INTEGER POINTS ON SPHERES AND THEIR ORTHOGONAL GRIDS

MENNY AKA, MANFRED EINSIEDLER, AND URI SHAPIRA

Abstract. The set of primitive vectors on large spheres in the euclidean space of dimension $d \geq 3$ equidistribute when projected on the unit sphere. We consider here a refinement of this problem concerning the direction of the vector together with the shape of the lattice in its orthogonal complement. Using unipotent dynamics we obtained the desired equidistribution result in dimension $d \geq 6$ and in dimension $d = 4, 5$ under a mild congruence condition on the square of the radius. The case of $d = 3$ is considered in a separate paper.

1. Introduction

Let $d \geq 3$ be a fixed integer. Let $\mathbb{Z}^d_{\text{prim}}$ be the set of primitive vectors in $\mathbb{Z}^d$. Set

$$\mathbb{S}^{d-1}(D) \overset{\text{def}}{=} \left\{ v \in \mathbb{Z}^d_{\text{prim}} : \|v\|_2^2 = D \right\} = \mathbb{Z}^d_{\text{prim}} \cap \left(\sqrt{D}\mathbb{S}^{d-1} \right),$$

where $\mathbb{S}^{d-1} \overset{\text{def}}{=} \left\{ x \in \mathbb{R}^d : \|x\|_2 = 1 \right\}$. We would like to discuss the simultaneous equidistribution of the direction $\frac{v}{\sqrt{D}} \in \mathbb{S}^{d-1}$ of the elements in $\mathbb{S}^{d-1}(D)$ and the *shape* $[\Lambda_v]$ of the orthogonal lattice

$$\Lambda_v = \mathbb{Z}^d \cap v^{\perp}.$$

To make this more precise fix a copy of $\mathbb{R}^{d-1} \overset{\text{def}}{=} \mathbb{R}^{d-1} \times \{0\}$ in $\mathbb{R}^d$ and choose for every $v \in \mathbb{S}^{d-1}(D)$ a rotation $k_v \in \mathrm{SO}_d(\mathbb{R})$ with $k_v v = \sqrt{D} e_d$ so that $k_v \Lambda_v$ becomes a lattice in $\mathbb{R}^{d-1}$. Note that

$$[\mathbb{Z}^d : (\mathbb{Z}v \oplus \Lambda_v)] = D \tag{1.1}$$

since primitivity of v implies that the homomorphism $\mathbb{Z}^d \to \mathbb{Z}$ defined by $u \mapsto (u, v)$ is surjective and $\mathbb{Z}v \oplus \Lambda_v$ is the preimage of $D\mathbb{Z}$.

Therefore, $k_v \Lambda_v$ is a lattice in $\mathbb{R}^{d-1}$ of covolume $\sqrt{D}$. In order to normalize this covolume, we further multiply by the diagonal matrix $a_v = \mathrm{diag}(D^{\frac{-1}{2(d-1)}}, \cdots, D^{\frac{-1}{2(d-1)}}, D^{\frac{1}{2}})$. Note that the set of possible choice of k_v is precisely $\mathrm{SO}_{d-1}(\mathbb{R}) k_v$ and that a_v commutes with $\mathrm{SO}_{d-1}(\mathbb{R})$. Recall

M.A. acknowledges the support of ISEF, Advanced Research Grant 228304 from the ERC, and SNF Grant 200021-152819.

M.E. acknowledges the support of the SNF Grant 200021-127145 and 200021-152819.

U.S. acknowledges the support of the Chaya fellowship and ISF grant 357/13.

that $\mathrm{SL}_{d-1}(\mathbb{R})/\mathrm{SL}_{d-1}(\mathbb{Z})$ is identified with the space of unimodular lattices in $\mathbb{R}^{d-1}$ so that we obtain an element

$$[\Lambda_v] \overset{\mathrm{def}}{=} \mathrm{SO}_{d-1}(\mathbb{R})a_v k_v \Lambda_v \in \mathcal{X}_{d-1} = \mathrm{SO}_{d-1}(\mathbb{R})\backslash \mathrm{SL}_{d-1}(\mathbb{R})/\mathrm{SL}_{d-1}(\mathbb{Z}),$$

which we refer to as the *shape of the lattice* Λ_v.

It is possible to obtain still a bit more geometric information from the primitive vector v as follows. Given $v \in \mathbb{S}^{d-1}(D)$ choose $w \in \mathbb{Z}^d$ with $(w, v) = 1$. If now $v_1, \dots, v_{d-1}$ is a $\mathbb{Z}$-basis of Λ_v we see that $v_1, \dots, v_{d-1}, w$ is a $\mathbb{Z}$-basis of $\mathbb{Z}^d$ and we may assume that $\det(v_1, \cdots, v_{d-1}, w) = 1$. Let $g_v \in \mathrm{SL}_d(\mathbb{Z})$ denote the matrix whose columns are $v_1, \cdots, v_{d-1}, w$. Set $\mathrm{ASL}_{d-1} = \left\{\begin{pmatrix} g & * \\ 0 & 1\end{pmatrix} \mid g \in \mathrm{SL}_{d-1}\right\}$. The set of possible choices for g_v is the coset $g_v\mathrm{ASL}_{d-1}(\mathbb{Z})$. We define a *grid in* $\mathbb{R}^{d-1}$ to be a unimodular lattice Λ in $\mathbb{R}^{d-1}$ together with a marked point on the $(d-1)$-dimensional torus $\mathbb{R}^{d-1}/\Lambda$. The space $\mathrm{ASL}_{d-1}(\mathbb{R})/\mathrm{ASL}_{d-1}(\mathbb{Z})$ is the moduli space of grids in $\mathbb{R}^{d-1}$. Thus, $k_v g_v \mathrm{ASL}_{d-1}(\mathbb{Z})$ represent the grid consisting of the rotated image of Λ_v to $\mathbb{R}^{d-1}$ together with the rotated image of w orthogonally projected into $\mathbb{R}^{d-1}$, and the well-defined double coset

$$[\Delta_v] \overset{\mathrm{def}}{=} \mathrm{SO}_{d-1}(\mathbb{R})a_v k_v g_v \mathrm{ASL}_{d-1}(\mathbb{Z})$$

represent this grid up-to rotations of the hyperplane $\mathbb{R}^{d-1}$. Thus we obtain the element $[\Delta_v]$ of the space

$$\mathcal{Y}_{d-1} \overset{\mathrm{def}}{=} \mathrm{SO}_{\mathrm{d-1}}(\mathbb{R}) \setminus \mathrm{ASL}_{\mathrm{d-1}}(\mathbb{R})/\mathrm{ASL}_{\mathrm{d-1}}(\mathbb{Z}).$$

One should think about $[\Delta_v]$ as the shape of the orthogonal lattice Λ_v together with a point on the corresponding $(d-1)$-dimensional torus which marks the position of orthogonal projection of w to the hyperplane containing Λ_v.

