E'' \subset E' \) satisfies \( |E''| > r^{2\alpha}|E| \).
Lemma 6.7. For any $\epsilon > 0$, there is a $C_\epsilon > 0$ so that the following holds. Let $\mu$ be a probability measure on $\mathbb{T}^d$ and let

$$A_t(\mu) = \{ b \in \mathbb{Z}^d : |\hat{\mu}(b)| > t \}.$$ 

Assume that for some $N > M, \alpha$

$$N(A_t(\mu) \cap B_{0,N}; M) \geq \left( \frac{N}{M} \right)^{\alpha}.$$ 

Then there is an $M < N' < N$ with

$$\log \frac{N'}{M} > \left( \frac{d - \alpha + \epsilon}{d - \alpha + 8\epsilon} \right) \log \frac{N}{M}$$

so that $A_{t/4}(\mu) \cap B_{0,N'}$ contains a subset which is $(C_\epsilon t^{-2}, \alpha - 10\epsilon)$-regular at scale $M$.

Proof. By Lemma 5.2 there is a point $x \in B_{0,N}$ so that $A \cap B_{x,N'}$ supports a probability measure $\rho$ which is $(C_\epsilon, \alpha - 9\epsilon)$-regular measure at scale $M$ with

$$\frac{N'}{M} = \left( \frac{N}{M} \right)^{\frac{d - \alpha + \epsilon}{d - \alpha + 8\epsilon}}.$$ 

Replacing $C_\epsilon$ by $4C_\epsilon$, we may assume all $b \in \text{supp}(\rho)$ satisfy that $\hat{\mu}(b)$ lie in a single quadrant of $\mathbb{C}$, and hence

$$\left| \sum_b \rho(b)\hat{\mu}(b) \right| \geq \frac{t}{\sqrt{2}}.$$ 

By Cauchy-Schwartz,

$$\sum_{b,b_1} \hat{\mu}(b - b_1)\rho(b)\rho(b_1) = \int_{\mathbb{T}^d} \left| \sum_b \rho(b) e(b \cdot x) \right|^2 \, dx \geq \left| \int_{\mathbb{T}^d} \sum_b \rho(b) e(b \cdot x) \, dx \right|^2 \geq \left| \sum_b \hat{\mu}(b)\rho(b) \right|^2 \geq \frac{t^2}{2};$$

hence

(6.12) $$\rho \ast \hat{\rho}(A_{t/4}(\mu)) \geq \frac{t^2}{4}.$$ 

Let $\rho_2$ be the probability measure $\rho \ast \hat{\rho}|_{A_{t/4}(\mu)}$. As $\rho$ was $(4C_\epsilon, \alpha - 9\epsilon)$-regular on $B_{x,N'}$, the measure $\rho \ast \hat{\rho}$ is $(2^{d+2}C_\epsilon, \alpha - 9\epsilon)$-regular on $B_{0,2N'}$; hence by (6.12)

$$\rho_2$$

is $(2^{d+4}C_\epsilon t^{-2}, \alpha - 9\epsilon)$-regular on $B(0,2N')$.

By Lemma 5.3 there is some

$$\tilde{A} \subset \text{supp}(\rho_2) \subset A_{t/4}(\mu) \cap B_{0,N'}$$

which is $M$-separated and $(C'_\epsilon t^{-2}, \alpha - 10\epsilon)$-regular on $B_{0,N'}$. \hfill \square

---

3 Our convention is that for any measure $\rho$ and set $E$, $\rho|_E(A) = \rho(A \cap E)/\rho(E)$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Lemma 6.8. Given $\alpha_{\text{ini}} > 0$ and $\alpha_{\text{high}} < d$, there exist $\alpha_{\text{inc}}, c_6, C > 0$ (depending on $\nu$) so that if for some $t \in (0, 1/2)$, $1 \leq M < N$ with
\[
\log \frac{N}{M} > c_6 \log \frac{1}{t} \quad \text{and} \quad n \geq c_6 \log \frac{N}{M}
\]
it holds that
\[
N(A_{t,n} \cap B_{0,N}; \alpha) > \left( \frac{N}{M} \right)^{\alpha}
\]
for some $\alpha_{\text{ini}} \leq \alpha \leq \alpha_{\text{high}}$,
then there are $m, M', N'$ with $M' \geq M$,
\[
m \leq c_6 \log \frac{N}{M'}, \quad N' \leq N \left( \frac{N}{M} \right)^{c_6}, \quad \frac{N'}{M'} \geq \left( \frac{N}{M} \right)^{1/c_6}
\]
and $\xi \in \mathbb{P}^{d-1}$ so that if $R$ denotes the “rectangle” $B_{0,N'} \cap \text{Nbd}_{M'}(\xi)$,
\[
N(A_{t,n-m} \cap R; M') > \left( \frac{N'}{M'} \right)^{(\alpha+2\alpha_{\text{inc}})/d}
\]
for $t' = Ct^4$.

Proof. Let $\alpha_{\Delta}, \epsilon_0$ be as in Theorem 6.6 for $\alpha_0 = \kappa = \min(\alpha_{\text{ini}}, d - \alpha_{\text{high}})/2$. Since the statement of Theorem 6.6 becomes weaker if either $\alpha_{\Delta}$ or $\epsilon_0$ is decreased, we may as well assume $\epsilon_0 = \alpha_{\Delta}/10$ for simplicity.

By Lemma 6.7 applied with $\epsilon = \alpha_{\Delta}/20$, there is an $M < N_1 < N$ with
\[
\log(N_1/M) > c \log(N/M)
\]
and an $M$-separated subset
\[
A \subset A_{t/4,n} \cap B_{0,N_1}
\]
which is $(Ct^{-2}, \alpha - \alpha_{\Delta}/2)$-regular at scale $M$ on $B_{0,N_1}$; in particular
\[
|A| > C^{-1} t^2 \left( \frac{N_1}{M} \right)^{\alpha - \alpha_{\Delta}/2}.
\]
Both the constants $c$ and $C$ depend only on $\alpha_{\text{ini}}$ and $\alpha_{\text{high}}$ (and $\alpha_{\Delta}$ which is determined by these two quantities).

Let $\omega > 0$ be small (specifically, we require that $\omega < \min(\lambda_1 - \lambda_2, \lambda_1, \alpha_{\Delta})/20$) and let $m$ be the smallest integer so that
\[
e^{(\lambda_1 - \lambda_2 - 2\omega)m} > \frac{N_1}{M}.
\]
Let $n' = n - m$ and set $M', N'$ by
\[
(m1) \quad N' = e^{(\lambda_1 + \omega)m} \cdot N_1,
(m2) \quad M' = e^{(\lambda_1 - \omega)m} \cdot M;
\]
then also
\[
(m3) \quad e^{(\lambda_2 + \omega)m} \cdot N_1 \leq M'.
\]
Assuming the constant $c_6$ in (6.13) is sufficiently large, we will have that $m$ is greater than or equal to the constant $m_0(\omega)$ in Theorem 4.3 Invoking that theorem, we conclude that the set
\[
\mathcal{G}_{\text{len}} = \left\{ g \in \Gamma : |\lambda_i - \frac{1}{m} \log \sigma_i(g)| < \omega \quad \text{for} \quad i = 1, 2 \right\}
\]
satisfies
\[ \nu^* m(G_{\text{len}}) > 1 - e^{-p_{\omega} m}. \]

Conditions (m1)–(m3) imply that for any \( g \in G_{\text{len}} \)
\[ g^r(B_{0,N_1}) \subset B_{0,N'} \cap \text{Nbd}_{M'}(\xi) \quad \text{with} \quad \xi = \theta(g^r), \]
i.e., the linear transformation \( g^r \) maps the ball \( B_{0,N_1} \) into a cylinder of length \( 2N' \) and base of radius \( M' \).

Let \( \eta \in \text{Prob}(\mathbb{P}^{d-1}) \) denote the distribution of \( \theta(g) \) where \( g \in \Gamma \) is distributed according to \( \nu^* m \), i.e., \( \eta(\Theta) = \nu^* m \{ g \in \Gamma : \theta(g) \in \Theta \} \). Lemma \ref{reglem} provides the regularity of \( \eta \) as in condition \ref{regularity} of Theorem \ref{mainthm}.

Let \( E = N_1^{-1} \cdot A \subset B_{0,1} \subset \mathbb{P}^{d-1} \) and \( r = M/N_1 \). Theorem \ref{distthm} gives us a set \( E' \subset E \) with \( |E'| > r^{\alpha_\Delta/10} |E| \) and \( \Theta \subset \mathbb{P}^{d-1} \) with \( \eta(\Theta) > 1 - r^{\alpha_\Delta/10} \) so that
\[ \mathcal{N}(\pi_\theta(E''):r) \geq r^{-(\alpha + \frac{2}{5} \alpha_\Delta)/d} \forall E'' \subset E', \theta \in \Theta \text{ with } |E''| > r^{\alpha_\Delta/10} |E'|. \]

Let \( B = N_1 E' \) and \( G_{\text{proj}} = \{ g \in \Gamma : \theta(g) \in \Theta \} \).

We have
\[ \nu^* m(G_{\text{proj}}) = \eta(\Theta) > 1 - r^{\alpha_\Delta/10}. \]

Since \( b \in B \subset A \subset A_{\ell^d/A,n} \), we have that \( |\hat{\mu}_n(b)| > \frac{1}{4} t^2 \) for all \( b \in B \); by reducing \( B \) slightly, we may also assume that \( |B|^{-1} \sum_{b \in B} \hat{\mu}_n(b) \geq \frac{1}{4} t^2 \). Using the identity \( \mu_n = \nu^* m \ast \mu_n \) (recall that \( n' = n - m \)) and the Cauchy-Schwartz inequality, we may conclude that
\[ \sum_{g \in \Gamma} \nu^* m(g) \cdot \frac{1}{|B|} \sum_{b \in B} |\hat{\mu}_n'(g^{rr}b)|^2 \geq \left[ \frac{1}{|B|} \sum_{g \in \Gamma} \sum_{b \in B} \nu^* m(g) \hat{\mu}_n'(g^{rr}b) \right]^2 = \left[ \frac{1}{|B|} \sum_{b \in B} \hat{\mu}_n(b) \right]^2 > 2^{-6} t^4 \]
and therefore the set
\[ G_{\text{stat}} = \left\{ g \in \Gamma : \frac{1}{|B|} \sum_{b \in B} |\hat{\mu}_n'(g^{rr}b)|^2 > 2^{-7} t^4 \right\} \]
has
\[ \nu^* m(G_{\text{stat}}) > 2^{-7} t^4. \]

Note that for each \( g \in G_{\text{stat}} \) the set
\[ B_g = \{ b \in B : |\hat{\mu}_n'(g^{rr}b)|^2 > 2^{-8} t^4 \} \]
has \( |B_g| > 2^{-8} t^4 \cdot |B| \). Let \( G = G_{\text{len}} \cap G_{\text{proj}} \cap G_{\text{stat}} \). From (6.18), (6.17), and (6.15) we have
\[ \nu^* m(G) > 2^{-7} t^4 - r^{\alpha_\Delta/10} - e^{-p_{\omega} m} > 2^{-8} t^4, \quad \text{where} \quad r = \frac{M}{N_1}, \]
assuming \( r^{\alpha_\Delta/10}, e^{-p_{\omega} m} < 2^{-9} t^4 \) which is guaranteed by taking \( c_6 \) large enough.
Moreover, for any \( g \in \mathcal{G} \) we have that \( |B_g| > 2^{-8t^4} \cdot |B| \) and (assuming as we may that \( 2^{-8t^4} > r^{\alpha \Delta /10} \)) by (6.10) \[
\mathcal{N}(\pi_\xi(B_g); M) \geq \tau^{-2(\alpha + \frac{1}{2} \Delta)} \] which in view of (6.20) implies (6.14).


\begin{lemma}
Let \( \xi \in \mathbb{T}^{d-1} \), and let \( R = B_{0, N_1} \cap \text{Nbd}_{M_1}(\xi) \). Then there are \( m_2, M_2, M_1 \) with
\[
m_2, |\log(N_1) - \log(N_2)|, |\log(M_1) - \log(M_2)| \leq c_7 \log(1/t_1)
\]
so that for \( t_2 = (t_1/8)^{2d} \)
\[
\mathcal{N}(A_{t_1, n_1 - m_2} \cap B_{0, N_2}; M_2) \geq c_7^{-1} t_1^{16} \mathcal{N}(A_{t_1, n_1} \cap R; M_1)
\]
where \( c_7 \) also depends only on \( \nu \).
\end{lemma}

\begin{proof}
Let \( \omega = (\lambda_1 - \lambda_2)/10 \), and let \( m_2 \) be such that the sets
\[
\mathcal{G}_\text{len} = \left\{ \tilde{g} \in \Gamma^d : |\lambda_i - \frac{1}{m_2} \log \sigma_i(g_j)| < \omega \quad \text{for } i = 1, 2 \text{ and } j = 1, \ldots, d \right\},
\]
\[
\mathcal{G}_\text{ang} = \left\{ \tilde{g} \in \Gamma^d : d_\mathcal{L}(\xi, H_g(\tilde{g}_1)) \geq 2e^{-\omega m_2} \quad \text{for } j = 1, \ldots, d \right\},
\]
\[
\mathcal{G}_\text{vol} = \left\{ \tilde{g} \in \Gamma^d : \text{vol}(\theta(\tilde{g}_1), \ldots, \theta(\tilde{g}_d)) > \left( \frac{t_1}{8} \right)^{2d} \right\} \quad \text{(p as in Lemma 4.6)}
\]
satisfy
\[
\min((\nu^{\delta m_2})^{d(\mathcal{G}_\text{len})}, (\nu^{\delta m_2})^{d(\mathcal{G}_\text{ang})}, (\nu^{\delta m_2})^{d(\mathcal{G}_\text{vol})}) \geq 1 - \frac{1}{6}(t_1/4)^{2d}.
\]
By Lemma 4.6, Theorem 4.4 and Theorem 4.7 one can find such \( m_2 \) with \( m_2 < \tau_1 |\log t_1| \) for some constant \( \tau_1 \). In particular if the constant \( c_7 \) of (6.21) is sufficiently large, \( n_2 = n_1 - m_2 > 0 \), which we shall assume henceforth.

