ASYMPTOTIC METRIC BEHAVIOR OF RANDOM CAYLEY GRAPHS OF FINITE ABELIAN GROUPS

URI SHAPIRA AND REUT ZUCK

Abstract. Using methods of Marklof and Strömbergsson we establish several limit laws for metric parameters of random Cayley graphs of finite abelian groups with respect to a randomly chosen set of generators of a fixed size. Doing so we settle a conjecture of Amir and Gurel-Gurevich.

1. Introduction

1.1. **The main result.** For a finite group Γ and a generating set $s \subset \Gamma$ we denote by $C_\Gamma(s)$ the corresponding Cayley graph and by $C^+_\Gamma(s)$ the corresponding directed Cayley graph (digraph for short). Let $m \geq n$ be integers with $m \geq 2$ and let $\Sigma < \mathbb{Z}^n$ be a finite index subgroup. Consider the set

$$\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) \stackrel{\text{def}}{=} \{s : s \subset \mathbb{Z}^n/\Sigma, |s| = m, \langle s \rangle = \mathbb{Z}^n/\Sigma\}.$$

Our aim is to establish several limit laws for (proper scalings of) some metric parameters on random Cayley graphs or digraphs which are obtained by choosing $s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ at random, as $\Sigma \to \infty$ in the following sense.

Definition 1.1. If $m > n$ we say that $\Sigma \to \infty$ if $|\Sigma| \to \infty$, where we denote by $|L|$ the covolume of a lattice $L < \mathbb{R}^n$. If $n = m$, we say that $\Sigma \to \infty$ if $|\Sigma|/(\gcd \Sigma)^n \to \infty$, where $\gcd \Sigma$ denotes the largest positive integer ℓ for which $\ell^{-1}\Sigma \subset \mathbb{Z}^n$ (in case $m = n$, we basically want to exclude the sequence $\Sigma = k\mathbb{Z}^n$, where $|\Sigma| = (\gcd \Sigma)^n$).

Our results will refer to a metric parameter $\xi(\mathcal{G})$ of a graph or digraph according to the following list. We will refer to the choice $\mathcal{G} = C_{\mathbb{Z}^n/\Sigma}(s)$ as the *undirected case* and to $\mathcal{G} = C^+_{\mathbb{Z}^n/\Sigma}(s)$ as the *directed case*:

(I) $\xi(\mathcal{G}) = \mathrm{diam}(\mathcal{G})$ (both directed and undirected cases),
(II) $\xi(\mathcal{G})^\alpha = \frac{1}{|\mathrm{V}_\mathcal{G}|^2} \sum_{x,y \in \mathrm{V}_\mathcal{G}} \mathrm{d}^\alpha_\mathcal{G}(x,y)$, for $\alpha > 0$ (both directed and undirected cases),
(III) $\xi(\mathcal{G}) = \mathrm{girth}(\mathcal{G})$ (only in the directed case).

Above $\mathrm{V}_\mathcal{G}$ denotes the set of vertices of $\mathcal{G}$ and $\mathrm{d}_\mathcal{G}$ denotes the graph metric in the undirected case and non-symmetric metric (ns-metric for short), in the directed case.

Theorem 1.2. *Let ξ be as in (I), (II), or (III). Then, as $\Sigma \to \infty$ in the sense of Definition 1.1, the random variable $s \mapsto |\Sigma|^{-\frac{1}{m}} \xi(\mathcal{G})$, defined on $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ (where $\mathcal{G} = C_{\mathbb{Z}^n/\Sigma}(s)$ or $\mathcal{G} = C^+_{\mathbb{Z}^n/\Sigma}(s)$ according to the case, and s is chosen uniformly at random), converges in distribution and the limit distribution is given by an explicit random variable (which depends on ξ) on the space of unimodular lattices in $\mathbb{R}^m$ equipped with the natural $\mathrm{SL}_m(\mathbb{R})$-invariant probability measure.*

The explicit description of the random variables giving the limit distributions will be given as soon as we introduce the necessary terminology at the end of §2.1.

If one restricts attention to the case $n = 1$ and ξ as in (I) then Theorem 1.2 settles [AGG10, Conjecture 3].

Our methods are adaptations of those introduced by Marklof and Strömbergsson in [MS13]. In some respects we improve on their results where the main input which allows us to do so is an observation that certain collections of sublattices of $\mathbb{Z}^m$ that appear naturally in the discussion are invariant under the action of $\mathrm{SL}_m(\mathbb{Z})$ (similar invariance was noticed and used in [EMSS16]). We then invoke equidistribution results for such invariant sets ([GM03, COU01, EO06]).

We now wish to highlight the differences between our results and the results in [MS13]. The first difference is that in [MS13] only the case $n = 1, m \geq 2$ is considered, namely their random graphs are Cayley graphs of $\mathbb{Z}/k\mathbb{Z}$. The second (and most significant difference) is that in [MS13] the random graph is not chosen from $\left\{C_{\mathbb{Z}/k\mathbb{Z}}(s) : s \in \mathcal{S}_{\mathbb{Z}/k\mathbb{Z}}(m)\right\}$ for a given k but from the union $\cup_{\ell \leq k} \left\{C_{\mathbb{Z}/\ell\mathbb{Z}}(s) : s \in \mathcal{S}_{\mathbb{Z}/\ell\mathbb{Z}}(m)\right\}$ (i.e. the group with respect to which the random Cayley graph is chosen is not fixed), which is less natural from the graph theoretic point of view. On the other hand, the discussion in [MS13] allows to choose the generating set s at random with respect to some non-uniform measures on $\cup_{\ell \leq k} \mathcal{S}_{\mathbb{Z}/\ell\mathbb{Z}}(m)$, as opposed to the statement in Theorem 1.2 where s is chosen uniformly from $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$. The input that allows [MS13] to work with non-uniform measures is that in their work they apply a more sophisticated equidistribution result from [Mar10] than Theorem 4.4 that we are using. It is that input that forces them to randomly choose the group and the generating set and not just the generating set. Recently the equidistribution result from [Mar10] was generalized in [EMSS16]. In §5 we prove Theorem 5.1 which generalize Theorem 1.2 under certain restrictions so that the generating set s would be chosen according to a non-uniform measure on $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$. Similarly to [MS13] the limit distribution does not depend on the law with respect to which we choose s. The restrictions under which this stronger result holds are that $m > n$ and $\Sigma = k\mathbb{Z}^n$ so that the parameter going to ∞ is k. If $n = 1$ as in [MS13] this is the general case but in general we do not know at the moment what happens in the case $n = m$ or for general Σ.