Let $\tilde{\nu}_D$ denote the normalized counting measure on the set

$$\left\{\left(\frac{v}{\|v\|}, [\Delta_v]\right) : v \in \mathbb{S}^{d-1}(D)\right\} \subset \mathbb{S}^{d-1} \times \mathcal{Y}_{d-1}.$$

We are interested to find $A \subset \mathbb{N}$ for which

$$\tilde{\nu}_D \overset{\mathrm{weak}^*}{\longrightarrow} m_{\mathbb{S}^{d-1}} \otimes m_{\mathcal{Y}_{d-1}} \text{ as } D \to \infty \text{ with } D \in A \tag{1.2}$$

where $m_{\mathbb{S}^{d-1}} \otimes m_{\mathcal{Y}_{d-1}}$ is the product of the natural uniform measures on $\mathbb{S}^{d-1}$ and $\mathcal{Y}_{d-1}$. We propose the following conjecture as a generalization of Linnik's Problem on spheres:

Conjecture 1.1. *The convergence in (1.2) holds for the subset $A = \mathbb{N}$ if $d > 4$, holds for $A = \mathbb{N} \setminus (8\mathbb{N})$ if $d = 4$, and for the subset*

$$A = \left\{D \geq 1 \mid D \textit{ is not congruent to } 0, 4, 7 \textit{ modulo } 8\right\}$$

if $d = 3$.

By a theorem of Legendre the restriction to the proper subset of $\mathbb{N}$ as in the above conjecture for $d = 3$ is equivalent to $\mathbb{S}^2(D)$ being nonempty, and hence necessary. A similar statement holds for $d = 4$.

In a separate paper [AES14] we obtain for the case $d = 3$ some partial results towards this conjecture. However, for $d > 3$ we can give much stronger results using the techniques presented here. For an odd rational prime p let $\mathbb{D}(p) = \{D : p \nmid D\}$. The main result of this paper is the following:

Theorem 1.2. *Conjecture 1.1 is true for $d > 5$. For $d = 5$ (resp. $d = 4$), the convergence in (1.2) holds for the subset $A = \mathbb{D}(p)$ (resp. $A = \mathbb{D}(p) \setminus (8\mathbb{N})$) where p is any fixed odd prime.*

Theorem 1.2 will be proven using the theorem of Mozes and Shah [MS95] concerning limits of algebraic measures with unipotent flows acting ergodically. More precisely we will need a p-adic analogue of this result, which has been given more recently by Gorodnik and Oh [GO11]. In particular we note that Theorem 1.2 should therefore be considered a corollary of the measure classification theorems for unipotent flows on S-arithmetic quotients (see [Ra95] and [MT94]).

As explained in Lemma 3.7, the congruence condition $D \in \mathbb{D}(p)$ is a splitting condition which enables us to use the existing theory of unipotent dynamics. It is possible to remove this splitting condition for $d = 4, 5$ by giving effective dynamical arguments in the spirit of [EMMV14] (see also [EMV09]), but this result is not general enough for that purpose. In [ERW14] René Rühr, Philipp Wirth, and the second named author use the methods of [EMMV14] to remove the congruence condition for $d = 4, 5$ in Theorem 1.2. We note however, that the case $d = 3$ remains open (apart from the partial results in [AES14] that concerns itself only with the problem on $\mathbb{S}^2 \times \mathcal{X}_2$ and involves some stronger congruence conditions).

Our interest in this problem arose through the work of W. Schmidt [Sch98], J. Marklof [Mar10] (see also [EMSS]). However, as Peter Sarnak and Ruixiang Zhang pointed out to us, Maass [Maa56] already asked similar questions in 1956 (see also [Maa59]). More precisely, the above question is the common refinement of Linnik's problem and the question of Maass.

2. Notation and organization of the paper

A sequence of probability measures μ_n on a metric space X is said to equidistribute to a probability measure μ if μ_n converge to μ in the weak* topology on the space of probability measures on X. A probability measure μ is called a weak* *limit* of a sequence of measures μ_n if there exists a subsequence (n_k) such that μ_{n_k} equidistribute to μ as $k \to \infty$. For a probability measure μ and a measurable set A of positive measure, the restriction $\mu|_A$ of μ to A is defined by $\mu|_A(B) = \frac{1}{\mu(A)}\mu(A \cap B)$ for any measurable set B.

Recall that a discrete subgroup $\Lambda < L$ is called a lattice if L/Λ admits an L-invariant probability measure. Given a locally compact group L and a subgroup $M < L$ such that L/M admits an L-invariant probability measure, it is unique, we denote it by $\mu_{L/M}$, and call it the *uniform measure* or the *Haar measure* on L/M. If furthermore, $K < L$ is a compact subgroup then there is a natural quotient map $L/M \to K\backslash L/M$, and the uniform measure on $K\backslash L/M$ is by definition the push forward of the Haar measure on L/M.

We recall that the Haar measure on a finite volume orbit $Hg\Gamma$ is the push-forward of the uniform measure on $H/\left(H \cap g\Gamma g^{-1}\right)$. Note that a twisted orbit of the form $gH\Gamma$ can be thought of as an orbit for the subgroup gHg^{-1} since $gH\Gamma = gHg^{-1}g\Gamma$.