Let \( E \subset A_{t_1, n_1} \cap R \) be an \( M_1 \)-separated set such that the following hold:

\begin{enumerate}
\item[(E1)] For every distinct \( b, b' \in E \)
\[
d_\mathcal{L}(\xi, \frac{b - b'}{|b - b'|}) \leq e^{-\omega m_2}.
\]
\item[(E2)] \( |\sum_{b \in E} \hat{\mu}_{n_1}(b) - \frac{1}{2}t_1 |E| \|
\]
\end{enumerate}
Clearly one can find such an \( E \) so that
\[
|E| \geq c e^{-\varphi m_2} \mathcal{N}(A_{t_1, n_1} \cap R; M_1)
\]
where \( c \) is some constant depending only on \( d \). Note that in order to satisfy (E2) one can, e.g., take \( E \) so that \( \{ \hat{\mu}_{n_1}(b) : b \in E \} \) lie in a single quadrant of \( \mathbb{C} \).
Write $G(x) = |E|^{-1} \sum_g \nu^{*m_2}(g) \sum_{b \in E} e_g \cdot b(x)$. Then

$$2^{-2d} t_1^{2d} \leq \left| \frac{1}{|E|} \sum_{b \in E} \widehat{\mu}(b) \right|^{2d} = \left| \frac{1}{|E|} \sum_g \nu^{*m_2}(g) \widehat{\mu}(g \cdot b) \right|^{2d}$$

$$= \left( \int G(x) \, d\mu_n(x) \right)^{2d} \leq \int |G(x)|^{2d} \, d\mu_n(x)$$

(6.24)

$$= \frac{1}{|E|^{2d}} \sum_{g_1, \ldots, g_{2d}} \nu^{*m_2}(g_1) \cdots \nu^{*m_2}(g_{2d}) \cdot \sum_{b_1, \ldots, b_{2d} \in E} \widehat{\mu}(g_1 \cdot b_1 + \cdots + g_{2d} \cdot b_{2d}) - g_{d+1}^{tr} b_{d+1} - \cdots - g_{2d}^{tr} b_{2d}.$$ 

Set $\Sigma(g_1, \ldots, g_d)(\vec{b}) = \sum_{i=1}^d g_i^{tr} b_i$. Fix $(g_{d+1}, \ldots, g_{2d}) \in G_{\text{len}}$ and $b_{d+1}, \ldots, b_{2d} \in E$ with

$$|E|^{-d} \sum_{g_1, \ldots, g_{2d}} \nu^{*m_2}(g_1) \cdots \nu^{*m_2}(g_{2d}) \sum_{b \in E} |\widehat{\mu}(\Sigma(g_1, \ldots, g_d)(\vec{b}) - \vec{b})| \geq \left( \frac{t_1}{4} \right)^{2d}$$

where $\vec{b} = g_{d+1}^{tr} b_{d+1} + \cdots + g_{2d}^{tr} b_{2d}$. Such a choice exists in view of the estimate (6.23) on the measure of $G_{\text{len}}$ and (6.24). Set

$$G_{\text{stat}} = \left\{ \vec{g} \in \mathbb{R}^d : |E|^{-d} \sum_{b \in E} |\widehat{\mu}(\Sigma_{\vec{g}}(\vec{b}) - \vec{b})| > \frac{1}{2} \left( \frac{t_1}{4} \right)^{2d} \right\}.$$ 

In view of (6.25), $(\nu^{*m_2})^d(G_{\text{stat}}) \geq \frac{1}{2} (t_1/4)^{2d}$; hence by (6.23) the set $G = G_{\text{stat}} \cap G_{\text{vol}} \cap G_{\text{len}} \cap G_{\text{ang}}$ is nonempty. Let $t_2 = (t_1/8)^{2d}$.

We claim that if

$$t_2 e^{(\lambda_1 - 2\omega)m_2} > 4de^{(\lambda_2 + \omega)m_2},$$

then for any $\vec{g} \in G$,

$$\mathcal{N}(A_{t_2, n_2} \cap (\Sigma_{\vec{g}}(E^d) - \vec{b}); M_2) \geq t_2 |E|^d$$

with $M_2 = \frac{1}{4} t_2 e^{(\lambda_1 - 2\omega)m_2} M_1$; note that $\vec{g}, (g_{d+1}, \ldots, g_{2d}) \in G_{\text{len}}$ and $E \subset B_{0, N_1}$ imply

$$\Sigma_{\vec{g}}(E^d) - \vec{b} \subset B_{0, N_2}$$

where $N_2 = 2de^{(\lambda_1 + \omega)m_2} N_1$.

As

$$|E| \geq ce^{-d\omega m_2} \mathcal{N}(A_{t_1, n_1} \cap R; M_1),$$

it follows from (6.26) and (6.27) that

$$\mathcal{N}(A_{t_2, n_2} \cap B_{0, N_2}; M_2) \geq c't_2 e^{-d \omega m_2} \mathcal{N}(A_{t_1, n_1} \cap R; M_1)^d,$$

establishing Lemma (6.9 assuming the claim (6.26)).

We now turn to proving (6.20). Let $\xi_i = \theta(g_i^{tr})$ for $i = 1, \ldots, d$. We shall use the following auxiliary expression, which is meant to approximate $\Sigma_{\vec{g}}(\vec{b})$:

$$\Sigma_{\vec{g}}(\vec{b}) = \sum_{i=1}^d \pi_{\xi_i}(g_i^{tr} b_i),$$
where we consider \( \pi_{\xi_j} \) as a rank one map \( \mathbb{R}^d \rightarrow \mathbb{R}^d \) whose image is in the vector space spanned by \( \xi_j \). Indeed, for \( \tilde{g} \in \mathcal{G}_{\text{ten}} \)
\[
\left\| \Sigma_{\tilde{g}}(\tilde{b}) - \Sigma_{\tilde{g}}(\tilde{b}) \right\| \leq e^{(\lambda_2 + \omega) m_2} \sum_i \|b_i\| .
\]

Let \( \tilde{b}^{(i)} = (b_1^{(i)}, \ldots, b_d^{(i)}) \) \( (i = 1, 2) \) be two distinct points in \( E^d \); assume they differ in the \( j \)th coordinate \( b_j^{(i)} \). Write \( b_j = b_j^{(1)} - b_j^{(2)} \) as \( b_j' + b_j'' \) with \( b_j'' \in H(g_j^{(r)}) \) and \( b_j' \perp b_j'' \). As \( E \) is \( M_1 \)-separated, \( \|b_j\| \geq M_1 \). Then \( d_\xi (\xi_j, b_j/\|b_j\|) < e^{-\omega m_2} \) (cf. (E1)); hence as \( \tilde{g} \in \mathcal{G}_{\text{ang}} \)
\[
d_\xi \left( \frac{b_j}{\|b_j\|}, H(g_j) \right) \geq d_\xi (\xi, H(g_j^{(r)})) - d_\xi \left( \frac{b_j}{\|b_j\|}, \xi \right) \geq e^{-\omega m_2}
\]
and
\[
|b_j'| \geq e^{-\omega m_2} |b_j| \geq e^{-\omega m_2} M_1 .
\]
In this notation, \( \pi_{\xi_j} (g_j^{(r)} b_j) = g_j^{(r)} b_j' \), and it follows that
\[
\|\pi_{\xi_j} (g_j^{(r)} b_j)\| \geq e^{(\lambda_1 - 2\omega) m_2} \|b_j\| .
\]
Then as \( \tilde{g} \in \mathcal{G}_{\text{vol}} \)
\[
\left\| \Sigma_{\tilde{g}}(\tilde{b}^{(1)}) - \tilde{b}^{(2)} \right\| \geq \text{vol}(\Sigma_{\tilde{g}}(\tilde{b}^{(1)}) - \tilde{b}^{(2)}), \xi_1, \ldots, \xi_j, \ldots, \xi_{j+1}, \ldots, \xi_d)
\]
\[
= \left\| \pi_{\xi_j} (g_j^{(r)} b_j) \right\| \text{vol}(\xi_1, \ldots, \xi_d)
\]
\[
\geq \frac{1}{2} d_{\xi_j} e^{(\lambda_1 - 2\omega) m_2} \|b_j\| .
\]
Hence
\[
\left\| \Sigma_{\tilde{g}}(\tilde{b}^{(1)}) - \tilde{b}^{(2)} \right\| \geq \frac{1}{2} d_{\xi_j} e^{(\lambda_1 - 2\omega) m_2} \|b_j\| - de^{(\lambda_2 + \omega) m_2} \|b_j\|
\]
under the assumption that this last expression is
\[
\geq \frac{1}{2} d_{\xi_j} e^{(\lambda_1 - 2\omega) m_2} \|b_j\| \geq M_2
\]
from which it follows that \( \Sigma_{\tilde{g}}(E^d) \) is \( M_2 \)-separated and (6.26) is proved, concluding the proof of Lemma 6.9. \( \square \)

**Proof of Proposition 6.3.** Apply Lemma 6.8 to find \( N_1, M_1, m_1, n_1 = n - m_1 \) with
\[
m_1 \leq c_6 \log(N/M), \quad N_1 \leq N(N/M)^{c_6}, \quad (N_1/M_1) \geq (N/M)^{1/c_6}
\]
and a \( \xi \in \mathbb{R}^{d-1} \) so that
\[
(6.28) \quad \mathcal{N} (A_{t_1, n_1} \cap R; M_1) > \left( \frac{N_1}{M_1} \right)^{(\alpha + 2\alpha_{\text{inc}})/d} (t_1 = Ct^4)
\]
with \( R = B_{0, N_1} \cap \text{Nbd}_{M_1}(\xi) \). Now apply Lemma 6.9 to find \( m_2, n_2 = n_1 - m_2, M_2, N_2 \) with
\[
m_2, |\log(N_1) - \log(N_2)|, |\log(M_1) - \log(M_2)| \leq c_7 \log(1/t_1)
\]
so that
\[
\mathcal{N} (A_{t_2, n_2} \cap B_{0, N_2}; M_2) \geq c_7 t_2 \mathcal{N} (A_{t_1, n_1} \cap R; M_1)
\]
\[
\geq c_7 t_2 \left( \frac{N_1}{M_1} \right)^{(\alpha + 2\alpha_{\text{inc}})}
\]
with \( t_2 = (t_1/8)^{2d} \). Note that by choosing \( c_2 \) of (6.3) to be large enough guarantees that (6.21) holds. Moreover, if this constant \( c_2 \) is large enough,

\[
c_7 t_1^{\alpha} \left( \frac{N_1}{M_1} \right)^{\alpha + 2\alpha_{\text{inc}}} > \left( \frac{N_2}{M_2} \right)^{\alpha + \alpha_{\text{inc}}},
\]

establishing Proposition 6.3. \( \Box \)

6.C. From high dimension to positive density: Proof of Proposition 6.5. Underlying (and motivating) the proof of Proposition 6.5 is the following theorem of Falconer [13] regarding projection of sets. Falconer shows that if \( \eta \) is a measure on the set of directions with dimension \( \beta > 0 \), then if the dimension of \( \rho \) is larger than \( d - \beta \), one has that for \( \eta \) almost every direction \( \theta \) the projection \( \rho_\theta \) of \( \rho \) in the direction \( \theta \) is absolutely continuous with respect to Lebesgue measure; we follow the treatment of this result by Peres and Schlag in [28, Sec. 6]. In fact, the argument gives a much more quantitative result connecting the \( \alpha \)-energy of \( \rho \) to the projections of \( \rho \).

We need a version of this theorem for measures \( \rho \) which are \((C, \alpha)\)-regular at some scale \( r \) but are possibly singular at finer scales (indeed the measure we shall consider will be purely atomic). As we have already remarked in Section 5, this can be achieved by applying Falconer’s theorem to \( \rho \) convolved with an appropriate smoothing function.

Let \( \Phi \) be a fixed radially symmetric nonnegative smooth function on \( \mathbb{R}^d \) with \( \| \Phi \|_1 = 1 \) supported on \( B_{0,1} \), and set for \( r > 0 \)

(6.29) \[
\Phi_r(x) = r^{-d} \Phi(r^{-1}x).
\]

Let \( \Psi : \mathbb{R} \to \mathbb{R}^+ \) be the smooth compactly supported function

\[
\Psi(x_1) = \int dx_2 \ldots \int dx_d \Phi(x_1, x_2, \ldots, x_d),
\]

and define \( \Psi_r \) analogously to (6.29).