We wish to suggest the following problem which is natural from the point of view taken in this paper and leads to an interesting equidistribution question in the space of lattices.

Problem 1.3. *Let $m > n$, and let $\mathbf{b} = \{v_i\}_1^n$ be a basis for $\mathbb{Z}^n$. For a finite index subgroup $\Sigma < \mathbb{Z}^n$ consider the subset $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(\mathbf{b}, m) = \left\{s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) : s \supset \mathbf{b} \bmod \Sigma\right\}$ (that is, we restrict attention to the generating sets which contain the reduction of $\mathbf{b}$ modulo Σ). Is it true that Theorem 1.2 holds when instead of choosing s at random from $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$, we choose s at random from $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(\mathbf{b}, m)$.*

1.2. **Outline of the proof.** We begin with some notation. We denote by X_m the space of unimodular lattices on $\mathbb{R}^m$ (i.e. lattices of covolume 1) and equip it with the natural 'uniform' probability measure m_{X_m}; that is, the unique $\mathrm{SL}_m(\mathbb{R})$-invariant Borel probability measure on it. In our discussion we will often encounter lattices $\Lambda < \mathbb{R}^m$ which are not unimodular. We then denote by $\bar{\Lambda} \in X_m$ the properly scaled lattice $|\Lambda|^{-1/m}\Lambda$.

The structure of the proof is as follows. We will define a map whose fibers have constant cardinality $s \mapsto \Lambda_s$ from $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ to the space of subgroups of $\mathbb{Z}^m$ of index $|\Sigma|$ with the following two fundamental properties:

(1) The Cayley graphs $C_{\mathbb{Z}^n/\Sigma}(s)$ and $C_{\mathbb{Z}^m/\Lambda_s}(I)$ (and the corresponding digraphs) are isomorphic, where I denotes the standard generators of $\mathbb{Z}^m$.
(2) The finite collection $\left\{\bar{\Lambda}_s : s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)\right\}$ becomes equidistributed in X_m as $\Sigma \to \infty$.

The isomorphism in (1) means that we can study the metric properties of the random graphs $C_{\mathbb{Z}^m/\Lambda_s}(I)$ instead. The advantage of these Cayley graphs, which we refer to as *approximate torus graphs*, is that since the generating set is fixed, they are basically a discrete version of the continuous torus $\mathbb{R}^m/\Lambda_s$. We are therefore reduced to study the relevant metric properties of the random torus $\mathbb{R}^m/\Lambda_s$. As the metric parameters we are interested in are scaled in a simple fashion, we are further reduced to study the metric properties of a random torus $\mathbb{R}^m/\bar{\Lambda}_s$ as $s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}$ is chosen uniformly at random. At this point, property (2) kicks in and tells us that this random torus is basically a random torus of the form $\mathbb{R}^m/L$ where $L \in X_m$ is chosen at random with respect to m_{X_m}.

Acknowledgments. We would like to thank Jens Marklof, Manfred Einsiedler, Shahar Mozes, and Nimish Shah, for useful discussions. We would also like to thank the anonymous referees for spotting some inaccuracies and helping to improve the paper. The authors acknowledge the support of ISF grant 357/13.

2. Preparations

2.1. **The limit distributions.** As stated in Theorem 1.2, the limit distributions that appear in our discussion will be given in terms of functions $\zeta : X_m \to \mathbb{R}$ which we now turn to discuss. Let $\mathbf{B}$ denote the following subset of $\mathbb{R}^m$ or $\mathbb{R}^m_+ \stackrel{\text{def}}{=} \{v \in \mathbb{R}^m : \forall i\ v_i > 0\}$ according to the case,

(1) $\mathbf{B} = \{v \in \mathbb{R}^m : \sum_1^m |v_i| < 1\}$ in the undirected case,
(2) $\mathbf{B} = \left\{v \in \mathbb{R}^m_+ : \sum_1^m v_i < 1\right\}$ in the directed case.

This is nothing but the unit ball (or its intersection with $\mathbb{R}^m_+$) with respect to the ℓ_1-metric. For $x, y \in \mathbb{R}^n$ we define

$$\mathrm{d}_{\mathbb{R}^m}(x, y) = \inf\{t > 0 : y \in x + t\mathbf{B}\}. \tag{2.1}$$

In the undirected case (1) this is the usual ℓ_1-distance from x to y and in the directed case (2) this is a non symmetric distance which is finite only if $y \in x + \mathbb{R}^m_+$. Given a lattice $\Lambda < \mathbb{R}^m$ the (ns-)distance $\mathrm{d}_{\mathbb{R}^m}$ descends to a finite (ns-)distance on the torus $\mathbb{R}^m/\Lambda$ defined by

$$\mathrm{d}_{\mathbb{R}^m/\Lambda}(x + \Lambda, y + \Lambda) = \inf\{\mathrm{d}_{\mathbb{R}^m}(x, y + v) : v \in \Lambda\}. \tag{2.2}$$

In fact, the quantity on the right is a minimum due to the discreteness of Λ.

Corresponding to the choice (I)-(III) of ξ in Theorem 1.2 we have the following list of functions ζ on lattices $\Lambda < \mathbb{R}^m$:

(A) If ξ is chosen as in (I) we shall denote

$$\zeta(\Lambda) = \inf\{t > 0 : \Lambda + t\mathbf{B} = \mathbb{R}^m\}$$

where $\mathbf{B}$ is chosen as in (1) or (2) according to whether we are in the undirected or the directed case respectively. This is the *covering radius* of Λ with respect to $\mathbf{B}$.

(B) If ξ is chosen as in (II) with $\alpha > 0$ fixed, we shall denote

$$\begin{aligned}\zeta(\Lambda)^\alpha &= \frac{1}{(\lambda(\mathbb{R}^m/\Lambda))^2}\int_{(\mathbb{R}^m/\Lambda)^2} \mathrm{d}^\alpha_{\mathbb{R}^m/\Lambda}(x,y)d\lambda(x)d\lambda(y)\\ &= \frac{1}{\lambda(\mathbb{R}^m/\Lambda)}\int_{\mathbb{R}^m/\Lambda} \mathrm{d}^\alpha_{\mathbb{R}^m/\Lambda}(0,x)d\lambda(x),\end{aligned}$$

where λ is the Lebegues measure on $\mathbb{R}^m$ and $\mathrm{d}_{\mathbb{R}^m/\Lambda}$ is the distance (resp. ns-distance) defined above according to the case.