For a finite set S of valuations on $\mathbb{Q}$ we set $\mathbb{Q}_S = \prod_{v\in S}\mathbb{Q}_v$ and $\mathbb{Z}^S = \mathbb{Z}\left[\left\{\frac{1}{p} : p \in S \setminus \{\infty\}\right\}\right]$. For a prime number p, $\mathbb{Z}_p$ denotes the ring of p-adic integers (so with this notation $\mathbb{Z}^{\{p\}} \cap \mathbb{Z}_p = \mathbb{Z}$). As usual we will embedd $\mathbb{Z}^S$ diagonally into $\mathbb{Q}_S$, where $q \in \mathbb{Z}^S$ is mapped to $(q, \ldots, q) \in \mathbb{Q}_S$. When $\infty \in S$, the group $\mathbb{Z}^S$ is a discrete and cocompact subgroup of $\mathbb{Q}_S$.

For an algebraic group $\mathbb{P}$ we write $\mathbb{P}_S \overset{\text{def}}{=} \mathbb{P}(\mathbb{Q}_S)$. For a semisimple algebraic $\mathbb{Q}$-group $\mathbb{P}$ we let $\pi_{\mathbb{P}} : \tilde{\mathbb{P}} \to \mathbb{P}$ be the simply connected covering map over $\mathbb{Q}$, which is unique up-to $\mathbb{Q}$-isomorphism (See [Pro07, Thereom 2.6] for details). We denote by $\mathbb{P}_S^+$ the image of $\tilde{\mathbb{P}}_S$ under $\pi_{\mathbb{P}}$. We also recall that $\mathbb{P}(\mathbb{Z}^S)$ is a lattice in $\mathbb{P}(\mathbb{Q}_S)$ if $\infty \in S$ and $\mathbb{P}$ is semisimple and also if $\mathbb{P} = \mathrm{ASL}_{d-1}$. As we will see later the subgroup $\mathbb{P}_S^+ < \mathbb{P}_S$ plays an important role in some of the ergodic theorems on $\mathbb{P}(\mathbb{Q}_S)/\mathbb{P}(\mathbb{Z}^S)$ that we will use.

The letter e will always denote the identity element of a group, and we will sometimes use subscripts to indicate the corresponding group, e.g. we may write $e_\infty \in \mathbb{P}(\mathbb{R}), e_p \in \mathbb{P}(\mathbb{Q}_p)$, or $e_f \in \mathbb{P}(\prod_{p\in S\setminus\{\infty\}}\mathbb{Q}_p)$.

This paper is organised as follows: The desired equidistribution (1.2) follows from an equidistribution of "joined" orbits on a product of S-adic homogeneous spaces, which is proved in §3 using unipotent dynamics. The translation between the result of §3 to (1.2) is stated in §4 and proved in §5.

3. Equidistribution of joined S-adic orbits

Fix some finite set $S \ni \infty$ of valuations of $\mathbb{Q}$. We define the algebraic groups $\mathbb{G}_1 = \mathrm{SO_d}, \mathbb{G}_2 = \mathrm{ASL_{d-1}}$, $\overline{\mathbb{G}}_2 = \mathrm{SL_{d-1}}$, $\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2$, and $\overline{\mathbb{G}} = \mathbb{G}_1 \times \overline{\mathbb{G}_2}$. Consider the homogeneous spaces $\mathcal{Y}^S \overset{\text{def}}{=} \mathbb{G}_S/\mathbb{G}(\mathbb{Z}^S)$ and $\mathcal{X}^S \overset{\text{def}}{=} \overline{\mathbb{G}}_S/\overline{\mathbb{G}}(\mathbb{Z}^S)$. We write $\pi^S : \mathcal{Y}^S \to \mathcal{X}^S$ for the map induced by the natural projection $\rho_{\mathrm{SL_{d-1}}} : \mathrm{ASL}_{d-1} \to \mathrm{SL}_{d-1}$. Finally, let $\mathcal{Y}_i^S = \mathbb{G}_{i,S}/\mathbb{G}_i(\mathbb{Z}^S)$.

For $v \in \mathbb{Z}^d_{\text{prim}}$ we set $\mathbb{H}_v \overset{\text{def}}{=} \mathrm{Stab}_{\mathbb{G}_1}(v)$ under the natural action. The group $\mathbb{H}_v$ is defined over $\mathbb{Z} \subset \mathbb{Q}$ as $v \in \mathbb{Z}^d$. Let us mention at this point that we will prove Theorem 1.2 by studying the dynamics and the orbits of the stabilizer $\mathbb{H}_v$ of v which in particular will allows us to conclude that there are many primitive vectors in $\mathbb{S}(\|v\|^2)$ if $D = \|v\|^2$ is sufficiently large.

We set $\mathrm{SO}_{d-1}(\mathbb{R}) = \mathrm{Stab}_{\mathbb{G}_1}(e_d)(\mathbb{R})$ and note that $k_v^{-1}\mathrm{Stab}_{\mathbb{G}_1}(e_d)(\mathbb{R})k_v = k_v^{-1}\mathrm{SO}_{d-1}(\mathbb{R})k_v = \mathbb{H}_v(\mathbb{R})$. Consider the diagonally embedded algebraic group $\mathbb{L}_v$ defined by

$$\mathbb{L}_v(R) \overset{\mathrm{def}}{=} \left\{\left(h, g_v^{-1}hg_v\right) : h \in \mathbb{H}_v(R)\right\} \tag{3.1}$$

for any ring R. As $g_v \in \mathrm{SL}_d(\mathbb{Z})$, the group $\mathbb{L}_v$ is also defined over $\mathbb{Z} \subset \mathbb{Q}$. We also define

$$\overline{\mathbb{L}}_v(R) \overset{\mathrm{def}}{=} \left\{\left(h, \rho_{\mathrm{SL_{d-1}}}(g_v^{-1}hg_v)\right) : h \in \mathbb{H}_v(R)\right\}.$$

For $v \in \mathbb{S}^{d-1}(D)$ let $\theta_v = a_v k_v g_v, \bar{\theta}_v = \rho_{\mathrm{SL_{d-1}}}(a_v k_v g_v)$ and consider the orbits

$$\mathbf{O}_{v,S} \overset{\mathrm{def}}{=} (k_v, e_f, \theta_v, e_f)\mathbb{L}_{v,S}^{+}\mathbb{G}(\mathbb{Z}^S) \subset \mathcal{Y}_S \tag{3.2}$$

and

$$\overline{\mathbf{O}}_{v,S} \overset{\mathrm{def}}{=} (k_v, e_f, \bar{\theta}_v, e_f)\overline{\mathbb{L}}_{v,S}^{+}\overline{\mathbb{G}}(\mathbb{Z}^S) \subset \mathcal{X}_S.$$