**Lemma 6.10.** Let \( \rho \) be a probability measure on \( \mathbb{R} \), and let \( \phi \) be the Radon-Nykodym derivative \( \phi = \frac{d(\rho*\Psi_r)}{dx} \). Then for every \( r < r_1 < 1 \)

(6.30) \[
\mathcal{N}(\text{supp } \rho; r_1) \geq (4r_1 \| \phi \|_2^2)^{-1}.
\]

Moreover, for any subset \( X \subset \text{supp } \rho \),

(6.31) \[
\mathcal{N}(X; r_1) \geq \frac{\rho(X)^2}{4r_1 \| \phi \|_2^2}.
\]

**Proof.** Let \( B = \text{supp } \rho + [-r, r] \), and let \( 1_B \) be the corresponding indicator function. Then the Lebesgue measure of \( B \) satisfies \( \lambda(B) \leq 4r_1 \mathcal{N}(\text{supp } \rho; r_1) \). By Cauchy-Schwartz

\[
1 = \int 1_B(x) \phi(x) \, dx \leq \| 1_B \|_2 \| \phi \|_2.
\]

Since \( \| 1_B \|_2 = \sqrt{\lambda(B)} \), equation (6.30) follows.
To see (6.31), apply (6.30) on the probability measure \( \rho \mid X \) defined by \( \rho \mid X(Y) = 1/\rho(X \cap Y) \); one has
\[
\frac{d(\rho \mid X \ast \Psi_r)}{dx}(y) = \begin{cases} 
\frac{1}{\rho(X)} d(\rho \ast \Psi_r)(y) & \text{if } y \in X, \\
0 & \text{if } y \not\in X;
\end{cases}
\]
hence \( \|d(\rho \mid X \ast \Psi_r)/dx\|_2^2 \leq \rho(X)^{-2} \|d(\rho \ast \Psi_r)/dx\|_2^2 \). \( \Box \)

**Proposition 6.11.** Let \( \rho \) be a probability measure supported on the unit ball \( B_{0,1} \) of \( \mathbb{R}^d \) so that \( \mathcal{E}_\alpha(\rho) < \infty \) for some \( 0 < \alpha < d, 0 < r < 1 \), and let \( \eta \) be a measure on \( S^{d-1} \) such that for some \( c_\eta, \beta > 0 \)
\begin{equation}
(6.32) \quad \eta(B_{\theta, \epsilon}) \leq c_\eta \epsilon^\beta \quad \text{for every } \epsilon > r \text{ and } \theta \in S^{d-1}.
\end{equation}

Then for any \( \beta' < \beta \)
\begin{equation}
(6.33) \quad \int_{\theta} \int \left| \hat{\rho}(t) \right|^2 \left| \hat{\Psi}_r(t) \right|^2 (1 + |t|)^{\beta' + \alpha - d} dt \, d\eta(\theta)
\leq c_\eta C_d \int_{\mathbb{R}^d} \left| \hat{\rho}(x) \right|^2 \left| \hat{\Phi}_r(x) \right|^2 (1 + |x|)^{\alpha - d} dx + c_\eta C(\alpha, \beta, \beta', d).
\end{equation}

**Interpretation:** if \( \alpha + \beta' > d \) and \( \eta \) is \( (C, \alpha') \)-regular at scale \( r \) for \( \alpha' > \alpha \), then by (6.32) the right-hand side of (6.33) is bounded from above by a constant (depending on \( \alpha, \alpha', \beta, \beta', \alpha', \ldots \)) while the left-hand side dominates
\[
\int_{\theta} \left\| \frac{d(\rho \ast \Psi_r)}{dx} \right\|_2^2 d\eta(\theta).
\]

In view of Lemma 6.10 this in particular implies that for \( \eta \)-many choices of \( \theta \), the covering number of \( \text{supp}(\rho_\theta) \) by \( r \)-intervals is large.

**Proof of Proposition 6.11** Our proof follows closely that of [28 Prop. 6.1]. Let \( \chi \) be a smooth, compactly supported function on \( \mathbb{R}^d \) with nonnegative Fourier transform and let \( \hat{\chi} = 1 \) on \( B_{0,1} \). Then \( \rho = \rho \cdot \chi \) and hence \( \hat{\rho} = \hat{\rho} \ast \hat{\chi} \). It follows that \( |\hat{\rho}|^2 \leq |\hat{\rho}|^2 \ast \hat{\chi} \); also since \( \chi \) is smooth, compactly supported,
\[
|\hat{\chi}(\xi)| < C_N (1 + |\xi|)^{-N} \quad \text{for every } N;
\]
we shall assume below that \( N \geq 2d \). Thus
\begin{equation}
(6.34) \quad \int_{S^{d-1}} \int_{\mathbb{R}^d} \left| \hat{\rho}(t) \hat{\Psi}_r(t) \right|^2 (1 + |t|)^{\beta' + \alpha - d} dt \, d\eta(\theta)
\leq C \int_{S^{d-1}} \int_{\mathbb{R}^d} \hat{\chi}(\theta t - x) \left| \hat{\rho}(x) \hat{\Phi}_r(x) \right|^2 (1 + |t|)^{\beta' + \alpha - d} dt \, d\eta(\theta) \, dx
\leq C' \int_{\mathbb{R}^d} \left| \hat{\rho}(x) \hat{\Phi}_r(x) \right|^2 \int_{S^{d-1}} (1 + |\theta t - x|)^{-N} (1 + |t|)^{\beta' + \alpha - d} dt \, d\eta(\theta) \, dx.
\end{equation}
We estimate the innermost integral in the last line of the above equation as follows:
\[
\int_{\mathbb{R}} (1 + |\theta t - x|)^{-N} (1 + |t|)^{\beta' + \alpha - d} \, dt \\
\leq 2^d (1 + |x|)^{\beta' + \alpha - d} \int_{|x|/2 < |t| < 2|x|} (1 + |\theta t - x|)^{-N} \, dt \\
+ C(N, \beta', \alpha)(1 + |x|)^{-N} \\
\leq C_d, N (1 + |x|)^{\beta' + \alpha - d} \left( 1 + |x| \right) \left( \frac{x}{|x|} \right)^{-N + d} \\
+ C(N, \beta', \alpha)(1 + |x|)^{-N}.
\]
Using (6.32), we have (recall that \(C'_d, N \leq d \eta \leq 10 \leq N\) is large enough (depending on \(1 + |x|\))
\[
\int_{S^d - 1} \left( 1 + |x| \right) d\mathcal{L} \left( \frac{x}{|x|} \right)^{-N + d} d\eta(\theta) \\
\leq \eta \left\{ \theta : d\mathcal{L} \left( \frac{x}{|x|} \right) < |x|^{-1} \right\} \\
+ \sum_{k \geq 0} 2^{-\beta d k} \eta \left\{ \theta : 2^k |x|^{-1} \leq d\mathcal{L} \left( \frac{x}{|x|} \right) < 2^{k+1} |x|^{-1} \right\} \\
\leq 10c_\eta \max(r, (1 + |x|)^{-1} \beta).
\]
It follows that the integral on the last line of (6.34) is at most
\[
10 C_d, N c_\eta \int_{|x| < r^{-\beta'/\beta'}} \max(r, (1 + |x|)^{-1} \beta) |\hat{\rho}(x)\hat{\Phi}_r(x)|^2 (1 + |x|)^{\beta' + \alpha - d} \, dx \\
+ 10 C_d, N c_\eta \int_{|x| > r^{-\beta'/\beta'}} r^\beta |\hat{\Phi}_r(x)|^2 (1 + |x|)^{\beta' + \alpha - d} \, dx \\
+ C'(N, \beta', \alpha).
\]
For \(|x| < r^{-\beta'/\beta'}\) one has the trivial inequality
\[
r^\beta \leq \max(|x|, 1)^{-\beta'} \leq \left( \frac{1 + |x|}{2} \right)^{-\beta'};
\]
hence as \(\beta' \leq d\),
\[
\max(r, (1 + |x|)^{-1}) \beta \leq 2^d (1 + |x|)^{-\beta'}.
\]
We also note that \(\hat{\Phi}_r(x) < C_{N_1} (r |x|)^{-N_1}\) for every \(N_1\); hence (6.35) is bounded from above by
\[
(6.36) \quad C'_d, N c_\eta \int |\hat{\rho}(x)\hat{\Phi}_r(x)|^2 (1 + |x|)^{\alpha - d} \, dx + C'(N, \beta', \alpha) \\
+ C'_d, N c_\eta C_{N_1} \int_{|x| > r^{-\beta'/\beta'}} r^\beta (r |x|)^{-N_1} |x|^{\beta' + \alpha - d} \, dx.
\]
As long as \(N_1\) is large enough (depending on \(\beta, \beta', d, \alpha\)), the integral on the second line of (6.36) is bounded by a constant (depending on the same set of parameters).
As in Section 6.B, we interpret the identity
\[ \hat{\mu}_n(b) = \sum_g \nu^m(g) \hat{\mu}_{n-m}(g^r b) \]
to mean that for “many” \( g \) in the support of \( \nu^m \), the set of large Fourier coefficients \( A_{l',n-m} \) of \( \mu_{n-m} \) contains “a substantial proportion of” \( g^r A \). This later set we consider as a perturbation of a rescaled and rotated orthogonal projection of \( A \) in the direction \( g \) expands the most (in the notation of Section 4.A, the direction perpendicular to \( H(g) \)).

**Lemma 6.12.** There are \( \epsilon_0, C, c_8 > 0 \) (depending on \( \nu \)) and an absolute constant \( q > 0 \) so that if for some \( 1/2 > t > 0, 1 \leq M < N \) with
\[ \log \frac{N}{M} > c_8 \log \frac{1}{t} \quad \text{and} \quad n \geq c_8 \log \frac{N}{M} \]
it holds that
\[ \mathcal{N}(A_{l,n} \cap B_{0,N}; M) > \left( \frac{N}{M} \right)^{d-\epsilon_0} \]
then there are \( m, M', N' \) with \( M' \geq M \),
\[ m \leq c_8 \log \frac{N}{M}, \quad N' \leq N \left( \frac{N}{M} \right)^{c_8}, \quad \frac{N'}{M'} \geq \left( \frac{N}{M} \right)^{1/c_8}, \]
and \( \xi \in \mathbb{P}^{d-1} \) so that if \( R \) denotes the “rectangle” \( B_{0,N'} \cap \text{Nbd}_{M'}(\xi) \) and \( t' = Ct^q \), then
\[ \mathcal{N}(A_{l',n-m} \cap R; M') > \frac{t'N'}{M'}. \]

**Proof.** Let \( \tau \) be as in Lemma 4.15 and set \( \epsilon_0 = \tau / 3 \). Assume that for \( t, n, M, N \) as in the statement of Lemma 6.12 we have that
\[ \mathcal{N}(A_{l,n} \cap B_{0,N}; M) > \left( \frac{N}{M} \right)^{d-\epsilon_0} \]
By Lemma 6.7 applied with \( \epsilon = \tau / 30 \) there is an \( N_1 \in (M, N) \) with \( \log(N_1/M) > \frac{1}{2} \log(N/M) \) so that \( A_{l,n} \cap B_{0,N_1} \) contains a subset \( E \) which is \((Ct^{-2}, d-2\tau/3)\)-regular at scale \( M \), where \( t_1 = t^2 / 4 \) and \( C \) depends only on \( \tau \). As before, we may assume
\[ \frac{1}{|E|} \sum_{b \in E} \hat{\mu}_n(b) \geq \frac{t_1}{2} \]
since we may always choose a subset \( E_1 \subset E \) of cardinality \( |E| / 4 \) on which the above inequality holds which is \((Ct^{-2}, d-2\tau/3)\)-regular (possibly for a slightly different \( C \)).

Let \( m_1 = \kappa \log(N_1/M) \) (for a large constant \( \kappa \) to be determined later depending on \( \nu \)), and set \( n_1 = n - m_1 \). For any \( g \in \text{supp}(\nu^{m_1}) \) set
\[ E(g) = E \cap (g^r)^{-1} A_{l',n_1} \]
\[ G_{\text{stat}} = \left\{ g \in \text{supp} \nu^{m_1} : |E(g)| > \frac{t_1}{8} |E| \right\}. \]
By (6.39), as \( \mu_n = \nu^{*m_1} * \mu_{n_1} \),

\[
\frac{1}{|E|} \sum_g \nu^{*m_1}(g) \left| \sum_{b \in E} \tilde{\mu}_{n_1}(g^{\tau b}) \right| \geq \frac{t_1}{2},
\]

and it follows that for a set of \( \nu \)-measure at least \( t_1/4 \) one has

\[
\sum_{b \in E} \tilde{\mu}_{n_1}(g^{\tau b}) \geq \frac{t_1}{4} |E|.
\]

By Chebyshev inequality any such \( g \) satisfies \( |E(g)| \geq t_1 |E|/8 \); hence we conclude that

\[
\nu^{*m_1}(G_{\text{stat}}) \geq \frac{t_1}{4}.
\]

Let \( \omega = (\lambda_1 - \lambda_2)/20 \), and set

\[
G_{\text{len}} = \left\{ g \in \Gamma : |\lambda_i - \frac{1}{m_1} \log \sigma_i(g)| < \omega \, \text{ for } \, i = 1, 2 \right\}.
\]

By Theorem 4.3 and (6.37), if \( c_8 \) is sufficiently large (depending on \( \nu \)),

\[
\nu^{*m_1}(G_{\text{len}}) > 1 - t_1/8;
\]

hence \( \nu^{*m_1}(G_{\text{len}} \cap G_{\text{stat}}) \geq t_1/8 \). Let \( G = G_{\text{stat}} \cap G_{\text{len}} \) and let \( \eta \) be the probability measure on \( \mathbb{P}^{d-1} \) defined by

\[
\eta(\Omega) = \frac{\nu^{*m_1} \{ g \in G : \theta(g) \in \Omega \}}{\nu^{*m_1}(G)}.
\]

By Lemma 4.5 for any \( \xi \in \mathbb{P}^{d-1} \) and \( e^{-m_1} < r < r_0 \) (with \( r_0 = e^{-m_0} \) and \( \tau \) as in that lemma)

\[
\eta(B_{\xi,r}) \leq 4 t_1^{-1} r^\tau.
\]