(C) If ξ is chosen as in (III), we shall denote

$$\zeta(\Lambda) = \inf\left\{t > 0 : t\mathbf{B} \cap \Lambda \neq \{0\}\right\},$$

where $\mathbf{B}$ is as in (2). This is the *length of the shortest vector* in Λ with respect to the ns-distance $\mathrm{d}_{\mathbb{R}^m}$.

In Theorem 1.2 the random variables converge in distribution to the random variable ζ on (X_m, m_{X_m}), where ζ is as in (A)-(C) according to the choice of ξ as in (I)-(III).

2.2. **Topological and measure theoretic notions.** We review some relevant notions and prove two lemmas that will be used in the proof. Given a locally compact Hausdorff space X, and a sequence of Borel probability measures on it, μ_i, we say that μ_i converges in the weak-star topology to a Borel probability measure μ on X and denote $\mu_i \xrightarrow{\mathrm{w}^*} \mu$ if for any continuous function with compact support $f \in C_c(X)$, $\int f d\mu_i \to \int f d\mu$.

A continuous function $\zeta : X \to \mathbb{R}$ is said to be *proper* if the pre-image of compact sets is compact. The importance of properness to our discussion is that if ζ is proper and $f \in C_c(\mathbb{R})$ then $f\circ\zeta \in C_c(X)$. This allows us to translate weak-star convergence of measures on X to weak-star convergence of measures on $\mathbb{R}$ which is exactly the notion of convergence in distribution appearing in Theorem 1.2. This will be used in our discussion in the form of the following lemma.

Lemma 2.1. *Let X be a locally compact Hausdorff space and let $\mu_i \xrightarrow{\mathrm{w}^*} \mu$ be a converging sequence of Borel probability measures on X. Let $\zeta : X \to (0,\infty)$ be a continuous proper function and let $\xi_i : \operatorname{supp}\mu_i \to (0,\infty)$ be measurable functions such that on every compact set $K \subset X$, $\sup\{|\zeta(x) - \xi_i(x)| : x \in K \cap \operatorname{supp}\mu_i\} \to 0$ as $i \to \infty$. Then $(\xi_i)_*\mu_i \xrightarrow{\mathrm{w}^*} \zeta_*\mu$ or in other words, the random variables ξ_i on (X,μ_i) converge in distribution to the random variable ζ on (X,μ).*

Proof. Let $f \in C_c((0,\infty))$. Our goal is to show that $|\int_X f(\xi_i(x))d\mu_i(x) - \int_X f(\zeta(x))d\mu(x)| \to 0$. To this end, let $\epsilon > 0$ and let $\delta > 0$ be such that for $t, s \in (0,\infty)$ with $|t-s| < \delta$ we have $|f(t) - f(s)| < \epsilon$. Let $K \subset X$ be a compact set containing $\zeta^{-1}(\operatorname{supp} f)$ (which is compact by the properness assumption), such that for all large enough i, $\mu_i(X \smallsetminus K) < ||f||^{-1}\epsilon$. The existence of such a set follows from the fact that μ is a Borel probability measure and that $\mu_i \xrightarrow{\mathrm{w}^*} \mu$. Our assumptions imply that for all large enough i we also have, $|\zeta(x) - \xi_i(x)| < \delta$ for $x \in K \cap \operatorname{supp}\mu_i$. We therefore have for such i,

$$|\int_X f(\xi_i(x))d\mu_i(x) - \int_X f(\zeta(x))d\mu_i(x)| \le \int_K \epsilon d\mu_i + \int_{X\smallsetminus K} ||f||_\infty d\mu_i \le 2\epsilon.$$

Finally, by the assumed convergence $\mu_i \xrightarrow{\mathrm{w}^*} \mu$ and the properness of ζ we conclude that $f\circ\zeta \in C_c(X)$ and that for all large enough i, $|\int_X f(\zeta(x))d\mu_i(x) - \int_X f(\zeta(x))d\mu(x)| < \epsilon$.

Together this gives that for all large enough i, $|\int_X f(\xi_i(x))d\mu_i(x) - \int_X f(\zeta(x))d\mu(x)| < 3\epsilon$ which concludes the proof. □

At some point in the proof we will need to use the equicontinuity of a family of functions which are induced from the function $f(x) = \mathrm{d}^{\alpha}_{\mathbb{R}^m}(0,x)$, where $\mathrm{d}_{\mathbb{R}^m}$ is either the distance or the ns-distance introduced in §(2.1) which is defined for x in $\mathbb{R}^m$ or $\mathbb{R}^m_+$ respectively. The following lemma achieves that.

Lemma 2.2. *Let f be a continuous non-negative function on either $\mathbb{R}^m$ or $\mathbb{R}^m_+$ such that $\lim_{x\to\infty} f(x) = \infty$. For a lattice $\Lambda < \mathbb{R}^m$ define a Λ-invariant function on $\mathbb{R}^m$ by $f_{\mathbb{R}^m/\Lambda}(x) = \min\{f(x+v) : v \in \Lambda\}$. Then, for any compact set $K \subset \mathbb{R}^m$ or $\mathbb{R}^m_+$, the family of restrictions $\{f_{\mathbb{R}^m/\Lambda}|_K\}$ (as Λ varies), is equicontinuous.*

Proof. Let $K' \supset K$ be a larger compact set to be chosen shortly. Given $\epsilon > 0$ by the uniform continuity of f on K' we may choose $\delta > 0$ such that if $x, y \in K'$ are such that $||x-y|| \le \delta$, then $|f(x) - f(y)| < \epsilon$.

Let Λ be a lattice and let $x, y \in K$ be such that $||x-y|| \le \delta$. Assume without loss of generality that $f_{\mathbb{R}^m/\Lambda}(x) \le f_{\mathbb{R}^m/\Lambda}(y)$ and let $v_x \in \Lambda$ by such that $f_{\mathbb{R}^m/\Lambda}(x) = f(x+v_x)$. Because f diverges at ∞ we know that if K' is chosen large enough then $K + v_x \subset K'$ and therefore $f_{\mathbb{R}^m/\Lambda}(x) \le f_{\mathbb{R}^m/\Lambda}(y) \le f(y+v_x) \le f(x+v_x) + \epsilon = f_{\mathbb{R}^m/\Lambda}(x) + \epsilon$. □

3. Approximated tori graphs

In light of the outline described in §1.2, we turn now to discuss a family of graphs we refer to as approximated tori graphs. The goal of this section is to prove Corollary 3.5 which isolates an important component in the proof of Theorem 1.2.