As $\mathbb{L}_v$ is $\mathbb{Q}$-anisotropic (e.g. because $\mathbb{L}_v(\mathbb{R})$ is compact), the Borel Harish-Chandra Theorem (see e.g. [Mar91, Theorem I.3.2.4]) implies that these are compact orbits. Let $\mu_{v,S}$ (resp. $\overline{\mu}_{v,S}$) be the Haar measure on these orbits and define $\mu_S \overset{\mathrm{def}}{=} \mu_{\mathbb{G}_S^+/\mathbb{G}_S^+\cap\mathbb{G}(\mathbb{Z}^S)}$ and $\overline{\mu}_S \overset{\mathrm{def}}{=} \mu_{\overline{\mathbb{G}}_S^+/\overline{\mathbb{G}}_S^+\cap\overline{\mathbb{G}}(\mathbb{Z}^S)}$.

Remark 3.1. We have $\pi_*^S(\mu_{v,S}) = \overline{\mu}_{v,S}$ and $\pi_*^S(\mu_S) = \overline{\mu_S}$.

Theorem 3.2. *Let p be a fixed odd prime and set $S = \{\infty, p\}$. For $d > 5$ and for any sequence $\{v_n\} \subset \mathbb{Z}^d_{prim}$ with $\|v_n\| \to \infty$ as $n \to \infty$ we have that μ_{v_n} converge in the weak* topology to μ_S.*
The same conclusion holds for $d = 4$ or 5 when $\{v_n\}$ is a sequence of primitive vectors with $\|v_n\| \to \infty$ as $n \to \infty$ and $\|v_n\|_2^2 \in \mathbb{D}(p)$ for any $n \in \mathbb{N}$, where p is a fixed odd prime number.

The proof of Theorem 3.2 is divided into three steps. In the first we prove some preliminaries on quadratic forms and recall a theorem by Gorodnik and Oh. In the second we will establish the analog of Theorem 3.2 for the measures $\overline{\mu}_{v,S}$. In the last step, we will deduce the desired statement for the measures $\mu_{v,S}$.

3.1. **Properties of the quadratic forms.** Let Q_0 denote the quadratic form $\sum_{i=1}^{d} x_i^2$. Fix a vector $v \in \mathbb{S}^{d-1}(D)$ and a rational matrix $\gamma \in \mathrm{SL_{d-1}}(\mathbb{Q})$. Fix a choice of g_v and consider the following quadratic map

$$\phi_v^{\gamma} : \mathbb{Q}^{d-1} \to \mathbb{Q},\ u \mapsto (Q_0 \circ g_v \circ \gamma)(u).$$

As before we identify $\mathbb{Q}^{d-1}$ with $\mathbb{Q}^{d-1} \times \{0\} \subset \mathbb{Q}^d$ so that $g_v(\gamma(u)) \in \mathbb{Q}^d$ is well-defined. We set $\phi_v \overset{\mathrm{def}}{=} \phi_v^e$. For a quadratic map ϕ let B_ϕ be the associated bilinear form

$$B_\phi(u_1, u_2) = \frac{1}{2}\left(\phi(u_1 + u_2) - \phi(u_1) - \phi(u_2)\right).$$

Finally, the determinant of ϕ with respect to $b_1, \cdots, b_{d-1}$ is $\det M_\phi$ where $M_\phi = (B_\phi(b_i, b_j))_{1\le i,j\le d-1}$. When $b_1, \cdots, b_{d-1}$ is a basis for $\mathbb{Z}^{d-1} \subset \mathbb{Q}^{d-1}$ and $\phi(b_i) \in \mathbb{Z}$ for all i, the determinant is a well-defined integer which does not depend of the choice of the basis. This is the case for ϕ_v with the standard basis and the choice of g_v merely changes the basis, so does not influence the value of the determinant.

Lemma 3.3. *For any $v \in \mathbb{S}^{d-1}(D)$ we have $\det(\phi_v) = D$. Moreover, there exist $u_1, u_2 \in \mathbb{Z}^{d-1}$ such that $B_{\phi_v}(u_1, u_2) = 1$.*

Proof. Using Equation (1.1) we see that the determinant of Q_0 with respect $v_1, \cdots, v_{d-1}, v$ is D^2. But M_{Q_0} with respect this basis, is a block matrix having a $d-1$-block whose determinant is $\det(\phi_v)$ and a 1-block whose value is $(v, v) = D$. Thus the first assertion follows.

Let $v_1, \cdots, v_{d-1}, w$ be a basis chosen as in the introduction. Since $d \ge 3$ we can assume without loss of generality that v_1 is in $v^\perp \cap w^\perp$. It is enough to show the second assertion while considering the map ϕ_v with this choice of a basis as the columns of the matrix g_v. As v_1 is primitive we can find $u \in \mathbb{Z}^d$ with $(u, v_1) = 1$. As $(w, v_1) = 0$ we can add to u multiples of w, so we can assume (as $v_1, \cdots, v_{d-1}, w$ is a basis for $\mathbb{Z}^d$) that $u = \sum_{i=1}^{d-1} a_i v_i, a_i \in \mathbb{Z}$. This implies that $\sum_{i=1}^{d-1} a_i(v_i, v_1) = 1$ showing $B_{\phi_v}(e_1, (a_1, \cdots, a_{d-1})) = 1$. $\square$

Define $\mathbb{H}_\phi = \mathrm{SO}(\phi) < \mathrm{SL}_{d-1}$ by $\{T \in \mathrm{SL}_{d-1} : \phi \circ T = \phi\}$. Recall that $\rho_{\mathrm{SL}_{d-1}} : \mathrm{ASL}_{d-1} \to \mathrm{SL}_{d-1}$ denotes the natural projection. Following the definitions, we have that

$$\mathbb{H}_{\phi_v^\gamma} = \gamma^{-1}\mathbb{H}_{\phi_v}\gamma = \gamma^{-1}\rho_{\mathrm{SL_{d-1}}}(g_v^{-1}\mathbb{H}_v g_v)\gamma. \tag{3.3}$$