Applying Proposition 6.11 with \( \beta = \tau, \beta' = \frac{5\tau}{6}, \alpha = d - \frac{5\tau}{6}, \) and \( \rho = \frac{1}{|E|} \sum_{b \in E} \delta_b/N_1 \),

we get

\[
(6.40) \quad \int_\xi \left\| \frac{d(\rho_\xi * \Psi_r)}{dx} \right\|_2^2 \, d\eta(\xi) \leq C t_1^{-1} \left[ C_d \int_{\mathbb{R}^d} |\rho(x)|^2 \left| \Phi_r(x) \right|^2 (1 + |x|)^{\alpha-d} \, dx + C(\alpha, \beta, \beta', d) \right].
\]

Recall that \( \rho \) is \( (ct^{-2}, d - \frac{2\tau}{3}) \)-regular at scale \( M/N_1 \); moreover if \( \kappa \geq c_1^{-1} \), we have that \( r := M/N_1 \geq e^{-c_1 m_1} \). It follows that

\[
\int_{\mathbb{R}^d} |\rho(x)|^2 \left| \Phi_r(x) \right|^2 (1 + |x|)^{\alpha-d} \, dx \asymp \mathcal{E}_\alpha(\rho * \Psi_r)
\]

(by (5.5))

\[
\leq c'' t_1^{-2} = 8e'' t_1^{-1}
\]

since \( \alpha < d - 2\tau/3 \).

with \( c', c'' \) depending on \( \tau, \nu \). Substituting into (6.40), we get

\[
\int_\xi \left\| \frac{d(\rho_\xi * \Psi_r)}{dx} \right\|_2^2 \, d\eta(\xi) \leq c_s t_1^{-2}.
\]

We conclude that there is a \( g_0 \in G \) for which

\[
(6.41) \quad \left\| \frac{d(\rho_{\xi_0} * \Psi_{r_0})}{dx} \right\|_2^2 \leq c_s t_1^{-2} \quad \text{with} \, \xi_0 = \theta(g_0).
\]
Set
\[ M' = \max(N_1 e^{\sigma_2(g_0)}, Me^{\sigma_1(g_0)}), \]
\[ N' = N_1 e^{\sigma_1(g_0)}. \]

Since \( g_0 \in G_{\text{stat}} \), we have that
\[ \log(N'/M') \geq \min(\log(N_1/M), (\lambda_1 - \lambda_2 - 2\omega)m_1) \gg \log(N/M) \]
(the implicit constant depending on \( \nu \)). Also clearly \( M' \geq M \). Since \( g_0 \in G_{\text{stat}} \), we have that \( |E(g_0)| > t_1 |E|/8 \); hence \( \rho(\frac{1}{N_1}E(g_0)) \geq t_1/8 \). Let \( \pi_{\xi_0} \) denote the orthogonal projection to the direction \( \xi_0 = \theta(g_0) \) (considered as a map \( \mathbb{R}^d \to \mathbb{R} \)).

By Lemma 6.10 and (6.41) it follows that
\[ \mathcal{N}(\pi_{\xi_0}(\frac{1}{N_1}E(g_0)); r') \geq c_*(r')^{-1}t_1^4 \]
where \( r' = M'/N' \geq r \) and \( c_* = 2^{-8}c_1^{-1} \). By definition of \( E(g_0) \), we have that
\[ g_0^{tr}(E(g_0)) \subset A_{t_1/8,n_1}; \]
moreover for \( b \in B_{0,N_1} \)
\[ \|g_0^{tr} b - e^{\sigma_1(g_0)}\pi_{\xi_0}(b)\theta(g_0^{tr})\| \leq N_1 e^{\sigma_2(g_0)} \leq M'. \]

In particular, setting \( \xi = \theta(g_0) \) and with \( R \) the rectangle \( B_{0,N'} \cap \text{Nbd}_{M'}(\xi) \),
\[ (6.42) \quad \mathcal{N}(\pi_{\xi}(\frac{1}{N_1}E(g_0)); r') \geq c_*(r')^{-1}t_1^4 \]
(6.43)
\[ g_0^{tr}(E(g_0)) \subset R \cap A_{t_1/8,n_1}, \]
(6.44)
\[ \mathcal{N}(g_0^{tr}(E(g_0)); M') \geq \frac{1}{2} \mathcal{N}(\pi_{\xi_0}(E(g_0)); r'). \]

By (6.42), (6.43), and (6.44), keeping in mind that \( r' = M'/N' \), the desired inequality (6.38) follows. \( \square \)

Similarly to the proof of Proposition 6.3 Proposition 6.5 can easily be deduced from Lemma 6.12 using Lemma 6.9. Note that in the notation of Lemma 6.9
\[ \log \frac{N_1}{M_1} - \log \frac{N_2}{M_2} \ll \log t_1 \]
with the implicit constant depending on \( \nu \). We omit the details.

7. Granulated measures

The goal of this section is to prove Proposition 3.1 and hence our main result, Theorem A, which follows easily from it. Assume that \( \mu_n = \nu^m * \mu_0 \) satisfies
\[ |\hat{\mu}_{n_0}(a_0)| \geq t_0 > 0 \]
where \( n_0 \) is assumed to be larger than a constant multiple of \( \log(2||a_0||/t_0) \). The goal is to deduce that for any \( \lambda < \lambda_1 \) there is a \( C \) so that there exists some \( m^* \) so that for every \( m > m^* \)
\[ \mu_{n_0-m}(W_{Q,e^{-\lambda}m}) \geq \left( \frac{t_0}{2} \right)^C, \quad \text{where} \quad Q < \left( \frac{2||a_0||}{t_0} \right)^C. \]

We recall the notation
\[ R_Q = \left\{ \left( \frac{p_1}{q}, \ldots, \frac{p_d}{q} \right) \in \mathbb{R}^d : q \leq Q \right\}, \quad W_{Q,r} = \bigcup_{x \in R_Q} B_{x,r}. \]

Unless otherwise specified, all other constants defined in this section depend only on \( \nu \) (and hence indirectly also on \( \Gamma \)).
We outline the ingredients of the argument in Propositions 7.1–7.4 below and formally deduce Proposition 3.1. The proofs of Propositions 7.1–7.4 are given in Sections 7A–7D below.

In the first phase of the proof (Section 6, Theorem 6.1) it was shown that the set of significant Fourier coefficients \{a \in \mathbb{Z}^d : |\hat{\rho}_{n_0-m}(a)| > t\} in large balls \{a \in \mathbb{Z}^d : ||a|| < N\} has positive density when viewed at resolution \(M = N^{1-\kappa}\). We shall use this information on Fourier coefficients to show that a certain portion of the measure \(\mu_{n_0-m}\) on the torus \(\mathbb{T}^d\) is \((1-\kappa)\)-granulated at scale \(\rho = 1/N\) in the following sense.

Let \(\mu\) be a probability measure on \(\mathbb{T}^d\). Say that a \(t\)-portion of \(\mu\) is \(\alpha\)-granulated at scale \(\rho\) (here \(\alpha < 1\) and \(\rho > 0\) is smaller than a power of \(1/2\)) if there exists a \(\rho^\alpha\)-separated set \(X \subset \mathbb{T}^d\) so that

\[
\mu(\text{Nbd}_\rho(X)) = \mu\left(\bigcup_{x \in X} B_{x,\rho}\right) > t.
\]

The information on significant Fourier coefficients of \(\mu_n\) obtained in the first phase of the proof (Section 6, Theorem 6.1) enables one to show that a significant portion of the measures \(\mu_{n_0-m}\) is \((1-\kappa)\)-granulated.

**Proposition 7.1** (Initial granulation estimate). There exist constants \(1 < L_1 < L_2, \kappa > 0, \) and \(c_1, c_2\) so that if \(|\hat{\rho}_{n_0}(a_0)| > t_0 > 0, a_0 \neq 0\), then for \(m \geq c_1 \cdot \log \frac{2|\text{Nbd}_\rho|}{t_0}\), there exist \(\rho \in (L_2^{-m}, L_1^{-m})\) and a finite set \(X \subset \mathbb{T}^d\) so that

1. \(X\) is \(r = \rho^{1-\kappa}\)-separated,
2. \(\mu_{n_0-m}\left(\bigcup_{x \in X} B_{x,\rho}\right) > \left(\frac{L_2}{L_1}\right)^{c_2}\).

Let us say that a probability measure \(\mu\) is \(\beta\)-concentrated around \(x \in \mathbb{T}^d\) at scale \(\rho\) if \(\mu(B_{x,\rho}) > \rho^\beta\). So Lebesgue measure is \(d\)-concentrated, while atomic measures are \(0\)-concentrated, at all scales. Observe that if \(\alpha < d\) and \(\alpha \cdot d < \beta < d\), then a probability measure \(\mu\) which is \(\alpha\)-granulated at sufficiently small scale \(\rho\) has points which are \(\beta\)-concentrated: since a \(\rho^\alpha\)-separated subset on the \(d\)-torus has \(O(\rho^{d-\alpha})\) points, an average \(\rho\)-ball with center \(x \in X\) has \(\mu\)-mass

\[
\mu(B_{x,\rho}) > \text{const} \cdot t \cdot \rho^{\alpha - d} > \rho^\beta.
\]

Thus \(\mu_{n_0-m}\) has points which are \(\beta\)-concentrated where \(\beta = d - \kappa > (1-\kappa) \cdot d\), assuming the scale \(\rho\) is small compared to \(t\). The next step of the argument allows us to bootstrap this concentration phenomenon from \(\beta_1 = d - \kappa\) down to \(\beta_N = \delta\), where \(\delta > 0\) is some fixed concentration goal determined in Proposition 7.3 below. The bootstrapping procedure is performed some finite number \(N = N(\kappa, \delta)\) times.

**Proposition 7.2** (Bootstrapping concentration). Given \(\epsilon > 0\), there are \(\gamma > 0\) and \(\ell_0\) so that for \(n > \ell > \ell_0\) the following holds: given scales \(\rho < e^{-d\lambda_1 - \epsilon} \cdot r\), there are scales

\[
r' = e^{-(\lambda_1 + \epsilon) \cdot \ell} \cdot r, \quad \rho' = e^{-(\lambda_1 - \epsilon) \cdot \ell} \cdot \rho
\]

so that given an \(r\)-separated set \(X \subset \mathbb{T}^d\), one can construct an \(r'\)-separated set \(X' \subset \mathbb{T}^d\) with

\[
|X'| \leq |X| \quad \text{and} \quad \mu_{n - \ell}\left(\bigcup_{y \in X'} B_{y,\rho'}\right) > \left(\mu_{n}\left(\bigcup_{x \in X} B_{x,\rho}\right)\right)^d - e^{-\gamma \cdot \ell}.
\]
The initial granulation $\alpha = 1 - \kappa$ gives $\frac{\tau_0}{\rho_0} = \rho_0^{-\kappa}$ so the above proposition can be applied with $\ell$ as big as $\frac{1}{\Delta_1} \log(\frac{\tau_0}{\rho_0}) = \frac{\kappa}{\Delta_1} \log(\frac{1}{\rho_0})$. With half that big $\ell$, we still get a shrinking factor of $e^{-\kappa/10}$ in the scale of concentrated balls produced in the proposition. The fact that the ratio $\frac{n}{m}$ in the output is close to the initial ratio $\frac{\Delta_1}{\Delta_2}$ allows to apply the proposition with a fixed $\ell$ for a number $N$ of iterations and obtain very high concentrations. The loss of mass is not very drastic if the initial portion $\tau_0 > (t_0/2)^2$ of $(1-\kappa)$-granulated measure $\mu_{n_0-m}$ is large compared to the scale $\rho$ and $e^{-\gamma t}$.

The following proposition shows that a certain level of concentration can occur only near rational points. This determines the desired concentration level $\delta > 0$ mentioned above.

**Proposition 7.3** (Rational approximation). There are $\delta > 0$ and $c_4 < \infty$ so that for any small $\rho > 0$

$$
\mu_n(B_{z,\rho}) > \rho^{\frac{c}{r^{1/10}} \Rightarrow B_{z,\rho} \subset W_{Q,r},}
$$

for $r = \rho^{9/10}$ and $Q = \rho^{-1/10}$, provided $n > c_4 \cdot \log(1/\rho)$.

Hence assuming that a significant $\mu_n$-mass is granulated with exponent $\delta$, $\mu_n$ gives this significant mass to $W_{Q,r}$ with $r = Q^{-9}$. Of course the factor 9 is arbitrary here; for the following we could work with any factor bigger than say 3.

The final step of the proof uses the $\Gamma$-invariance of the set $R_Q$ to show that most of the $\mu_n$ mass of $W_{Q,r} = \bigcup_{x \in R_Q} B_{x,r}$ must be concentrated near the centers $R_Q$ of these balls.

**Proposition 7.4** (Tight bootstrapping). Given $\epsilon > 0$, there are $m_*$ and $\omega > 0$ so that if $r > 0$, $Q < \infty$, and $m > m_*$ satisfy

$$
e^{d\lambda_1 : m} \cdot r < \frac{1}{Q^2},
$$

then

$$
\mu_{n-m}(W_{Q,r} \cap \cdot m) > \mu_n(W_{Q,r}) - e^{-\omega \cdot m}
$$

assuming $n > m$.

This is done by considering the intersections of a large number $N > e^{\delta \cdot m}$ of translates $g_i^{-1}(W_{Q,r})$, where $g_1, \ldots, g_N$ are chosen using the distribution $\nu^* m$ of the $m$-step random walk.