Definition 3.1. Let $\Lambda < \mathbb{Z}^m$ be a finite index subgroup and let I be the standard basis of $\mathbb{R}^m$. The *approximate torus graph* (resp. *digraph*) associated to Λ is defined to be the Cayley graph $C_{\mathbb{Z}^m/\Lambda}(I)$ (resp. Cayley digraph $C^+_{\mathbb{Z}^m/\Lambda}(I)$).

We say that two (ns-)metric spaces $(X, \mathrm{d}_X), (Y, \mathrm{d}_Y)$ are *of bounded distance* if there are maps $\varphi : X \to Y, \psi : Y \to X$ and a constant C such that for all $x_1, x_2 \in X$, $|\mathrm{d}_X(x_1,x_2) - \mathrm{d}_Y(\varphi(x_1),\varphi(x_2))| \le C$ and for all $y_1, y_2 \in Y$, $|\mathrm{d}_Y(y_1,y_2) - \mathrm{d}_X(\psi(y_1),\psi(y_2))| \le C$. We refer to C as a *distance bound*. The reason for the terminology in Definition 3.1 is the following lemma which is left to the reader (cf. [MS13, equation (2.14)]).

Lemma 3.2. *As $\Lambda < \mathbb{Z}^m$ ranges over the finite index subgroup, the (ns-)metric spaces $(\mathcal{G}, \mathrm{d}_{\mathcal{G}})$, $(\mathbb{R}^m/\Lambda, \mathrm{d}_{\mathbb{R}^m/\Lambda})$ are of bounded distance with a uniform distance bound which depends only on the dimension m. Here $\mathcal{G} = C_{\mathbb{Z}^m/\Lambda}(I)$ or $C^+_{\mathbb{Z}^m/\Lambda}(I)$ and $\mathrm{d}_{\mathbb{Z}^m/\Lambda}$ is the distance or ns-distance defined in (2.2) respectively.*

The next two lemmas show that the metric parameters in (I), (II), (III), appearing in Theorem 1.2 of an approximated torus graph or digraph $\mathcal{G}$, are naturally linked with the corresponding quantities in (A), (B), (C), of the lattice giving rise to the approximated torus graph or digraph. The first lemma deals with the diameter and the girth, and the second lemma, which is more subtle deals with the average distance and its moments.

Lemma 3.3. *Let ξ be as in (I) or (III) and ζ be as in (A) or (C) respectively. Then, as $\Lambda < \mathbb{Z}^m$ ranges over the finite index subgroup,*

$$|\xi(\mathcal{G}) - \zeta(\Lambda)| = O(1), \tag{3.1}$$

$$||\Lambda|^{-1/m}\xi(\mathcal{G}) - \zeta(\bar{\Lambda})| = O(|\Lambda|^{-1/m}), \tag{3.2}$$

where $\mathcal{G} = C_{\mathbb{Z}^m/\Lambda}(I)$ or $C^+_{\mathbb{Z}^m/\Lambda}(I)$ according to the case.

Proof. First note that the quantities ζ that we consider are homogeneous in the sense that $\zeta(t\Lambda) = t\zeta(\Lambda)$ and therefore (3.2) follows immediately from (3.1).

Regarding case (I): It is straightforward from the definition of the covering radius that $\operatorname{diam}(\mathbb{R}^m/\Lambda) = \zeta(\Lambda)$. Lemma 3.2 implies that $\operatorname{diam}(\mathbb{R}^m/\Lambda) = \operatorname{diam}(\mathcal{G}) + O(1)$, where $\mathcal{G} = C_{\mathbb{Z}^m/\Lambda}(I)$ or $C^+_{\mathbb{Z}^m/\Lambda}(I)$ according to the case. The validity of (3.1) follows.

Regarding case (III): It is straightforward to show that in fact $\zeta(\Lambda) = \operatorname{girth}(C^+_{\mathbb{Z}^m/\Lambda}(I))$ and so (3.1) holds with $O(1)$ replaced by zero. □

Before stating the next lemma we introduce some notation. Given $\Lambda < \mathbb{Z}^m$ we denote by ν_Λ the normalized counting measure supported on the finite set $\mathbb{Z}^m/\Lambda$ viewed as a subset of the torus $\mathbb{R}^m/\Lambda$. Let $\bar{\nu}_\Lambda$ denote the image measure on the scaled torus $\mathbb{R}^m/\bar{\Lambda}$. Because of the scaling properties of the α'th power of the (ns)-distances we have the following equality which expresses $\xi(\mathcal{G})$ for ξ as in (II) in a form that resembles ζ as in (B). Here $\mathcal{G}$ is $C_{\mathbb{Z}^m/\Lambda}(I)$ or $C^+_{\mathbb{Z}^m/\Lambda}(I)$ according to the case.

$$\begin{aligned}\xi(\mathcal{G})^\alpha &= |\,\mathrm{V}_{\mathcal{G}}\,|^{-2} \sum_{x,y\in \mathrm{V}_{\mathcal{G}}} \mathrm{d}^\alpha_{\mathcal{G}}(x,y) = \int_{(\mathbb{R}^m/\Lambda)^2} \mathrm{d}^\alpha_{\mathbb{R}^m/\Lambda}(x,y)d\nu_\Lambda(x)d\nu_\Lambda(y) \\ &= \int_{\mathbb{R}^m/\Lambda} \mathrm{d}^\alpha_{\mathbb{R}^m/\Lambda}(0,x)d\nu_\Lambda(x) = |\Lambda|^{\frac{\alpha}{m}} \int_{\mathbb{R}^m/\bar{\Lambda}} \mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,x)d\bar{\nu}_\Lambda(x).\end{aligned} \tag{3.3}$$

Lemma 3.4. *Let ξ be as in (II) and ζ as in (B). Given a compact subset $K \subset X_m$, as $|\Lambda| \to \infty$, where $\Lambda < \mathbb{Z}^m$ satisfies $\bar{\Lambda} \in K$, one has that $||\Lambda|^{-\frac{1}{m}}\xi(\mathcal{G}) - \zeta(\bar{\Lambda})| \to 0$, where $\mathcal{G}$ is $C_{\mathbb{Z}^m/\Lambda}(I)$ (resp. $C^+_{\mathbb{Z}^m/\Lambda}(I)$) and $\mathrm{d}_{\mathbb{R}^m/\bar{\Lambda}}$ is the distance (resp. ns-distance) defined in (2.2) according to the case.*

Proof. Using (3.3) we are reduced to showing

$$|\int_{\mathbb{R}^m/\bar{\Lambda}} \mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,x)d\lambda - \int_{\mathbb{R}^m/\bar{\Lambda}} \mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,x)d\bar{\nu}_\Lambda| \to 0. \tag{3.4}$$

Note that strictly speaking we should have raised the integrals in (3.4) to a power of $1/\alpha$ but since ζ is a proper function the integral on the left is bounded in terms of K and so it is enough to establish (3.4) as it is.