Lemma 3.4. *Let $\phi, \phi' : \mathbb{Q}^{d-1} \to \mathbb{Q}$ be two quadratic maps and assume that $\mathbb{H}_\phi = \mathbb{H}_{\phi'}$ as $\mathbb{Q}$-algebraic subgroups of SL_{d-1}. Then there exists $r \in \mathbb{Q}^\times$ such that $\phi = r\phi'$.*

Proof. It is enough to prove this statement over $\mathbb{C}$. Thus, we can assume that M_ϕ is the identity matrix. We need to show that $M_{\phi'}$ is a scalar matrix. Fix $1 \le i < j \le d-1$ and let M_ϕ^{ij} be the 2 by 2 matrix whose entries are the ii, ij, ji, jj entries of M_ϕ and similarly for $M_{\phi'}^{ij}$. Acting on matrices with $A.M = A^t M A$, M_ϕ^{ij} is preserved by $\mathrm{SO}_2(\mathbb{C})$, and so is $M_{\phi'}^{ij}$ by our assumption. A direct calculation show that this implies that $M_{\phi'}^{ij} = \mathrm{diag}(r, r)$ for some $r \neq 0$. Applying this argument for all possible $i \neq j$ implies the claim. $\square$

Proposition 3.5. *If $\mathbb{H}_{\phi_v^{\gamma_v}} = \mathbb{H}_{\phi_u^{\gamma_u}}$ for some $v, u \in \mathbb{Z}^d_{prim}$ and some $\gamma_v, \gamma_u \in \mathrm{SL}_{d-1}(\mathbb{Z}^S)$, then $\frac{\|v\|^2}{\|u\|^2} \in (\mathbb{Z}^S)^\times$.*

Proof. By Lemma 3.4 $\phi_v^{\gamma_v} = r\phi_u^{\gamma_u}$ for some $r \in \mathbb{Q}$. Using the standard basis of $\mathbb{Z}^{d-1}$, it follows that $\gamma_v^t M_{\phi_v}\gamma_u = r \cdot \gamma_u^t M_{\phi_u}\gamma_u$. By Lemma 3.3 there exist $w_1, w_2 \in \mathbb{Z}^{d-1}$ with $w_1^t M_{\phi_u} w_2 = 1$. Since $\gamma_v, \gamma_u \in \mathrm{SL}_{d-1}(\mathbb{Z}^S)$ it follows that $r \in \mathbb{Z}^S$. Switching the roles of v and u we see that $r^{-1} \in \mathbb{Z}^S$ and so $r \in (\mathbb{Z}^S)^\times$. By Lemma 3.3, $\det M_{\phi_v} = \|v\|^2$ and similarly for u. Noting that $\det \gamma_v = \det \gamma_u = 1$, we get $\|v\|^2 = r^{d-1} \|u\|^2$ and the claim follows. □

Lemma 3.6. *If $\mathbb{P}$ is the orthogonal group of a definite quadratic form then $\mathbb{P}^+_{\{\infty\}} = \mathbb{P}(\mathbb{R})$.*

Proof. See [Pro07, §5.1]. □

Lemma 3.7. *Let $v \in \mathbb{S}^{d-1}(D)$ and recall that $p \neq 2$. Then the Lie algebra of $\mathbb{H}_v$ (resp. $\rho_{\mathrm{SL_{d-1}}}(g_v^{-1}\mathbb{H}_v g_v)$) is a maximal semisimple Lie sub-algebra of $\mathbb{G}_1$ (resp. $\overline{\mathbb{G}_2}$). If $d > 5$ these groups are $\mathbb{Q}_p$-isotropic and the same holds for $d = 4$ or 5 whenever $D \in \mathbb{D}(p)$.*

Proof. Maximality goes back to a classification made in 1952 by Dynkin [Dyn52] whose english translation may be found at [Dyn00]. As being isotropic is preserved by conjugation by g_v, it is enough to prove the second statement for $\mathbb{H}_v$. The group $\mathbb{H}_v$ is naturally the orthogonal group of the $d-1$ dimensional quadratic lattice $Q_v \overset{\text{def}}{=} (Q, \Lambda_v)$, so it is enough to show that Q_v is isotropic. This follows from [Kit99, Theorem 3.5.1] using the congruence condition $D \in \mathbb{D}(p)$ when $d = 4$ or 5. Indeed, for $d - 1 \geq 5$, Q_v is automatically isotropic over $\mathbb{Q}_p$. We have seen in Lemma 3.3 that Q_v has discriminant D. Denote the Hasse invariant of Q_v by $S(Q_v)$. Note that for $p \neq 2$ the congruence condition $p \nmid D$ implies that $S(Q_v) = 1$ (use [Kit99, Theorem 3.3.1(d)]). This, in turn, implies that Q_v is isotropic (use [Kit99, Theorem 3.5.1]). □

3.2. **Limits of algebraic measures.** Let $\mathbb{G} \subset \mathrm{SL}_k$ (for some integer k) be a connected semisimple $\mathbb{Q}$-group, S a finite set of valuations containing all the valuations for which $\mathbb{G}(\mathbb{Q}_v)$ is compact, $\mathbb{G}_S = \mathbb{G}(\mathbb{Q}_S)$ and Γ a finite-index subgroup of $\mathbb{G}(\mathbb{Z}^S) = \mathbb{G}(\mathbb{Q}_S) \cap \mathrm{SL}_k(\mathbb{Z}^S)$. Let $X_S \overset{\text{def}}{=} \mathbb{G}_S/\Gamma$ and let $\mathcal{P}(X_S)$ denote the space of probability measures on X_S.

Mozes and Shah showed in [MS95] that limits of algebraic probability measure are again algebraic if some unipotent flows act ergodically for each of the measures in the sequence. We are going to use the following analogue for S-arithmetic quotients obtained by Gorodnik and Oh, which we include here in a slightly simplified version.