Let us now deduce Proposition 3.1 from these propositions, which are proved in Sections 3.3 and 4 below.

**Proof of Proposition 3.1**. We assume that $|\hat{\mu}_{n_0}(a_0)| \geq t_0 > 0$ for some $a_0 \in \mathbb{Z}^d \setminus \{0\}$.

We shall work with $n_0 > m > C \cdot \log \frac{2||a_0||}{t_0}$ where the value of $C$ will be determined implicitly in the proof.

Our first goal is to show that for some constants $C_1$, $D$, $1 < L_3 < L_4$ and any $m_0 > C_1 \cdot \log \frac{2||a_0||}{t_0}$ there exist $\rho$ with $L_4^{-m_0} < \rho < L_3^{-m_0}$ and a finite set $Y \subset \mathbb{T}^d$ so that

$$
(7.1) \quad \mu_{n_0-m_0}(B_{y,\rho}) > \rho^\delta \quad (\forall \ y \in Y), \quad \mu_{n_0-m_0}(\bigcup_{y \in Y} B_{y,\rho}) > \left(\frac{t_0}{2}\right)^D
$$

where $\delta > 0$ is the constant from Proposition 7.3.
Proposition 7.1 provides \(1 < L_1 < L_2\) and \(\kappa > 0\), so that for large \(m_{00}\) there exist \(\rho_0 \in (L_2^{-m_{00}}, L_1^{-m_{00}})\) and a finite set \(X_0 \subset \mathbb{T}^d\) which is \(r_0\)-separated so that
\[
\mu_{m_{00}} \left( \bigcup_{x \in X_0} B_{x, \rho_0} \right) > \left( \frac{t_0}{2} \right)^{c_2}. 
\]
We shall amplify this initial concentration by a number \((N\) below) of iterations of the bootstrapping procedure in Proposition 7.2. The relevant parameters are chosen as follows:

\[
(7.2) \quad \ell \in \mathbb{N} \quad \text{so that} \quad e^{-2d\lambda_1 \cdot \ell} > \frac{\rho_0}{r_0} = \rho_0^\kappa > e^{-3d\lambda_1 \cdot \ell},
\]
\[
(7.3) \quad N \in \mathbb{N} \quad \text{so that} \quad \delta N \cdot \kappa > 6d^2,
\]
\[
(7.4) \quad \epsilon > 0 \quad \text{so that} \quad 2N \cdot \epsilon < d\lambda_1.
\]

Here \(\delta > 0\) is provided by Proposition 7.3 and \(\kappa\) by Proposition 7.1. Note that \(\ell \asymp \log \frac{1}{\rho_0} \asymp m_{00}\), i.e., the ratios between these quantities are bounded from below and above by finite positive constants (depending on \(\nu\)).

For \(j = 1, \ldots, N - 1\) set \(\rho_{j+1} = e^{-j(\lambda_1 - \epsilon)} \cdot \rho_0\) and \(r_{j+1} = e^{-j(\lambda_1 + \epsilon)} \cdot r_0\). Then
\[
(7.5) \quad \frac{\rho_0}{r_0} < \cdots < \frac{\rho_N}{r_N} = e^{2Net \cdot \rho_0} \cdot \frac{\rho_0}{r_0} < e^{2Net \cdot 2d\lambda_1 \cdot \ell} < e^{-d\lambda_1 \ell},
\]
where the last inequality is justified by (7.2) and (7.4).

We have arranged \(\rho_j < e^{-d\lambda_1 \cdot \ell} \cdot r_j\) for \(j = 0, \ldots, N\), and, assuming that \(\ell > \ell_0\), we may apply Proposition 7.2 inductively starting from the set \(X_0\) provided by Proposition 7.1. This yields a finite sequence of sets \(X_1, \ldots, X_N\), where each \(X_j\) is an \(r_j\)-separated set on the torus; the sets do not increase in cardinality:
\[
(7.6) \quad |X_N| \leq \cdots \leq |X_1| \leq |X_0| < \text{const} \cdot r_0^{-d} < \rho_0^{-d},
\]
while the masses
\[
\tau_j = \mu_{n_0 - j\ell} \left( \bigcup_{x \in X_j} B_{x, \rho_j} \right) \quad \text{satisfy} \quad \tau_{j+1} \cdot \tau_j^{-d} > e^{-\gamma \ell}.
\]

Here \(\gamma > 0\) depends on \(\epsilon > 0\), \(N\), \(\kappa > 0\) and \(\delta > 0\), and these constants depend on \(\nu\) but not on \(\ell\), \(m_{00}\), etc. So choosing \(C_1\) large enough, we may ensure that \(m_{00}\), and thus \(\ell\), is large compared to \(\log(2/t_0)\) so that
\[
e^{-\gamma \ell} < \left( \frac{t_0}{2} \right)^{c_2 \cdot (d+1)^N}.
\]

This implies, by induction on \(i\), that \(\tau_i > 2e^{-\gamma \ell}\) and \(\tau_{i+1} > \frac{1}{2} \tau_i^d > \tau_i^{d+1}\). In particular the last set \(X_N\) satisfies
\[
\mu_{n_0 - N\ell} \left( \bigcup_{x \in X_N} B_{x, \rho_N} \right) = \tau_N > \left( \frac{t_0}{2} \right)^{c_2 \cdot (d+1)^N}.
\]

We now use the fact that \(|X_N|\) has few elements, estimated by (7.6), to extract the subset \(Y\) of very concentrated \(\rho_N\)-balls:
\[
(7.7) \quad Y = \left\{ x \in X_N : \mu_{n_0 - N\ell} (B_{x, \rho_N}) > \frac{\tau_N}{2 \cdot |X_N|} \right\}.
\]
Then
\[ \mu_{m_0-N\ell}\left(\bigcup_{y \in Y} B_{y,\rho_N}\right) > \frac{\tau_N}{2} > \left(\frac{t_0}{2}\right)^D, \]
where \( D \) is set to be \( D = c_2 \cdot (d + 1)^N + 1 \). Finally we claim that
\[ \frac{\tau_N}{2|X_N|} > (\rho_N)\delta. \]
(7.8)
Indeed, assuming \( m_{00} \) is large compared to \( \log(2/t_0) \), we have
\[ \frac{\tau_N}{2|X_N|} > \left(\frac{t_0}{2}\right)^D \cdot \rho_0^{d(1-\kappa)} > \rho_0^d. \]
Using (7.3) and (7.2) and since \( \rho_0 \) is large compared to \( \log(2 \cdot m_0) \), the claim (7.1) is proven.

Applying Proposition 7.3 to the conclusion (7.1), we deduce that for some \( \kappa < \lambda_1 \), we choose
\[ \epsilon = \min\left(\frac{\lambda_1}{3}, \frac{\lambda_1 - \lambda}{2}\right) \]
and let \( \omega = \omega(\epsilon) > 0 \) be the corresponding constant from Proposition 7.4.

With \( \epsilon < \lambda_1 - \lambda \) there are \( 0 < \alpha < \beta \) and \( k_0 \in \mathbb{N} \), so that any large \( m \) can be written as
\[ m = m_0 + m_1 + m_2 + \cdots + m_k, \]
where \( k \leq k_0 \) and
\begin{align*}
\lambda m &< (\lambda_1 - \epsilon) \cdot (m - m_0), \\
\alpha \cdot m &< m_0 < \beta \cdot m, \\
(\frac{7}{10d\lambda_1}) \cdot \log L_3 \cdot m_0 &< m_1 < (\frac{7}{10d\lambda_1} \cdot \log L_4) \cdot m_0, \\
(1 + \frac{1}{3d}) \cdot m_i &< m_{i+1} < (1 + \frac{1}{2d}) \cdot m_i \quad (i \geq 1).
\end{align*}
(7.10) (7.11) (7.12) (7.13)
We set \( C \) to be large enough so that writing \( m > C \cdot \log \frac{2|\alpha||\omega|}{t_0} \) as \( m = m_0 + \cdots + m_k \) in the form above, we get \( m_0 > C_2 \cdot \log \frac{2|\alpha||\omega|}{t_0} \) and \( m_1 > m_+. \) Then for \( r \) and \( Q \) as in (7.4) condition (7.12) implies
\[ e^{d\lambda_1 m_1} < L_3^{\frac{7m_0}{t_0}} < Q^7 = \frac{1}{r \cdot Q^2}. \]
(7.14)
Denoting \( r_0 = r \) and \( r_i = e^{-\lambda_1 \epsilon (m_1 + \cdots + m_i)} \cdot r_i, \ i \geq 1, \) we also obtain
\[ e^{d\lambda_1 m_{i+1}} \cdot r_i < \frac{1}{Q^2}. \]
Indeed, this is proven by induction using (7.13):

\[ e^{d\lambda_1 m_{i+1}} < e^{d\lambda_1 m_i} \cdot e^{\frac{\lambda_i}{r_i} m_i} < \frac{1}{r_{i+1} \cdot Q^2}. \]

Therefore, Proposition 7.4 can be applied to deduce, using (7.10), that

\[ \mu_{n_0-m}(W_{Q,e^{-\lambda} m}) > \mu_{n_0-m}(W_{Q,e^{-(\lambda_1 + \cdots + \lambda_k)}},r) > \mu_{n_0-m_0}(W_{Q,r}) - e^{-\omega m_1} - \cdots - e^{-\omega m_k}. \]

For some \( c > 0 \), independent of \( m \), etc., we have \( \sum e^{-\omega m_i} < e^{-c m} \). If \( C > 2D/c \), then it follows, using (7.9), that

\[ \mu_{n_0-m}(W_{Q,e^{-\lambda} m}) > \mu_{n_0-m_0}(W_{Q,r}) - e^{-c m} > \left( \frac{t_0}{2} \right)^D - e^{-c m} > \left( \frac{t_0}{2} \right)^{D+1}. \]

This completes the proof of Proposition 3.1 \( \square \)

7.A. Initial granulation: Proof of Proposition 7.1. Proposition 7.1 follows from Theorem 6.1 and the following general statement with \( M = N^{1-\gamma}, \rho = \frac{1}{M} \), \( s = t = t_0^p \).

**Proposition 7.5.** There exists \( c > 0 \) so that if a probability measure \( \mu \) on \( \mathbb{T}^d \) satisfies

\[ \mathcal{N}\left( \{ a \in \mathbb{Z}^d \cap B_{0,N} : |\widehat{\mu}(a)| > t \}; M \right) > s \cdot \left( \frac{N}{M} \right)^d \]

with \( M < \text{const} \cdot N \), then there exists an \( \frac{1}{M} \)-separated set \( X \subset \mathbb{T}^d \) with

\[ \mu \left( \bigcup_{x \in X} B_x \right) > c \cdot (ts)^3. \]

**Proof.** We shall need an auxiliary smooth function \( F \) on the torus such that

\[ 0 \leq F \leq C_1 \cdot N^d, \quad \text{supp}(F) \subset B_{0,\frac{1}{M}}, \quad \int_{\mathbb{T}^d} F \, dx = 1 \]

and the Fourier coefficients

\[ \widehat{F}(a) \geq 0, \quad \widehat{F}(a) \geq \frac{1}{2} \quad \text{for} \quad a \in \mathbb{Z}^d \cap B_{0,N}. \]

Here \( C_1 < \infty \) is a constant depending on \( d \) only. To construct such a function, consider the step function \( F_1(x) = m(B_{0,r})^{-1} \cdot 1_{B_{0,r}}(x) \) where \( r = \epsilon/N \) for some fixed small \( \epsilon > 0 \). Then \( \widehat{F_1}(a) \) is close to 1 for \( a \in \mathbb{Z}^d \cap B_{0,N} \). If \( F_2 \) is a smooth symmetric approximation of \( F_1 \), then the convolution \( F = F_2 * \widehat{F_2} \) has the desired properties.