We start by finding a convenient fundamental domain for $\bar{\Lambda}$ that will allow us to evaluate the left hand side of (3.4) and will take advantage of the assumption that $\bar{\Lambda} \in K$. Throughout we use the bar notation to denote scaling by $|\Lambda|^{-1/m}$. The assumption that $\bar{\Lambda} \in K$ means that there is a fixed compact set $K' \subset \mathbb{R}^m_+$ which contains a fundamental domain for $\bar{\Lambda}$. Given a fundamental domain F' for Λ such that $\bar{F'} \subset K'$, we have that $A = F' \cap \mathbb{Z}^m$ is a set of representatives of $\mathbb{Z}^m/\Lambda$. Denoting $C = \{\sum_1^m t_i\mathbf{e}_i : 0 \le t_i < 1\}$, the standard fundamental domain of $\mathbb{Z}^m$, it is straightforward to show that the disjoint

union of cubes $F = \cup_{\mathbf{k}\in A}(\mathbf{k}+C)$ is again a fundamental domain of Λ. It follows that $\bar{F} = \cup_{\mathbf{k}\in A}(\bar{\mathbf{k}}+\bar{C})$ is a fundamental domain for $\bar{\Lambda}$ and since $\bar{A} \subset K'$, by slightly enlarging K' if necessary, we may assume that $\bar{F} \subset K'$.

On identifying $\mathbb{R}^m/\bar{\Lambda}$ with $\bar{F}$ we see that the support of $\bar{\nu}_\Lambda$ is exactly the set $\bar{A}$ and for $\mathbf{k} \in A$, the weight $\bar{\nu}_\Lambda(\bar{\mathbf{k}}) = |A|^{-1} = \lambda(\bar{C})$. Thus, by expressing the integrals on the left hand side of (3.4) as a sum over the cubes $\left\{\bar{\mathbf{k}}+\bar{C} : \mathbf{k} \in A\right\}$, using the triangle inequality, and inserting the absolute value into the integral, we see that the expression on the left hand side of (3.4) is bounded above by

$$\begin{aligned}&\sum_{\mathbf{k}\in A}\int_{\bar{C}} |\,\mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,\bar{\mathbf{k}}+x) - \mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,\bar{\mathbf{k}})|d\lambda(x) \\ &\leq \sup_{x\in\bar{F}}\sup_{y\in x+\bar{C}} |\,\mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,x) - \mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,y)|.\end{aligned} \tag{3.5}$$

By Lemma 2.2, as $\bar{\Lambda}$ varies, the family of functions $\mathrm{d}^\alpha_{\mathbb{R}^m/\bar{\Lambda}}(0,x)$ is equicontinuous on K' and therefore as the diameter of $\bar{C}$ goes to 0 the right hand side of (3.5) goes to zero as well. As this diameter goes to 0 as $|\Lambda| \to \infty$ the claim follows. □

We now collect the above preparations and isolate an important component in the proof of Theorem 1.2.

Corollary 3.5. *Let $\mathcal{A}_i$ be finite collections of subgroups of $\mathbb{Z}^m$ of index ℓ_i. Let μ_i denote the normalized counting measure on $\bar{\mathcal{A}}_i = \left\{\bar{\Lambda} \in X_m : \Lambda \in \mathcal{A}_i\right\}$ and assume $\mu_i \xrightarrow{\mathrm{w}^*} m_{X_m}$. Choose ξ as in (I), (II), or (III) and let $\xi_i : \bar{\mathcal{A}}_i \to (0,\infty)$ be defined as $\xi_i(\bar{\Lambda}) = \ell_i^{-\frac{1}{m}}\xi(\mathcal{G})$, where $\mathcal{G} = C_{\mathbb{Z}^m/\Lambda}(I)$ or $C^+_{\mathbb{Z}^m/\Lambda}(I)$ according to the case. Then, if $\zeta : X_m \to (0,\infty)$ is as in (A), (B), or (C) according to the choice of ξ, then $(\xi_i)_*\mu_i \xrightarrow{\mathrm{w}^*} \zeta_* m_{X_m}$.*

Proof. The proof in each case is an application of Lemma 2.1. Our task is therefore reduced to verifying the conditions in this lemma in each case. The first condition of Lemma 2.1 is properness of ζ. It is straightforward to deduce from Mahler's compactness criterion that if ζ is as in (A)-(C), then ζ is continuous and proper[1] on X_m. The second condition of Lemma 2.1 holds by Lemma 3.3 in cases (I), (III) (with no reference to a compact set in X_m), and by Lemma 3.4 in case (II). □

4. Random Cayley graphs are approximate torus graphs

In this section we prove Theorem 1.2. Let $\Sigma < \mathbb{Z}^n$ be a finite index subgroup and consider the set

$$\mathcal{A}_\Sigma = \{\Lambda < \mathbb{Z}^m : \mathbb{Z}^m/\Lambda \simeq \mathbb{Z}^n/\Sigma\}. \tag{4.1}$$

There is a natural map $\tau : \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) \to \mathcal{A}_\Sigma$ which is defined as follows: Given $s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$, let $\mathbf{u} \in \mathrm{Mat}_{n\times m}(\mathbb{Z})$ be a matrix whose columns represent the elements of s and define $\varphi_\mathbf{u} : \mathbb{Z}^m \to \mathbb{Z}^n/\Sigma$ to be the homomorphism induced by $\mathbf{u}$; that is, for $k \in \mathbb{Z}^m$, $\varphi_\mathbf{u}(k) = \mathbf{u}k + \Sigma$. We define

$$\tau(s) = \Lambda_s \stackrel{\mathrm{def}}{=} \ker\varphi_\mathbf{u} = \{k \in \mathbb{Z}^m : \mathbf{u}k \in \Sigma\}.$$

[1] Note that the properness refers to the range $(0,\infty)$ and in fact in case (C) $\zeta(\Lambda)$ can approach 0 as Λ develops short vectors.

It is clear that Λ_s does not depend on the choice of $\mathbf{u}$ but only on the set s. Since s is a generating set for $\mathbb{Z}^n/\Sigma$, $\varphi_{\mathbf{u}}$ is onto and therefore descends to an isomorphism $\overline{\varphi}_{\mathbf{u}} : \mathbb{Z}^m/\Lambda_s \to \mathbb{Z}^n/\Sigma$. Hence, $\Lambda_s \in \mathcal{A}_\Sigma$ as stated above. Moreover, since $\overline{\varphi}_{\mathbf{u}}$ takes the generating set I of $\mathbb{Z}^m/\Lambda_s$ to the generating set s of $\mathbb{Z}^n/\Sigma$ we conclude the following lemma which explains the importance of the lattices Λ_s to our discussion as they help us transport the discussion from random generating sets to random approximated torus graphs.