Theorem 3.8 ([GO11, Theorem 4.6])**.** *Let $\mathbf{L}_i$ be a sequence of connected semisimple subgroups of $\mathbb{G}$ and assume that there exists $p \in S$ such that for any $\mathbf{L}_i$ and any $\mathbb{Q}_p$-normal subgroup $\mathbf{N} < \mathbf{L}_i$, $\mathbf{N}(\mathbb{Q}_p)$ is non-compact. Let g_i be a sequence of elements of $\mathbb{G}_S$ and set $\nu_i \overset{\text{def}}{=} \mu_{g_i \mathbf{L}^+_{i,S}\Gamma}$. If the centralizers of all $\mathbf{L}_i$ are $\mathbb{Q}$-anisotropic, then $\{\nu_1, \nu_2, \ldots\}$ is relatively compact in $\mathcal{P}(X_S)$. Assume that ν_i weakly converge to ν in $\mathcal{P}(X_S)$, then the following statements hold:*

1. *There exists a Zariski connected algebraic group $\mathbb{M}$ defined over $\mathbb{Q}$ such that $\nu = \mu_{gM\Gamma}$ where M is a closed finite-index subgroup of $\mathbb{M}_S$*

and $g \in \mathbb{G}_S$. If the centralizers of all $\mathbf{L}_i$ are $\mathbb{Q}$-anisotropic, then $\mathbb{M}$ is semi-simple.

(2) There exists a sequence $\gamma_i \subset \Gamma$ such that for all i sufficiently large we have $\gamma_i \mathbf{L}_i \gamma_i^{-1} \subset \mathbb{M}$.

(3) There exists a sequence $h_i \in \mathbf{L}_{i,S}^+$ such that $g_i h_i \gamma_i^{-1}$ converges to g as $i \to \infty$.

3.3. **Step I: Proof of Theorem 3.2 for orthogonal lattices.** Let $C = \{v_n : n \in \mathbb{N}\}$ and $S = \{\infty, p\}$. We apply Theorem 3.8 with $\mathbf{L}_n = \overline{\mathbb{L}}_{v_n}$ and $g_n = (k_{v_n}, e_p, \bar{\theta}_v, e_p) \in \overline{\mathbb{G}}_S$. By Lemma 3.7 and the congruence assumption in Theorem 3.2 when $d = 4$ or 5 the main assumption to Theorem 3.8 is satisfied.

Let ν be a weak* limit of $\left(\overline{\mu}_{v,S}\right)_{v\in C}$ which is the limit of a subsequence $\left(\overline{\mu}_{v,S}\right)_{v\in C_1}$ for $C_1 \subset C$. We wish to show that $\nu = \overline{\mu}_S$. By Lemma 3.7 the centralizer of $\mathbb{H}_v$ is finite hence $\mathbb{Q}$-anisotropic so ν is a probability measure by Theorem 3.8.

Applying Theorem 3.8.(1)–(2), we find a semisimple algebraic $\mathbb{Q}$-group $\mathbb{M} < \overline{\mathbb{G}}$ and $C_2 \subset C_1$ such that $|C_1 \setminus C_2| < \infty$ and for all $v \in C_2$ we have

$$\gamma_v \overline{\mathbb{L}}_v \gamma_v^{-1} < \mathbb{M} \tag{3.4}$$

for some $\gamma_v \in \overline{\mathbb{G}}(\mathbb{Z}^S)$.

Assume, for a moment, that $\mathbb{M} = \overline{\mathbb{G}}$. We will again use Theorem 3.8 to conclude the desired equidistribution. First we note that all the dynamics takes place in the orbit of $\overline{\mathbb{G}}_S^+$. Indeed, by Lemma 3.6 the element $g_n = (k_{v_n}, e, \bar{\theta}_v, e)$ belongs to $\overline{\mathbb{G}}_S^+$ for any $n \in \mathbb{N}$ and $\overline{\mathbb{L}}_{v_n,S}^+ \subset \overline{\mathbb{G}}_S^+$. Using Theorem 3.8.(1), we see that $\nu = \mu_{gM_0\overline{\mathbb{G}}(\mathbb{Z}^S)}$ for a subgroup M_0 of finite-index in $\overline{\mathbb{G}}_S$ and some $g \in \overline{\mathbb{G}}_S$. By [BT73, §6.7] $\mathbb{M}_S^+ = \overline{\mathbb{G}}_S^+$ is a minimal finite-index subgroup of $\overline{\mathbb{G}}_S$ and therefore contained in M_0. Since ν is supported inside $\overline{\mathbb{G}}_S^+\overline{\mathbb{G}}(\mathbb{Z}^S)$, it follows that $M_0 = \overline{\mathbb{G}}_S^+$ and that $\nu = \mu_{\overline{\mathbb{G}}_S^+\overline{\mathbb{G}}(\mathbb{Z})} = \overline{\mu}_{v,S}$. Therefore, the proof of this step will be concluded once we show:

Claim. $\mathbb{M} = \overline{\mathbb{G}}$.

Proof of the Claim . Let $\pi_1 : \mathbb{G}_1 \times \overline{\mathbb{G}_2} \to \mathbb{G}_1$ and $\pi_2 : \mathbb{G}_1 \times \overline{\mathbb{G}_2} \to \overline{\mathbb{G}_2}$ denote the natural projection and define $\mathbb{M}_i \overset{\text{def}}{=} \pi_i(\mathbb{M})$. Since $\mathbb{M}$ is semisimple and $\mathbb{G}_1$ and $\overline{\mathbb{G}_2}$ have non-isomorphic simple Lie factors, it is enough to show that $\mathbb{M}_1 = \mathbb{G}_1$ and $\mathbb{M}_2 = \overline{\mathbb{G}}_2$.