Let \( \tilde{A} \) be an \( M \)-separated set of size \( |	ilde{A}| > s(N/M)^d \) consisting of coefficients \( a \in \mathbb{Z}^d \cap B_{0,N} \) with \( |\widehat{\mu}(a)| > t \). Upon passing to a subset \( A \subset \tilde{A} \) of size

\[ |A| \geq \frac{|	ilde{A}|}{4} > \frac{s}{4} \left( \frac{N}{M} \right)^d, \]

we may assume that \( \text{Re}(e^{i\theta} \cdot \widehat{\mu}(a)) > \frac{t}{2} \) for some fixed \( \theta \in [0,2\pi) \). Let

\[ \phi(x) = \sum_{a \in A} c_a(x). \]
As usual, \( e_a(x) = e^{-2\pi i \langle x, a \rangle} \) are the standard characters. Note that
\[
|\phi(x)|^2 = \left( \sum_{a \in A} e_a(x) \right) \cdot \left( \sum_{b \in \hat{A}} e_b(x) \right) = \sum_{a, b \in A} e_{a-b}(x).
\]
The probability measure \( \lambda = \mu \ast F \) has a smooth density \( g : \mathbb{T}^d \to [0, \infty) \) with \( \hat{g}(b) = \hat{\mu}(b) \cdot \hat{F}(b) \). On \( A \) we have \( \hat{F} \geq 1/2 \) and \( \text{Re}(e^{it\hat{\mu}}) > t/2 \). Therefore
\[
\left| \int_{\mathbb{T}^d} \phi \, d\lambda \right| \geq \sum_{a \in A} \text{Re}(e^{it\hat{\mu}} \cdot \hat{g}(a)) > \frac{t}{4} \cdot |A| > \frac{ts}{24} \cdot \left( \frac{N}{M} \right)^d.
\]  
We shall see that the right-hand side is close to an a priori upper estimate for the left-hand side. Partition \( \mathbb{T}^d \) into \( M \) “cubes” \( Q_i \) with side length \( \frac{1}{M} \) and centers \( c_i \in \mathbb{T}^d \). By the Cauchy-Schwartz inequality
\[
\left( \int_{\mathbb{T}^d} \phi \, d\lambda \right)^2 \leq \sum_{i} \left( \int_{\mathbb{T}^d} 1_{Q_i} \cdot \phi \, d\lambda \right)^2 \leq \sum_{i} \lambda(Q_i)^{1/2} \cdot \left( \int_{Q_i} |\phi|^2 \, d\lambda \right)^{1/2}.
\]
Let \( r = \sqrt{\frac{2}{M}} \) which is assumed to dominate \( \frac{1}{N} \). Then \( Q_i \subset B_{c_i, r/2} \) and \( y + Q_i \subset B_{c_i, r} \) for any \( y \in \text{supp}(F) \) \( \subset B_{0, \frac{r}{2}} \). Thus
\[
\lambda(Q_i) = \int_{\mathbb{T}^d} F(y) \cdot \mu(y + Q_i) \, dy \leq \mu(B_{c_i, r}).
\]
Since \( d\lambda(x) = g(x) \, dx \), we have
\[
\int_{Q_i} |\phi|^2 \, d\lambda \leq G_i \cdot \int_{Q_i} |\phi|^2 \, dx,
\]
where \( G_i = \max_{x \in Q_i} g(x) \).
We shall estimate \( \int_{Q_i} |\phi|^2 \, dx \) using an auxiliary function \( f \) on \( \mathbb{T}^d \); we take \( f \) to be the product \( f(x) = \prod_{i=1}^d b_M(x_i) \) of one-dimensional Fejér kernels\footnote{Note that \( f \) is a nonnegative function, with \( f(x) > 10^{-d} \cdot M^d \) on the \( \frac{1}{M} \)-cube \( Q_0 = [-\frac{1}{2M}, \frac{1}{2M}]^d + \mathbb{Z}^d \) around \( 0 \in \mathbb{T}^d \). The Fourier coefficients \( \hat{f} \) take values in \([0, 1]\) and vanish outside the \([-M, M]^d \cap \mathbb{Z}^d \)-cube. Thus
\[
\int_{Q_i} |\phi(x)|^2 \, dx = \int_{Q_0} |\phi(c_i + y)|^2 \, dy \leq \frac{10^d}{M^d} \int_{Q_0} |\phi(c_i + y)|^2 \cdot f(y) \, dy
\leq \frac{10^d}{M^d} \int_{\mathbb{T}^d} |\phi(c_i + y)|^2 \cdot f(y) \, dy = \frac{10^d}{M^d} \int_{\mathbb{T}^d} \sum_{a, b \in A} e_{a-b}(c_i + y) \cdot f(y) \, dy
= \frac{10^d}{M^d} \left( \sum_{a, b \in A} e_{a-b}(c_i) \hat{f}(a-b) \right) \leq \frac{10^d}{M^d} \cdot \sum_{a, b \in A} |\hat{f}(a-b)|.
\]
Let \( C_2 \) denote the constant which is \( 10^d \) times the maximal cardinality of a 1-separated set in \([-1, 1]^d \). Since \( A \) is \( M \)-separated and \( 0 \leq \hat{f} \leq 1 \), we have
\[
\frac{10^d}{M^d} \sum_{a, b \in A} |\hat{f}(a-b)| \leq \frac{C_2 \cdot |A|}{M^d} \leq \frac{C_2}{M^{2d}}. \]}
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
The density \( g \) of \( \lambda = \mu * F \) has the following upper bound:

\[
(7.16) \quad g(x) = \int F(x - y) \, d\mu(y) \leq C_1 \cdot N^d \cdot \mu(B_{x,\frac{1}{4}}).
\]

Since \( \text{Nbd}_{\frac{1}{4}}(Q_i) \subset B_{c_i,r} \), it follows that

\[
G_i = \max_{x \in Q_i} g(x) \leq C_1 N^d \mu(B_{c_i,r}).
\]

Let \( 0 \leq H_i \leq 1 \) denote the ratio, so \( G_i = H_i \cdot C_1 N^d \mu(B_{c_i,r}) \). By (7.14 and 7.15)

\[
\frac{ts}{2^4} \left( \frac{N}{M} \right)^d \leq \sum_i \mu(B_{c_i,r})^{\frac{1}{2}} \cdot G_i^{\frac{1}{2}} \cdot \sqrt{C_2} \cdot N^{\frac{d}{2}}
\]

\[
\leq \sum_i \mu(B_{c_i,r}) \cdot H_i^{\frac{1}{2}} \cdot \sqrt{C_1 \cdot C_2} \cdot \left( \frac{N}{M} \right)^d.
\]

Let \( C_3 = \sqrt{C_1 \cdot C_2} \). We have

\[
\sum_i \mu(B_{c_i,r}) \cdot H_i^{\frac{1}{2}} > \frac{ts}{2^4 C_3^3}.
\]

Therefore

\[
(7.17) \quad \sum_{i \in I} \mu(B_{c_i,r}) > \frac{ts}{2^8 C_3^3} \quad \text{where} \quad I = \left\{ i : H_i^{\frac{1}{2}} > \frac{ts}{2^5 C_3} \right\}.
\]

For each \( i \in I \) choose \( x_i \in Q_i \) so that

\[
g(x_i) > \left( \frac{ts}{2^4 C_3^3} \right)^2 \cdot C_1 N^d \cdot \mu(B_{c_i,r}).
\]

Then (7.16) gives

\[
\mu(B_{x_i,\frac{1}{4}}) > \frac{g(x_i)}{C_1 N^d} > \left( \frac{ts}{2^4 C_3^3} \right)^2 \cdot \mu(B_{c_i,r}),
\]

and using (7.17),

\[
\sum_{i \in I} \mu(B_{x_i,\frac{1}{4}}) > \left( \frac{ts}{2^5 C_3} \right)^3.
\]

The set \( \tilde{X} = \{ x_i : i \in I \} \) visits each of the cubes \( Q_j \) at most once. Thus it may be separated into \( 2^d \) subsets each of which never visits neighboring \( Q_j \)'s and is therefore \( \frac{1}{M} \)-separated. At least one of the \( 2^d \) such subsets \( X \subset \tilde{X} \) has

\[
\mu\left( \bigcup_{x \in X} B_{x,r} \right) = \sum_{x \in X} \mu(B_{x,\frac{1}{4}}) > 2^{-d} \cdot \sum_{i \in I} \mu(B_{x_i,\frac{1}{4}}) > \left( \frac{ts}{2^4 + 15 C_3^3} \right)^3.
\]

This completes the proof of the proposition. \( \Box \)

7.B. Bootstrapping the concentration: Proof of Proposition 7.2. We start with a few lemmas.

**Lemma 7.6.** Given \( \epsilon > 0 \), there are \( \gamma > 0 \) and \( m_0 \in \mathbb{N} \) so that for \( n > m \geq m_0 \) one can find a subset \( \mathcal{G} \subset \Gamma^d \) so that for \( (g_1, \ldots, g_d) \in \mathcal{G} \),

(i) \( \frac{1}{m} \log \sigma_j(g_i) - \lambda_j < \epsilon \) \quad (1 \leq i \leq d, \ 1 \leq j \leq d),

(ii) \( \text{vol}(\theta(g_1), \ldots, \theta(g_d)) > e^{-\epsilon m} \),

(iii) \( \text{vol}(\theta(g_1), \ldots, \theta(g_d)) > e^{-\epsilon m} \).
and such that for any Borel subset $A \subset \mathbb{T}^d$ one has
$$\mu_n(A)^d - e^{-\gamma m} \leq \sum_{\bar{g} \in G} \nu^m(g_1) \cdots \nu^m(g_d) \cdot \mu_{n-m}(g_1^{-1} A \cap \cdots \cap g_d^{-1} A).$$

**Proof.** By Theorem 4.3 for some $\rho > 0$ and sufficiently large $m$ the set $G_{\text{len}}$ of $d$-tuples $\bar{g} \in \Gamma^d$ satisfying (i) has
$$(\nu^m)^d(G_{\text{len}}) > (1 - e^{-\rho m})^d.$$ 

The set $G_{\text{trans}}$ of sufficiently “transversal” $d$-tuples $\bar{g} \in \Gamma^d$, namely ones satisfying conditions (ii) and (iii), has (Lemma 7.8) mass
$$(\nu^m)^d(G_{\text{trans}}) > 1 - e^{-(\epsilon/p)m}.$$ 

Let $G = G_{\text{len}} \cap G_{\text{trans}}$ and let $\gamma > 0$ be small enough so that
$$(\nu^m)^d(G) > (1 - e^{-\rho m})^d - e^{-(\epsilon/p)m} > 1 - e^{-\gamma m}.$$ 

Given $A \subset \mathbb{T}^d$, the function $f(x) = \sum_{g \in \Gamma} \nu^m(g) \cdot 1_A(gx)$ on $\mathbb{T}^d$ satisfies
$$\int_{\mathbb{T}^d} f(x) \, d\mu_{n-m}(x) = \sum_{g \in \Gamma} \nu^m(g) \cdot \mu_{n-m}(g^{-1} A) = \mu_n(A).$$ 

By the convexity of $t \mapsto t^d$ we deduce that
$$\mu_n(A)^d = \left( \int_{\mathbb{T}^d} f \, d\mu_{n-m} \right)^d \leq \int_{\mathbb{T}^d} f(x)^d \, d\mu_{n-m}(x) = \sum_{\bar{g} \in \Gamma^d} \nu^m(g_1) \cdots \nu^m(g_d) \cdot \mu_{n-m}(g_1^{-1} A \cap \cdots \cap g_d^{-1} A)$$

and the lemma follows by restricting the summation to $\bar{g} \in G$. \qed

**Lemma 7.7.** For any $\bar{x}_1, \ldots, \bar{x}_d, \bar{y}_1, \ldots, \bar{y}_d \in \mathbb{P}^{d-1}$ one has
$$|\text{vol}(\bar{x}_1, \ldots, \bar{x}_d) - \text{vol}(\bar{y}_1, \ldots, \bar{y}_d)| \leq \sqrt{2} \cdot \sum_{i=1}^d d_{\mathcal{L}}(\bar{x}_i, \bar{y}_i).$$

**Proof.** Assuming $x_i, y_i$ are unit vectors, we have
$$|\text{vol}(x_1, \ldots, x_d) - \text{vol}(y_1, \ldots, y_d)| \leq \sum_{i=1}^d |\text{vol}(x_1, \ldots, x_i - y_i, \ldots, y_d)|$$
$$\leq \sum_{i=1}^d \|x_i - y_i\| \leq \sqrt{2} \cdot \sum_{i=1}^d d_{\mathcal{L}}(\bar{x}_i, \bar{y}_i).$$ \qed

**Lemma 7.8.** Given $\epsilon > 0$, there is $m_0(\epsilon)$ so that for $m > m_0$ and any $g_1, \ldots, g_d \in \Gamma$ with
$$\frac{1}{m} \sigma_j(g) - \lambda_j < \epsilon \quad (j = 1, 2),$$
$$\text{vol}(\theta(g_1^{tr}), \ldots, \theta(g_d^{tr})) > e^{-\epsilon m}$$

one has
$$\forall \, v \in \mathbb{R}^d \setminus \{0\} : \max_{1 \leq i \leq d} \frac{\|g_i v\|}{\|v\|} \geq e^{(\lambda_1 - 3\epsilon)m}. $$
Proof. First let us estimate
\[
\delta = \max_{1 \leq i \leq d} d_\mathcal{L}(v, H(g_i)) = \max_{1 \leq i \leq d} \left( \theta(g_i^{tr}), v^\perp \right).
\]
If the \( y_i \) denote the projections of some unit vectors in \( \bar{x}_i = \theta(g_i^{tr}) \) to \( v^\perp \), then \( \text{vol}(\bar{y}_1, \ldots, \bar{y}_d) = 0 \). Hence it follows from Lemma 7.7 that
\[
\sqrt{2} \sum_{i=1}^d d_\mathcal{L}(\bar{x}_i, \bar{y}_i) \geq \text{vol}(\bar{x}_1, \ldots, \bar{x}_d) > e^{-\epsilon m}.
\]
Thus \( \delta > \frac{1}{\sqrt{2d}} \cdot e^{-\epsilon m} \), which is larger than \( e^{-2\epsilon m} \) for sufficiently large \( m \). We have
\[
\max_{1 \leq i \leq d} \frac{\|g_i v\|}{\|v\|} \geq \delta \cdot \min_{1 \leq i \leq d} \|g_i\| \geq e^{-2\epsilon m} \cdot e^{(\lambda_1 - \epsilon) m} > e^{(\lambda_1 - 3\epsilon) m}
\]
as claimed. \( \square \)

Proof of Proposition 7.2. Since \( \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_d \) and \( \lambda_1 + \cdots + \lambda_d = 0 \), we have the strict inequality \( \lambda_1 - \lambda_d < d \lambda_1 \). We fix a small \( 0 < \delta < \min(\frac{1}{\sqrt{d}}, (d-1)\lambda_1 + \lambda_d) \), with \( \ell_0 \) to be determined later. Lemma 7.4 provides a set \( \mathcal{G} \subset \Gamma^d \) of \( d \)-tuples \((g_1, \ldots, g_d)\) and \( \gamma > 0 \) so that
\[
\frac{1}{m} \log \sigma_j(g_i) - \lambda_j \mid 1 \leq i, j \leq d, \quad \text{vol}(\theta(g_1), \ldots, \theta(g_d)) > e^{-\delta \gamma},
\]
\[
\text{vol}(\theta(g_1^{tr}), \ldots, \theta(g_d^{tr})) > e^{-\delta \gamma},
\]
and for any \( A \subset \mathbb{T}^d \)
\[
\mu_n(A) - e^{-\gamma \ell} \leq \sum_{g \in \mathcal{G}} \nu^\ell(g_1) \cdots \nu^\ell(g_d) \cdot \mu_{n-\ell}(g_1^{-1} A \cap \cdots \cap g_d^{-1} A).
\]
We apply this to the set \( A = \text{Nbd}_\rho(X) = \bigcup_{x \in X} B_{x, \rho} \) of well-separated small balls on the torus and fix a \( d \)-tuple \((g_1, \ldots, g_d) \in \mathcal{G}\) with
\[
\mu_n(A) - e^{-\gamma \ell} \leq \mu_{n-\ell}(g_1^{-1} A \cap \cdots \cap g_d^{-1} A) = \mu_{n-\ell}(\bigcup_{x_1, \ldots, x_d \in X} g_1^{-1}(B_{x_1, \rho}) \cap \cdots \cap g_d^{-1}(B_{x_d, \rho})).
\]
Consider the components \( C_{x_1, \ldots, x_d} = g_1^{-1}(B_{x_1, \rho}) \cap \cdots \cap g_d^{-1}(B_{x_d, \rho}) \), indexed by \( d \)-tuples \( \bar{x} = (x_1, \ldots, x_d) \in X^d \), of the union in the right-hand side. We shall show that most of these components are empty; in fact, there are at most \( |X| \)-many components with \( C_\bar{x} \neq \emptyset \). We shall also show that these nonempty components are \( r' \)-separated and have diameter less than \( \rho' \). So choosing one point \( y \) from each nonempty component \( C_\bar{x} \) of \( g_1^{-1} A \cap \cdots \cap g_d^{-1} A \), we obtain a set \( Y \) with the desired properties.