Lemma 4.1. *Let Σ and s be as above.*

1. *Λ_s is a subgroup of index $|\Sigma|$ of $\mathbb{Z}^m$ and moreover there exists an isomorphism $\mathbb{Z}^m/\Lambda_s \to \mathbb{Z}^n/\Sigma$ which takes the generating set I to s.*
2. *The graph $C_{\mathbb{Z}^n/\Sigma}(s)$ is isomorphic to the approximated torus graph $C_{\mathbb{Z}^m/\Lambda_s}(I)$.*
3. *The digraph $C^+_{\mathbb{Z}^n/\Sigma}(s)$ is isomorphic to the approximated torus digraph $C^+_{\mathbb{Z}^m/\Lambda_s}(I)$.*

The object that will help us analyze the map $\tau : \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) \to \mathcal{A}_\Sigma$ is $\mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$; the collection of homomorphisms from $\mathbb{Z}^m$ onto $\mathbb{Z}^n/\Sigma$. We have the following natural diagram:

$$\begin{array}{ccc} & \mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma) & \\ {\scriptstyle \pi_1}\swarrow & & \searrow{\scriptstyle \pi_2} \\ \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) & \xrightarrow[\tau]{} & \mathcal{A}_\Sigma. \end{array}$$

Here, π_i are defined as follows: Given $\varphi \in \mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$, $\pi_1(\varphi) = \varphi(I)$ (where I is the standard basis of $\mathbb{Z}^m$), and $\pi_2(\varphi) = \ker\varphi$. The map τ defined above takes $s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ and chooses φ in the π_1-fiber and then applies π_2. That is, τ closes the above diagram in a commutative manner. On $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ there is a natural action of $\mathrm{Aut}(\mathbb{Z}^n/\Sigma)$ and on $\mathcal{A}_\Sigma$ there is a natural action of $\mathrm{GL}_m(\mathbb{Z})$. The main reason we introduce $\mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$ is that on it we have a natural action of the product $\mathrm{GL}_m(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}^n/\Sigma)$ such that each of π_1 and π_2 intertwines the action of the corresponding group. Namely, given $\varphi \in \mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$ and $(\gamma, \delta) \in \mathrm{GL}_m(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}^n/\Sigma)$ we define $(\gamma, \delta)\varphi = \delta\varphi\gamma^{-1}$.

Definition 4.2. We denote by $\nu_\Sigma, \mu_\Sigma, \bar{\mu}_\Sigma$ the normalized counting measures on $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$, $\mathcal{A}_\Sigma$, $\bar{\mathcal{A}}_\Sigma$ respectively.

Lemma 4.3.

1. *$\mathrm{GL}_m(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}^n/\Sigma)$ acts transitively on $\mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$.*
2. *$\mathrm{GL}_m(\mathbb{Z})$ acts transitively on $\mathcal{A}_\Sigma$.*
3. *The map $\tau : \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) \to \mathcal{A}_\Sigma$ has fibers of constant size and so $\tau_*\nu_\Sigma = \mu_\Sigma$.*
4. *As $\Sigma \to \infty$ according to Definition 1.1, $|\mathcal{A}_\Sigma| \to \infty$.*
5. *As $\Sigma \to \infty$ according to Definition 1.1, $\bar{\mu}_\Sigma \xrightarrow{\mathrm{w}^*} m_{X_m}$.*

Proof. (1). Let $\varphi_1, \varphi_2 \in \mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$ and assume first that $\ker\varphi_1 = \ker\varphi_2 = \Lambda$, if we denote by $\overline{\varphi}_i : \mathbb{Z}^m/\Lambda \to \mathbb{Z}^n/\Sigma$ the corresponding isomorphisms that φ_i descend to, then post-composing φ_2 with $\delta = \overline{\varphi}_1\overline{\varphi}_2^{-1} \in \mathrm{Aut}(\mathbb{Z}^n/\Sigma)$ we get that $\delta\varphi_2$ and φ_1 have the same kernel Λ and descend to the same map on $\mathbb{Z}^m/\Lambda$. We conclude that $\delta\varphi_2 = \varphi_1$. Thus in order to complete the proof of (1) we only need to show that given $\varphi_1, \varphi_2 \in \mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$ there exists $\gamma \in \mathrm{GL}_m(\mathbb{Z})$ such that $\ker\varphi_1 = \ker\varphi_2\gamma = \gamma^{-1}\ker\varphi_2$. Indeed, if $\ker\varphi_i = \Lambda_i$ then $\mathbb{Z}^m/\Lambda_i$ are isomorphic and since $\mathbb{Z}^m$ is a free abelian group