Case I: $\left(\|v\|^2\right)_{v\in C_2}$ is not eventually supported on a geometric progression of the form $\left(D_0 p^k\right)_{k\in\mathbb{N}}$. We begin with $\mathbb{M}_1$: we know that $\mathbb{M}_1$ contains subgroups of the form $\gamma_v^{-1}\mathbb{H}_v\gamma_v$ for any $v \in C_2$ where $\gamma_v \in \mathbb{G}_1(\mathbb{Z}^S)$. By Lemma 3.7, each $\gamma_v^{-1}\mathbb{H}_v\gamma_v$ is a maximal semisimple subgroup. Thus, if $\mathbb{M}_1 \neq \mathbb{G}_1$ then for all $v, u \in C_2$ we have $\gamma_v^{-1}\mathbb{H}_v\gamma_v = \gamma_u^{-1}\mathbb{H}_u\gamma_u$, which says that $\mathbb{H}_{\gamma_v^{-1}v} = \mathbb{H}_{\gamma_u^{-1}u}$. This in turn implies $\gamma_v^{-1}v = \alpha\gamma_u^{-1}u$ for some $\alpha \neq 0$. As v, u are primitive vectors in $\mathbb{Z}^d$, $\gamma_v^{-1}v, \gamma_v^{-1}u$ are primitive vectors in $(\mathbb{Z}^S)^d = \mathbb{Z}[\frac{1}{p}]^d$

(considered as a $\mathbb{Z}^S$-module). Thus $\alpha \in (\mathbb{Z}^S)^\times = \{\pm p^n : n \in \mathbb{Z}\}$. Noting that for all $v \in C_2$ we have $\left\|\gamma_v^{-1} v\right\|^2 = \|v\|^2$, we obtain a contradiction under the assumption of Case I.

Assume now that $\mathbb{M}_2 \neq \overline{\mathbb{G}}_2$. It follows from (3.4) and from (3.3) that $\mathbb{M}_2$ contains subgroups of the form $\mathbb{H}_{\phi_v^{\gamma_v}}$ for all $v \in C_2$ where $\gamma_v \in \overline{\mathbb{G}}_2(\mathbb{Z}^S)$. By Lemma 3.7 $\mathbb{H}_{\phi_v^\gamma}$ is always maximal, so we have that $\mathbb{H}_{\phi_u^{\gamma_u}} = \mathbb{H}_{\phi_v^{\gamma_v}}$ for all $v, u \in C_2$. It follows from Proposition 3.5, that the assumption of Case I is not satisfied. This concludes the proof of Case I.

Note that this is the only relevant case when $d = 4$ or 5 (as in that case we assume that $p \nmid \|v\|^2$ for all $v \in C$).

Case II: $\left(\|v\|^2\right)_{v \in C_2}$ *is eventually supported on a geometric progression of the form* $\left(D_0 p^k\right)_{k \in \mathbb{N}}$. Consider $R_{p,q} \overset{\text{def}}{=} \left(\overline{\mu}_{v,\{\infty,p,q\}}\right)_{v \in C_2}$ and $R_q \overset{\text{def}}{=} \left(\overline{\mu}_{v,\{\infty,q\}}\right)_{v \in C_2}$ for some odd prime $q \neq p$. For R_q we are again in Case I, so by the above, R_q converges to $\overline{\mu}_{\{\infty,q\}}$. We consider the space $\mathcal{X}^{\{\infty,p,q\}}$ with the natural projections

$$\begin{array}{ccc} & \mathcal{X}^{\{\infty,p,q\}} & \\ \swarrow & & \searrow \\ \mathcal{X}^{\{\infty,p\}} & & \mathcal{X}^{\{\infty,q\}} \end{array}$$

and apply Theorem 3.8 to $R_{p,q}$. For any converging subsequence $R'_{p,q} \subset R_{p,q}$ we obtain a subgroup $\mathbb{M}(R'_{p,q}) < \overline{\mathbb{G}}$. As the push-forward of $R'_{p,q}$ under the natural projection $\mathcal{X}^{\{\infty,p,q\}} \to \mathcal{X}^{\{\infty,q\}}$ equidistribute to $\overline{\mu}_{\{\infty,q\}}$ we have that $\mathbb{M}(R'_{p,q}) = \overline{\mathbb{G}}$. As above, this implies that $R_{p,q}$ converges to $\overline{\mu}_{\{\infty,p,q\}}$ and in turn, that $\left(\overline{\mu}_{v,\{\infty,p\}}\right)_{v \in C_2}$ equidistribute to $\overline{\mu}_{\{\infty,p\}}$ (and in particular that $\mathbb{M} = \overline{\mathbb{G}}$) as we needed to show. □

3.4. **Upgrading from orthogonal lattices to orthogonal grids.** Let ν be a weak* limit of $(\mu_{v,S})_{v \in C}$ which is the limit of a subsequence $(\mu_{v,S})_{v \in C_1}$ for $C_1 \subset C$. We need to show that $\nu = \mu_S$. First notice that $\pi^S : \mathcal{Y}^S \to \mathcal{X}^S$ has compact fibers, which together with Remark 3.1 and § 3.3 gives that $\pi^S_* \nu = \overline{\mu}_S$. In particular, ν is also a probability measure.

We will use the same type of argument as in §3.3: assuming that $\nu \neq \mu_S$ we will use the algebraic information furnished by Theorem 3.8 to deduce a contradiction to the fact that the primitive vectors in C_1 have their length going to infinity. As before, we may assume that $\left(\|v\|^2\right)_{v \in C_1}$ are not eventually varying along a geometric progression of the type $(D_0 p^n)_{n \in \mathbb{N}}$. In fact, if this is not the case, a similar argument as in Case II above can be applied, and we will not repeat it.

More precisely, we will apply Theorem 3.8 within the quotient

$$(\mathbb{G}_1 \times \mathrm{SL}_d)_S \,/\, (\mathbb{G}_1 \times \mathrm{SL}_d)\,(\mathbb{Z}^S).$$

To simplify the notation we set $\mathbb{G}' = \mathbb{G}_1 \times \mathrm{SL}_d$ and recall that

$$\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2 = \mathrm{SO}_d \times \mathrm{ASL}_{d-1} < \mathbb{G}'.$$

We note that the orbit $\mathbb{G}_S\mathbb{G}'(\mathbb{Z}^S)$ is isomorphic to (and will be identified with) $\mathcal{Y}_S = \mathbb{G}_S/\mathbb{G}(\mathbb{Z}^S)$. Recall that this implies that the finite volume orbit $\mathbb{G}_S\mathbb{G}'(\mathbb{Z}^S)$ is a closed subset of $\mathbb{G}'_S/\mathbb{G}'(\mathbb{Z}^S)$, equivalently a closed subset of $\mathbb{G}'_S$ or even of the homogeneous space $W = \mathbb{G}_S\backslash\mathbb{G}'_S$.