Let \( \bar{x} = (x_1, \ldots, x_d) \) and \( \bar{x}' = (x_1', \ldots, x_d') \) be two \( d \)-tuples from \( X \), where \( C_\bar{x} \) and \( C_{\bar{x}'} \) are not empty, and assume that \( x_1 = x_1' = x \). Then \( g_1^{-1}(B_{x, \rho}) \) intersects both \( g_j^{-1}(B_{x, \rho}) \) and \( g_j^{-1}(B_{x', \rho}) \). Applying \( g_j \), it follows that the set \((g_j g_1^{-1})(B_{x, \rho})\) intersects the \( \rho \)-balls around points \( x_j, x_j' \in X \), which yields
\[
\|x_j - x_j'\| < 2 \rho + \|g_j\| \cdot \|g_1^{-1}\| \cdot \rho < (2 + e^{(\lambda_1 + \delta) \cdot \ell}) \cdot e^{(-\lambda_d + \delta) \cdot \ell} \cdot \rho.
\]
Assuming $\ell_0$ is large enough, for $\ell \geq \ell_0$ one has
\[ 2 + e^{(\lambda_1 + \delta)\cdot \ell} \cdot e^{(-\lambda_2 + \delta)\cdot \ell} < e^{d\lambda_1 \cdot \ell}. \]
It follows that $\|x_j - x'_j\| < r$ and therefore $x_j = x'_j$. This consideration applies to all $j = 2, \ldots, d$. So $\vec{x} = \vec{x}'$.

Let us choose representatives $y \in C_{\vec{x}}$ in nonempty components of $g_1^{-1} A \cap \cdots \cap g_d^{-1} A$ and form the set $Y$. We just showed that associating $x_1$ to $y \in C_{x_1,\ldots,x_d}$ is an injective map $Y \to X$, so $|Y| \leq |X|$.

Let us show that $Y$ is $r'$-separated. Let $y \in C_{\vec{x}}$, $y' \in C_{\vec{x}'}$, and $y \neq y'$. Then $x_1 \neq x'_1 \in X$, while $g_1y, g_1y' \in B_{x_1,\rho}$ and $g_1y \in B_{x'_1,\rho}$. Therefore
\[
r < \|x_1 - x'_1\| \leq 2\rho + \|g_1\| \cdot \|y - y'\|.
\]
Since $\rho$ is much smaller than $r$ and since $\|g_1\| < e^{(\lambda_1 + \delta)\cdot \ell} < e^{(\lambda_1 + \epsilon)\cdot \ell}$, we have
\[
\|y - y'\| > \|g_1\|^{-1} \cdot (r - 2\rho) > e^{-(\lambda_1 + \epsilon)\cdot \ell} \cdot r = r'
\]
as claimed.

Let $C_{\vec{x}}$ be a nonempty component and let $y \in C_{\vec{x}}$. We claim that $C_{\vec{x}} \subset B_{y,\rho'}$. Indeed, for any $z \in C_{\vec{x}}$ and every $i = 1, \ldots, d$ both $g_iy$ and $g_iz$ are in $B_{x_i,\rho}$, so that
\[
\max_{1 \leq i \leq d} \|g_iy - g_iz\| \leq 2\rho.
\]
The above distances are measured on the torus. But since $\|g_i^{-1}\| \rho < 1/10$, the whole picture may safely be lifted to $\mathbb{R}^d$, and one might think of the vector $v = y - z$ being such that
\[
\max_{1 \leq i \leq d} \|g_iv\| \leq 2\rho.
\]
By Lemma 7.8 and the geometry of $g_1, \ldots, g_d$ this implies that
\[
\|y - z\| = \|v\| < e^{-(\lambda_1 - 3\delta)\cdot \ell} \cdot 2\rho < e^{-(\lambda_1 - \epsilon)\cdot \ell} \cdot \rho = \rho'.
\]
Therefore
\[
g_1^{-1} A \cap \cdots \cap g_d^{-1} A \subset \bigcup_{y \in Y} B_{y,\rho'}
\]
and
\[
\mu_{n - \ell}(\bigcup_{y \in Y} B_{y,\rho'}) \geq \mu_n(\bigcup_{x \in X} B_{x,\rho})^d - e^{-\gamma\cdot \ell}
\]
as required. \hfill \Box

7.C. Rational approximation: Proof of Proposition 7.3
We shall need the following technical lemma, which gives a sufficient condition for a linear combination of $d$ very proximal elements in SL$_d(\mathbb{R})$ to be invertible. Recall that for $g \in$ SL$_d(\mathbb{R})$ we denote by $\varrho(g)$ the ratio between the second longest and the longest axes of the ellipsoid $g(B_0,1)$, i.e., $\varrho(g) = \sigma_2(g)/\sigma_1(g) = \|g\wedge g\|/\|g\|^2$; proximal elements are those with small $\varrho(g)$.

Lemma 7.9. Given $g_1, \ldots, g_d \in$ SL$_d(\mathbb{R})$ and constants $c_1, \ldots, c_d$, let
\[
\rho = \max_{1 \leq i \leq d} \varrho(g_i), \quad C = \max_{1 \leq i,j \leq d} \frac{|c_i|}{|c_j|}, \quad L = \max_{1 \leq i,j \leq d} \|g_i/g_j\|
\]
and let $v = \min(v_1, v_2)$, where
\[
v_1 = \text{vol}(\vartheta(g_1), \ldots, \vartheta(g_d)), \quad v_2 = \text{vol}(\vartheta(g_1^r), \ldots, \vartheta(g_d^r)).
\]
Assume that
\[ \rho < \frac{v^3}{20d^3CL}. \]
Then the matrix \( h = \sum_{i=1}^{d} c_i g_i \) is invertible.

**Proof.** The idea is as follows: the transversality parameter \( v_2 > 0 \) provides a lower bound on the largest angle between an arbitrary vector \( z \) and the hyperplanes \( H(g_i) \) of “slow growth”. This lower bound and the proximality parameter \( \rho \) show that any given vector \( z \) is stretched significantly by at least some of the maps \( g_i \); in addition, for these maps \( g_i z \) is close to the axis \( \theta(g_i) \). The fact that these directions are in sufficiently general position (controlled by \( v_1 \)) is used to show that the longer among the images \( g_i z \) do not cancel each other and cannot be offset by the shorter images \( g_j z \) either. The details follow.

Given a unit vector \( ||z|| = 1 \), reorder the \( g_i \)'s so that
\[ \alpha_i = d_{\perp}(z, H(g_i)) = d_{\perp}(z^\perp, \theta(g_i)) \]
decrease: \( \alpha_1 \geq \cdots \geq \alpha_d \). Let \( \beta = 4d\rho/v \) and define \( k = \max\{1 \leq i \leq d : \alpha_i > \beta\} \).

Denoting \( x_i = c_i g_i z \), we shall prove that
\[ \|x_1 + \cdots + x_k\| > \|x_{k+1}\| + \cdots + \|x_d\| \]
thereby verifying that \( h z = x_1 + \cdots + x_d \neq 0 \). Since \( z \) was an arbitrary unit vector, \( h \) is nonsingular.

Let \( \bar{y}_i \) denote the projection of \( \theta(g_i^\perp) \) to \( z^\perp \). Then \( \text{vol}(\bar{y}_1, \ldots, \bar{y}_d) = 0 \) and it follows from Lemma 4.1 that
\[ \sum_{i=1}^{d} \alpha_i = \sum_{i=1}^{d} d_{\perp}(z^\perp, \theta(g_i^\perp)) \geq \frac{v}{\sqrt{2}}. \]
Therefore, \( \alpha_1 \geq v/2d \), which in turn is bigger than \( \beta = 4d\rho/v \) by the assumptions on \( \rho \). Hence we are guaranteed that \( k \geq 1 \). Using Lemma 4.1(3), for \( 1 \leq i \leq k \) we have (with \( \bar{x}_i \) denoting the unit vector in direction \( x_i \))
\[ \|x_i\| \geq |c_i| \cdot \|g_i\| \cdot \alpha_i, \quad d_{\perp}(\bar{x}_i, \theta(g_i)) \leq \frac{\rho}{\beta}. \]
Thus applying Lemma 7.7 to
\[ t = \text{vol}(\bar{x}_1, \ldots, \bar{x}_{k+1}, \theta(g_{k+1}), \ldots, \theta(g_d)) \quad \text{and} \quad \text{vol}(\theta(g_1), \ldots, \theta(g_d)) \geq v \]
gives
\[ t > v - \frac{\sqrt{2d\rho}}{\beta} > \frac{v}{2}. \]
Since \( t \leq d_{\perp}(\bar{x}_1, \text{span}(x_2, \ldots, x_k)) \), it follows that
\[ \|x_1 + \cdots + x_k\| \geq \|x_1\| \cdot t \geq |c_1| \cdot \|g_1\| \cdot \alpha_1 t \geq |c_1| \cdot \|g_1\| \cdot \frac{v^2}{4d}. \]
At the same time, for \( k < i \leq d \) one has (Lemma 7.7(2))
\[ \|x_i\| \leq |c_i| \cdot \|g_i\| \cdot (\alpha_i + \rho(g_i)) < CL \cdot |c_1| \cdot \|g_1\| \cdot \frac{5d\rho}{v} \]
using \( \alpha_i \leq \beta = 4d\rho/v \), \( c_i < CC_1 \), \( \|g_i\| \leq L\|g_1\| \). Hence (7.18) follows from the assumption \( \rho < (20d^3CL)^{-1} \cdot v^3 \). \( \square \)
Proof of Proposition 7.3 Let \(\gamma > 0\) and \(m_0\) be the constants from Lemma 7.6 corresponding to
\[
\epsilon = \min \left( \frac{\lambda_1 - \lambda_2}{10}, \frac{1}{2} \right)
\]
and choose \(\delta > 0\) small enough to ensure that \(\Delta_0 = \frac{d\delta}{\gamma} - \frac{1}{10d(\lambda_1 + 1)} > 0\). Then for all \(\rho > 0\), smaller than \(e^{-2\Delta_0}\), one can find an integer \(m\) so that
\[
\frac{1}{10d(\lambda_1 + 1)} \cdot \log \frac{1}{\rho} < m < \frac{d\delta}{\gamma} \cdot \log \frac{1}{\rho}. \tag{7.19}
\]
Taking \(c_4 = d\delta/\gamma\) and \(\rho_0 = \min\left(e^{-2\Delta_0}, e^{-m_0/c_4}\right)\), we shall also ensure that given \(0 < \rho < \rho_0\) and \(n > c_4 \log(1/\rho)\), our choice \(m = m(\rho)\) will satisfy \(m_0 \leq m < n\).