such an isomorphism must arise from an isomorphism $\mathbb{Z}^m \to \mathbb{Z}^m$ taking Λ_1 to Λ_2 which completes the proof.
(2). Since π_2 is onto and intertwines the actions of $\mathrm{GL}_m(\mathbb{Z})$, and since for $\delta \in \mathrm{Aut}(\mathbb{Z}^n/\Sigma)$ and $\varphi \in \mathrm{Hom}_{\mathrm{epi}}(\mathbb{Z}^m, \mathbb{Z}^n/\Sigma)$ we have that $\ker \varphi = \ker \delta\varphi$, the transitivity proved in (1) implies the transitivity claimed in (2).
(3) The fibers of π_1 are of size $m!$ and each such fiber is contained in a single π_2-fiber, thus the claim will follow once we establish that π_2 has fibers of constant size. Indeed, the transitivity proved in (1) and (2), and the fact (which was used in the proof of (2)) saying that the $\mathrm{Aut}(\mathbb{Z}^n/\Sigma)$-action preserves the π_2-fibers imply that given two π_2-fibers there exists an element of $\mathrm{GL}_m(\mathbb{Z})$ which maps one to the other. In particular, they are of the same size as claimed.
(4) Recall that given a sublattice $\Lambda < \mathbb{Z}^m$ there exist unique positive integers $\ell_1, \dots, \ell_m$ referred to as *the elementary divisors* of Λ in $\mathbb{Z}^m$, which satisfy the division relation $\ell_i | \ell_{i+1}$ and for which there exists a basis $\{v_i\}_1^m$ of $\mathbb{Z}^m$ such that $\{\ell_i v_i\}_1^m$ form a basis for Λ (see for example [SD01]). It is shown in the proof of [EMSS16, Theorem 5.3] that the cardinality of the orbit $\mathrm{GL}_m(\mathbb{Z})\Lambda$, which equals $|\mathcal{A}_\Sigma|$ by (2), goes to infinity if and only if the ratio ℓ_m/ℓ_1 does so too. Due to the division relation between the ℓ_i's, the latter is equivalent to the divergence of $(\prod_1^m \ell_i)/\ell_1^m = |\Lambda|/\ell_1^m = |\Sigma|/\ell_1^m$. We are therefore reduced to showing that as $\Sigma \to \infty$ according to Definition 1.1, one has $|\Sigma|/\ell_1^m \to \infty$. Since $\mathbb{Z}^n/\Sigma \simeq \mathbb{Z}^m/\Lambda$ and $m \geq n$ we have that the elementary divisors of Λ in $\mathbb{Z}^m$ are obtained from to those of Σ in $\mathbb{Z}^n$ by augmenting them by $m-n$ 1's in the beginning. Thus, if $m > n$ then $\ell_1 = 1$ and so $\Sigma \to \infty$ if and only if $|\Sigma|/\ell_1^m \to \infty$. In the case $n = m$, since ℓ_1 is the first elementary divisor of Σ in $\mathbb{Z}^n$, then we get that $\ell_1 = \gcd \Sigma$. Hence, again $\Sigma \to \infty$ if and only if $|\Sigma|/\ell_1^n \to \infty$, which concludes the proof of (4).
(5). This follows from part (4) and the following theorem which is a special case of [EO06, Theorem 1.2] (see also [COU01], [GM03]):

Theorem 4.4. *If μ_i is the normalized counting measure supported on a finite $\mathrm{GL}_m(\mathbb{Z})$-orbit in X_m such that the cardinality $|\operatorname{supp}(\mu_i)| \to \infty$ as $i \to \infty$, then $\mu_i \xrightarrow{\mathrm{w}^*} m_{X_m}$.*

□

We are now ready to prove the main result, Theorem 1.2.

Proof of Theorem 1.2. Choose $\Sigma_i \to \infty$ and let ξ be as in (I), (II), or (III). Consider the diagram

$$\begin{array}{ccc} \mathcal{S}_{\mathbb{Z}^n/\Sigma_i}(m) & \xrightarrow{s \mapsto \bar{\tau}(s) = \bar{\Lambda}_s} & \bar{\mathcal{A}}_{\Sigma_i} \\ & {\scriptstyle \xi_i} \searrow \quad \swarrow {\scriptstyle \xi_i'} & \\ & \mathbb{R} & \end{array}$$

where $\xi_i(s) = |\Sigma_i|^{-\frac{1}{m}} \xi(\mathcal{G})$, where $\mathcal{G} = C_{\mathbb{Z}^n/\Sigma_i}(s)$ or $C^+_{\mathbb{Z}^n/\Sigma_i}(s)$ according to the case, and similarly, $\xi_i'(\bar{\Lambda}) = |\Sigma_i|^{-\frac{1}{m}} \xi(\mathcal{G})$, where $\mathcal{G} = C_{\mathbb{Z}^m/\Lambda}(I)$ or $C^+_{\mathbb{Z}^m/\Lambda}(I)$ according to the case. By Lemma 4.1 the diagram is indeed commutative. Our goal is to show that ξ_i converge in distribution to the random variable ζ on X_m, where ζ is as in (A), (B), or (C) according to the choice of ξ. This is the same as saying that $(\xi_i)_* \nu_{\Sigma_i} \xrightarrow{\mathrm{w}^*} \zeta_* m_{X_m}$. Since $\xi_i = \xi_i' \circ \bar{\tau}$ and by Lemma 4.3(3) $\tau_* \nu_{\Sigma_i} = \mu_{\Sigma_i}$ (which is equivalent to saying that $\bar{\tau}_* \nu_{\Sigma_i} = \bar{\mu}_{\Sigma_i}$), we

are reduced to showing that $(\xi_i')_*\bar{\mu}_{\Sigma_i} \xrightarrow{\text{w}^*} \zeta_* m_{X_m}$. This follows from Corollary 3.5 which is applicable since $\bar{\mu}_{\Sigma_i} \xrightarrow{\text{w}^*} m_{X_m}$ by Lemma 4.3(5). □

5. A refinements of Theorem 1.2

In this section we restrict attention to the case $m > n$ and consider only groups of the form $\mathbb{Z}^n/\Sigma$ where $\Sigma = k\mathbb{Z}^n$. Thus according to Definition 1.1, $\Sigma \to \infty$ if and only if $k \to \infty$. We wish to define families of natural non-uniform probability measures on $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ with respect to which the conclusion of Theorem 1.2 will remain valid.

Our next goal is to put all the sets $\mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)$ in a fixed ambient space. As a first step, our restriction to $\Sigma = k\mathbb{Z}^n$ allows us to embed all the groups $\mathbb{Z}^n/\Sigma$ in a single continuous torus. Namely, let $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ and let $\iota_k : \mathbb{Z}^n/k\mathbb{Z}^n \hookrightarrow \mathbb{T}^n$ be defined by $\iota_k(u + k\mathbb{Z}^n) = \frac{1}{k}u + \mathbb{Z}^n$. Next, the collection of subsets of size m in $\mathbb{T}^n$ may be thought of as contained in the quotient of the product $(\mathbb{T}^n)^m$ by the permutation group S_m on $\{1, \dots, m\}$. Let us denote this quotient by $Y = S_m\backslash(\mathbb{T}^n)^m$. Thus, using ι_k we may and will identify $\mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)$ with a subset of Y. We shall refer to the push-forward probability measure $\pi_*\lambda^{\otimes m}$ on Y as the Lebesgue measure on Y, where $\pi : (\mathbb{T}^n)^m \to Y$ is the quotient map and λ is the usual Lebesgue measure on the torus $\mathbb{T}^n$.

Given a subset $D \subset Y$, we define the probability measure $\nu_{D,k}$ on $\mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)$ as the restriction of the uniform probability measure on $\mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)$ to D (assuming that $\mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m) \cap D \neq \varnothing$). Finally, by a Jordan measurable set $D \subset Y$ we mean a measurable set with boundary of Lebesgue measure zero. The importance of Jordan measurability to our discussion is that the characteristic function χ_D of such a set can be approximated from above and below (in L^1-norm) by continuous functions and thus χ_D behaves nicely when integrated against a sequence of measures which converge weak-star to the Lebesgue measure.

Theorem 5.1. *Fix $m > n$ and let $\Sigma < \mathbb{Z}^n$ be of the form $\Sigma = k\mathbb{Z}^n$. Let $D \subset Y$ be a Jordan measurable set of positive Lebesgue measure and let $\nu_{D,k}$ be the restriction of the uniform measure on $\mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ to D. Then, for all k large enough $\mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m) \cap D \neq \varnothing$ and the conclusion of Theorem 1.2 remains valid (with the same limit distributions) if s is chosen randomly according to $\nu_{D,k}$.*

Sketch of proof. The proof is identical to that of Theorem 1.2 where instead of using the collection $\mathcal{A}_\Sigma = \{\Lambda_s : s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)\}$ one uses the sub-collection $\{\Lambda_s : s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m) \cap D\}$. The only ingredient missing is an equidistribution result substituting Lemma 4.3(5) saying that the normalized counting measure $\bar{\mu}_{D,k}$ on $\{\bar{\Lambda}_s : s \in \mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m) \cap D\}$ satisfies $\bar{\mu}_{D,k} \xrightarrow{\text{w}^*} m_{X_m}$.

In order to justify this equidistribution statement we need to introduce some terminology and notation. For $s \in \mathcal{S}_{\mathbb{Z}^n/\Sigma}(m)$ let $\mathbf{u} \in \text{Mat}_{n\times m}(\mathbb{Z})$ be a matrix whose columns represent the elements of s. Let $d = n + m$ and consider the matrix $g_{\mathbf{u}} = \begin{pmatrix} I_m & 0 \\ \mathbf{u} & kI_n \end{pmatrix}$. It is clear that the lattice $L_s = g_{\mathbf{u}}\mathbb{Z}^d$ does not depend on the choice of $\mathbf{u}$ but only on s. We leave it as an exercise (see for example [EMSS16, equation (2.12)]) to check that $L_s \cap \mathbb{R}^m = \Lambda_s$ (where $\mathbb{R}^m$ denotes the subspace of the first m coordinates in $\mathbb{R}^d$). Let us denote by $L_s' \in X_d$ the unimodular lattice obtained by applying to the lattice L_s in $\mathbb{R}^d$ the diagonal matrix

$a(k) = \begin{pmatrix} k^{-\frac{n}{m}} I_m & 0 \\ 0 & I_n \end{pmatrix}$, so that by the above exercise $L'_s \cap \mathbb{R}^m = \bar{\Lambda}_s$. The equidistribution $\bar{\mu}_{D,k} \xrightarrow{\text{w}^*} m_{X_m}$ follows from [EMSS16, Theorem 1.3] which is a joint equidistribution theorem which may be restated (see Remark 5.2) as saying that the collection of pairs

$$\left\{(s, L'_s) : s \in \mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)\right\} \tag{5.1}$$

equidistributes in the product space $Y \times Z$. Here, Y is as above and $Z \subset X_d$ is the subspace defined by $Z = \{L \in X_d : L \cap \mathbb{R}^m \in X_m\}$. The space Z has a natural 'uniform' probability measure on it and the equidistribution eluded to above means that the normalized counting measure on the collection (5.1) converges weak-star to the product of the Lebesgue measure on Y and the uniform measure on Z. In turn, there is a natural projection $Z \to X_m$ defined by $L \mapsto L \cap \mathbb{R}^m$ and since the uniform measure on Z projects to m_{X_m} we conclude that the collection of pairs $\left\{(s, \bar{\Lambda}_s) : s \in \mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)\right\}$ equidistributes in the product $Y \times X_m$. In particular, the fact that the limit measure is a product measure implies that if we condition on the left coordinate being in D the right coordinate still equidistributes in X_m. That is, $\left\{\bar{\Lambda}_s : s \in \mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m) \cap D\right\}$ equidistributes in X_m as desired. The assumption that D is Jordan measurable and of positive measure is exactly the condition needed in order that the equidistribution in the product $Y \times Z$ may be conditioned on the fact that the left coordinate is in D. □

Remark 5.2. Strictly speaking [EMSS16, Theorem 1.3] does not deal with the product space $Y \times Z$ but with $(\mathbb{T}^n)^m \times Z$. Instead of considering subsets $s \in \mathcal{S}_{\mathbb{Z}^n/k\mathbb{Z}^n}(m)$ they consider m-tuples $\mathbf{u} = \{u_1, \ldots, u_m\} \in (\mathbb{Z}^n/k\mathbb{Z}^n)^m$ (which we think of as contained in $(\mathbb{T}^n)^m$ using ι_k), where the u_i's are assumed to generate $\mathbb{Z}^n/k\mathbb{Z}^n$. This difference entails a minor issue which is that m-tuples corresponds to subsets of size $\leq m$ rather than equal to m and furthermore, this correspondence is not 1-1 and the size of the fibers is not constant. Since the percentage of m-tuples which correspond to sets of size $< m$ is negligible these two issues may be ignored and it is straightforward to deduce the version of the theorem stated above from the formulation in [EMSS16]. We leave the details to the interested reader.

References

[AGG10] G. Amir and O. Gurel-Gurevich, *The diameter of a random Cayley graph of* $\mathbb{Z}_q$, Groups Complex. Cryptol. **2** (2010), no. 1, 59–65. MR2672553

[COU01] L. Clozel, H. Oh, and E. Ullmo, *Hecke operators and equidistribution of Hecke points*, Invent. Math. **144** (2001), no. 2, 327–351. MR1827734

[EMSS16] M. Einsiedler, S. Mozes, N. Shah, and U. Shapira, *Equidistribution of primitive rational points on expanding horospheres*, Compos. Math. **152** (2016), no. 4, 667–692. MR3484111

[EO06] A. Eskin and H. Oh, *Ergodic theoretic proof of equidistribution of Hecke points*, Ergodic Theory Dynam. Systems **26** (2006), no. 1, 163–167. MR2201942

[GM03] D. Goldstein and A. Mayer, *On the equidistribution of Hecke points*, Forum Math. **15** (2003), no. 2, 165–189. MR1956962

[Mar10] J. Marklof, *The asymptotic distribution of Frobenius numbers*, Invent. Math. **181** (2010), no. 1, 179–207. MR2651383

[MS13] J. Marklof and A. Strömbergsson, *Diameters of random circulant graphs*, Combinatorica **33** (2013), no. 4, 429–466. MR3133777

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001. MR1826558

Department of Mathematics, Technion, Haifa, Israel
E-mail address: ushapira@tx.technion.ac.il
E-mail address: reut@tx.technion.ac.il