Lemma 7.6 provides a set \(G \subset \Gamma^d\) of \(d\)-tuples \(g = (g_1, \ldots, g_d)\) with
\[
\frac{1}{m} \log g_i - \lambda_1 < \epsilon, \quad i = 1, \ldots, d,
\]
\[
\frac{1}{m} \log \sigma_i(g_i) - \lambda_2 < \epsilon, \quad i = 1, \ldots, d,
\]
\[
\text{vol}(\theta(g_1), \ldots, \theta(g_d)) > e^{-c_4},
\]
\[
\text{vol}(\theta(g_1^r), \ldots, \theta(g_d^r)) > e^{-c_4},
\]
and such that
\[
\mu_n(B_{z,\rho})^d - e^{-\gamma \cdot m} < \sum_{g \in G} \nu^m(g_1) \cdots \nu^m(g_d) \cdot \mu_{n-m}(\bigcap_{i=1}^d g_i^{-1}(B_{z,\rho})).
\]
The assumption \(\mu_n(B_{z,\rho}) > \rho^d\) implies, using the second inequality of (7.19), that
\[
\mu_n(B_{z,\rho})^d > \rho^d \cdot e^{-\gamma \cdot m}.
\]
Thus there exists a \(d\)-tuple \((g_1, \ldots, g_d) \in G\) with
\[
\mu_{n-m}(g_1^{-1}(B_{z,\rho}) \cap \cdots \cap g_d^{-1}(B_{z,\rho})) > 0.
\]
In particular, there exists \(w \in \mathbb{T}^d\) such that
\[
\{g_1 w, g_2 w, \ldots, g_d w\} \subset B_{z,\rho}.
\]
We use \(\| \cdot \|\) to denote the usual metric on both \(\mathbb{R}^d\) and \(\mathbb{T}^d\), and we denote by \(\pi : \mathbb{R}^d \rightarrow \mathbb{T}^d\) the locally isometric projection. Choose \(\vec{w}, \vec{z} \in \mathbb{R}^d\) with \(\pi(\vec{w}) = w\) and \(\pi(\vec{z}) = z\). For some integer vectors \(\vec{a}_i \in \mathbb{Z}^d\)
\[
\| g_i \vec{w} - \vec{a}_i - \vec{z} \| < \rho \quad (i = 1, \ldots, d).
\]
Let \(c_1 = \cdots = c_{d-1} = 1, c_d = 1 - d\), so that \(\sum c_i = 0\) and \(\sum |c_i| < 2d\). Combining the inequalities (7.20) with coefficients \(c_i\), we get
\[
\| h \vec{w} - \vec{b} \| < 2d\rho
\]
where \(h = \sum_{i=1}^d c_i g_i\) is an integer \(d \times d\) matrix and \(\vec{b} = \sum_{i=1}^d c_i \vec{a}_i\) is an integer vector. Our choice of \(\epsilon = \frac{\lambda_1 - \lambda_2}{10}\) and the following properties of \(g_1, \ldots, g_d\)
\[
\max g_i < \frac{\epsilon^2}{\epsilon(\lambda_1 - \lambda_2)} m, \quad \max \left| \frac{c_i}{c_j} \right| < d < e^{-m}, \quad \max \left| \frac{g_i}{g_j} \right| < e^{-2m},
\]
\[
\text{vol}(\theta(g_1), \ldots, \theta(g_d)) > e^{-c_4}, \quad \text{vol}(\theta(g_1^r), \ldots, \theta(g_d^r)) > e^{-c_4},
\]
imply that the assumptions of Lemma 7.9 are satisfied.
Thus the integer matrix $h$ is invertible, and its determinant $q = \det(h)$ is a nonzero integer; in particular $|q| \geq 1$. Then $h^{-1} = (1/q) \cdot k$ where $k \in M_{d \times d} \mathbb{Z}$. Set $\bar{p} = g_1 k b \in \mathbb{Z}^d$. We have

$$
\|z - \pi(\frac{\bar{p}}{q})\| \leq \|g_1 w - z\| + \|g_1 \bar{w} - \frac{1}{q} g_1 k b\| \\
\leq \rho + \|g_1 h^{-1}\| \cdot \|h \bar{w} - \bar{b}\| < (1 + 2d \|g_1\| \|h^{-1}\|) \cdot \rho.
$$

Let us estimate the factor $\|g_1\| \|h^{-1}\|$ in terms of $1/\rho$:

$$
\|h\| \leq \sum_{i=1}^{d} |c_i| \cdot \|g_i\| \leq 2d e^{(\lambda_1 + \epsilon)m}, \\
\|h^{-1}\| \leq \frac{1}{q} \cdot \|h\|^{-1} \leq \|h\|^{-1} \quad \text{(using } q \geq 1), \\
1 + 2d\|g_1\| \|h^{-1}\| < 1 + (2d) d e^{(\lambda_1 + \epsilon)m} < e^{d(\lambda_1 + \epsilon)m} < \rho^{-\frac{1}{m}},
$$

with the last step justified by the first inequality in (7.19). We also assumed that $e^{(1-\epsilon)m} > e^{-m_0/2}$ dominates the absolute factors like $(2d)^d$. This gives

$$
\|z - \pi(\frac{\bar{p}}{q})\| < \rho \frac{\|\bar{w}\|}{\rho}, \quad \text{with } |q| < \rho^{-\frac{1}{m}}
$$

as claimed. □

7.D. Final Bootstrap: Proof of Proposition 7.4

Lemma 7.10. Given $\epsilon_1, \epsilon_2 > 0$, there exist $\delta > 0$ and $m_0$ so that for $m \geq m_0$ any set $G \subset \Gamma$ with $\nu^* (G) > e^{-\delta \cdot m}$ contains a subset $F \subset G$ with cardinality $|F| \geq e^{\delta \cdot m}$, such that

$$
\left\{ \frac{1}{m} \log \sigma_j (g) - \lambda_j \right\} < \epsilon_1 \quad (j = 1, \ldots, d, \ g \in F)
$$

and every $d$-element subset $\{g_1, \ldots, g_d\} \subset F$ satisfies

$$
\text{vol}(\theta(g_1^{ir}), \ldots, \theta(g_d^{ir})) > e^{-\epsilon_2 \cdot m}.
$$

Proof. Let $G_{\text{len}} = \left\{ g \in \Gamma : \left\{ \frac{1}{m} \log \sigma_j (g) - \lambda_j \right\} < \epsilon_1 (1 \leq j \leq d) \right\}$. By Theorem 4.4, there exist $N = N(\epsilon_1)$ and $c_1 > 0$ so that for $m > N$ the set

$$
G_{\text{len}} = \left\{ g \in \Gamma : \left\{ \frac{1}{m} \log \sigma_j (g) - \lambda_j \right\} < \epsilon_1 \quad (j = 1, 2) \right\}
$$

has $\nu^* (G_{\text{len}}) > 1 - e^{-c_1 \cdot m}$. By Theorem 4.4 given $\epsilon_2 > 0$, there is $\epsilon_2 > 0$ so that for any hyperplane $H$,

$$
\nu^* \left\{ g \in \Gamma : d_L (\theta(g_j^{ir}), H) \leq e^{-\epsilon_2 \cdot m} \right\} < e^{-\epsilon_2 \cdot m}.
$$

Let us take positive $\delta < \min(\epsilon_1, \epsilon_2 / d)$. For such $\delta$ and large $m$

$$
(7.21) \quad e^{-\delta \cdot m} - e^{-c_1 \cdot m} - (e^{\delta \cdot m})^{d-1} \cdot e^{-\epsilon_2 \cdot m} > 0.
$$

Let $G$ with $\nu^* (G) > e^{-\delta \cdot m}$ be given. We shall form the subset $F \subset G$ by choosing inductively elements from $G' = G \cap G_{\text{len}}$. Suppose $g_1, \ldots, g_n$ are already chosen. For the next element $g_{n+1}$ we can choose any $g \in G'$ for which the axis $\theta(g_j^{ir})$ makes an angle of at least $e^{-\epsilon_2 \cdot m}$ with all hyperplanes of the form

$$
\theta(g_1^{ir}) \oplus \cdots \oplus \theta(g_{n-1}^{ir})
$$
where \( i_1 < \cdots < i_{d-1} \) is a \((d-1)\)-element subset of \( \{1, \ldots, n\} \). There are less than \( n^{d-1} \) such hyperplanes. It follows that

\[
\nu^m \left( G' \setminus \bigcup_{1 \leq i_1 < \cdots < i_{d-1} \leq n} \left\{ g : d_{\theta} \left( \theta(g_{i_1}^{r_1}), \theta(g_{i_2}^{r_2}) \oplus \cdots \oplus \theta(g_{i_{d-1}}^{r_{d-1}}) \right) < \epsilon^{-c_2} m \right\} \right) > e^{-\delta \cdot m} - e^{-c_1 \cdot m} - n^{d-1} \cdot e^{-c_2 \cdot m},
\]

and in view of (7.21) the right-hand side is positive as long as \( n \leq [e^{\delta \cdot m}] \). This allows us to construct the desired set \( \mathcal{F} \) with at least \( e^{\delta \cdot m} \) elements.

**Proof of Proposition 7.3.** Let \( \delta > 0 \) be associated to \( \epsilon_1 = c_2 = \frac{\epsilon}{3} \) in Lemma 7.10 take \( \omega = \delta/2 \) and \( m_0 \) large enough. The basic relation

\[
\mu_n(W_{Q,r}) = \sum_{g \in \Gamma} \nu^m(g) \cdot \mu_{n-m}(g^{-1}(W_{Q,r}))
\]

implies that the set

\[
\mathcal{G} = \left\{ g \in \Gamma : \mu_{n-m} \left( g^{-1}(W_{Q,r}) \right) > \mu_n(W_{Q,r}) - e^{-\delta \cdot m} \right\}
\]

has \( \nu^m(\mathcal{G}) > e^{-\delta \cdot m} \). Let \( \mathcal{F} \subset \mathcal{G} \) be a subset of size \( |\mathcal{F}| > e^{\delta \cdot m} \) of well-shaped elements in general position provided by Lemma 7.10. We shall consider the possible intersections of the sets

\[
g^{-1}(W_{Q,r}) = \bigcup_{x \in R_Q} g^{-1}(B_{x,r}) \quad (g \in \mathcal{F}).
\]

Note that the set \( R_Q \) of centers of the \( r \)-balls which form \( W_{Q,r} \) is \( Q^{-2} \)-separated:

\[
\left\| \frac{p_1}{q} \ldots, \frac{p_d}{q} - \frac{q_1'}{q'} \ldots, \frac{q_d'}{q'} \right\| = \left\| \frac{q' p_1 - q p_1'}{q \cdot q'} \ldots, \frac{q' p_d - q p_d'}{q \cdot q'} \right\| \geq \frac{1}{qq'} \geq \frac{1}{Q^2}.
\]

Suppose that for \( x, y \in R_Q \) and \( g, h \in \mathcal{F} \) the ellipses \( g^{-1}(B_{x,r}) \) and \( h^{-1}(B_{y,r}) \) have a common point, say \( w \). We have \( \|x - gw\| < r \), \( \|y - hw\| < r \), and \( \|g^{-1}\|, \|h^{-1}\| < e^{-(\lambda_d + \epsilon_1)} \cdot m \). Note also that \( -\lambda_d < d \lambda_1 \), and we may assume that \( 2e^{-(\lambda_d + \epsilon_1)} \cdot m < e^{d \lambda_1} \cdot m \). Therefore

\[
\|g^{-1}x - h^{-1}y\| \leq \|g^{-1}x - w\| + \|w - h^{-1}y\| < \|g^{-1}\| \cdot \|x - gw\| + \|h^{-1}\| \cdot \|y - hw\| < 2e^{-(\lambda_d + \epsilon_1)} \cdot m \cdot r < e^{d \lambda_1} \cdot m \cdot r < \frac{1}{Q^2}.
\]

Since \( g^{-1}x \) and \( h^{-1}y \) belong to the \( Q^{-2} \)-separated set \( R_Q \), they coincide: \( g^{-1}x = h^{-1}y = z \in R_Q \).

This computation shows that for any \( d \)-element subset \( \{g_1, \ldots, g_d\} \subset \mathcal{F} \) we have

\[
\bigcap_{i=1}^d g_i^{-1}(W_{Q,r}) = \bigcup_{z \in R_Q} \left( \bigcap_{i=1}^d g_i^{-1}(B_{z,r}) \right).
\]

The conditions on \( \mathcal{F} \) show, using Lemma 7.8, that for any \( d \)-element subset \( \{g_1, \ldots, g_d\} \subset \mathcal{F} \) and every \( v \in \mathbb{R}^d \)

\[
\max_{1 \leq i \leq d} \|g_i v\| \geq e^{(\lambda_1 - \epsilon) \cdot m} \cdot \|v\|.
\]
This implies that on the torus $\mathbb{T}^d$,

$$\bigcap_{i=1}^d g_i^{-1}(B_{g_i z, r}) \subset B_{z, e^{-(\lambda_1-\epsilon)} \cdot m \cdot r}.$$ 

Therefore for any $d$-element subset \{\(g_1, \ldots, g_d\)\} $\subset \mathcal{F}$ we have

$$\bigcap_{i=1}^d g_i^{-1}(W_{Q, r}) \subset W_{Q, e^{-(\lambda_1-\epsilon)} \cdot m \cdot r}.$$ 

For $g \in \mathcal{F}$ let $E_g = g^{-1}(W_{Q, r}) \setminus W_{Q, e^{-(\lambda_1-\epsilon)} \cdot m \cdot r}$. We just showed that the collection \{\(E_g \mid g \in \mathcal{F}\}\} has no $d$-fold intersections. Thus

$$d > \int \sum_{g \in \mathcal{F}} 1_{E_g}(x) \, d\mu_{n-m}(x) = \sum_{g \in \mathcal{F}} \mu_{n-m}(E_g).$$

Thus for at least one $h \in \mathcal{F} \subset \mathcal{G}$ one has

$$\mu_{n-m}(E_h) \leq \frac{d}{|\mathcal{F}|} < d \cdot e^{-\delta m}.$$ 

Therefore,

$$\mu_{n-m}(W_{Q, e^{-(\lambda_1-\epsilon)} \cdot m \cdot r}) \geq \mu_{n-m}(h^{-1}(W_{Q, r})) - \mu_{n-m}(E_h)$$

$$> \mu_{n}(W_{Q, r}) - e^{-\delta m} - d \cdot e^{-\delta m}$$

$$> \mu_{n}(W_{Q, r}) - e^{-\omega \cdot m},$$

assuming $m > m_0$ where $m_0$ is large enough. 

\[\square\]

References