From Theorem 3.8.(1)–(2) we find an algebraic $\mathbb{Q}$-subgroup $\mathbb{M} < \mathbb{G}'$ and $C_2 \subset C_1$ such that $|C_1 \setminus C_2| < \infty$ and for all $v \in C_2$

$$\gamma_v \mathbb{L}_v \gamma_v^{-1} < \mathbb{M} \tag{3.5}$$

for some $\gamma_v \in \mathbb{G}_1 \times \mathrm{SL}_d(\mathbb{Z}^S)$. Moreover, $\nu = \mu_{gM_0\mathbb{G}_1\times\mathrm{SL}_d(\mathbb{Z}^S)}$ for some finite-index subgroup $M_0 < \mathbb{M}_S$ and $g \in \mathbb{G}'_S$. By construction all orbits in our sequence are contained in $\mathbb{G}_S\mathbb{G}'(\mathbb{Z}^S)$, which implies that the support of ν is also contained in this set and in particular that $g\mathbb{G}'(\mathbb{Z}^S) \in \mathbb{G}_S\mathbb{G}'(\mathbb{Z}^S)$. This implies that we may change $\mathbb{M}$ by a conjugate $\gamma\mathbb{M}\gamma^{-1}$ for some $\gamma \in \mathbb{G}'(\mathbb{Z}^S)$ and assume that $g \in \mathbb{G}_S$.

If $m \in M_0$, we obtain that the element $gm\mathbb{G}'(\mathbb{Z}^S)$ belongs to the support of ν. Therefore, $\mathbb{G}_S m \in W$ belongs to the closed (and discrete) set $\mathbb{G}_S\mathbb{G}'(\mathbb{Z}^S)$. If $m \in \mathbb{M}_S$ is sufficiently close to the identity this implies $m \in \mathbb{G}_S$. As $\mathbb{M}$ is Zariski connected we conclude that $\mathbb{M} < \mathbb{G}$. Using the same argument it also follows from Theorem 3.8.(3) that $(\gamma_v)_{v\in C_3} \subset \mathbb{G}$ for some subset $C_3 \subset C_2$ with $|C_2 \setminus C_3| < \infty$.

By the previous step we know that $\pi^S_*\nu = \overline{\mu}_S$, which implies that either $\mathbb{M} = \mathbb{G}$ or $\mathbb{M} = \mathbb{G}_1 \times \mathbb{M}_2$ where $\mathbb{M}_2$ is a $\mathbb{Q}$-subgroup which is $\mathbb{Q}$-isomorphic to a fixed copy of SL_{d-1}. Such subgroups are of the form $\mathrm{SL}^{\mathrm{q}}_{\mathrm{d-1}}$ where $\mathrm{SL}^{\mathrm{q}}_{\mathrm{d-1}}$ is the conjugation of $\iota(\mathrm{SL}_{d-1}) = \begin{pmatrix} \mathrm{SL}_{d-1} & 0 \\ 0 & 1 \end{pmatrix}$ by $c_q = \begin{pmatrix} I_{d-1} & q \\ 0 & 1 \end{pmatrix}$ for some fixed $q \in \mathbb{Q}^{d-1}$. As above, we will be done once we show that $\mathbb{M} = \mathbb{G}$. Assume therefore that we are in the second case and $\mathbb{M}_2 = \mathrm{SL}^{\mathrm{q}}_{\mathrm{d-1}}$. Using the definition of $\mathbb{L}_v$ in (3.1) and projecting (3.5) using the canonical map $\mathbb{G} \to \mathbb{G}_2$, we get that for all $v \in C_3$ that

$$c_q^{-1}\gamma_{v,2}^{-1}g_v^{-1}\mathbb{H}_v g_v \gamma_{v,2} c_q \subset \iota(\mathrm{SL}_{d-1}),$$

where $\gamma_{v,2}$ genotes the projection of γ_v to $\mathbb{G}_2$. Let $N \in \mathbb{N}$ be such that $Nq \in \mathbb{Z}^{d-1}$ and set $u \overset{\mathrm{def}}{=} g_v\gamma_v c_q(Ne_d)$. Note that Ne_d is a simultaneous eigenvector of the right hand side. It follows that for each $v \in C_3$, we have that $u \in (\mathbb{Z}^S)^d$ and that u is a simultaneous eigenvector for $\mathbb{H}_v$. Therefore $u = \alpha_v v$ for some $\alpha_v \in \mathbb{Z}^S \setminus \{0\}$. Using that $\gamma_v \in \mathbb{G}_2$, and the definition of g_v, we see that $u = Nw + \sum_{i=1}^{d-1} a_i v_i$ with $a_i \in \mathbb{Z}^S$. Recall that $(w, v) = 1$.

Taking the inner product of u with v we get

$$\alpha_v \|v\|^2 = (u,v) = (Nw,v) = N$$

for all $v \in C_3$. This gives a contradiction under the assumption that $\left(\|v\|^2\right)_{v\in C_1}$ is not eventually varying along a geometric progression of the type $(D_0 p^n)_{n\in\mathbb{N}}$.

4. An equivalence relation

Let $G_i = \mathbb{G}_i(\mathbb{R}), \Gamma_i = \mathbb{G}_i(\mathbb{Z})$ for $i = 1, 2$, $K = \mathbb{H}_{e_d}(\mathbb{R})$ and fix $v \in \mathbb{S}^{d-1}(D)$ throughout this section. We identify $K \setminus G_1 \cong \mathbb{S}^{d-1}$ via the action of G_1 on $\mathbb{S}^{d-1}$ defined by $w \mapsto k^{-1}w$ using the initial point e_d. We will also write $w.k = k^{-1}w$ for this right action of $k \in G_1$ on $w \in \mathbb{S}^{d-1}(\mathbb{R})$. Recall that this action is transitive with $K \overset{\text{def}}{=} \mathrm{SO_{d-1}}(\mathbb{R}) = \mathrm{Stab}_G(e_d)$. As in the introduction, the group K can also be embedded into G_2. We denote the diagonal embedding of K by $\Theta_K \overset{\text{def}}{=} \{(k,k) : k \in K\} \subset G_1 \times G_2$.

Let $\mathbf{S}^{d-1} = \mathbb{S}^{d-1}/\Gamma_1$ and $\mathbf{S}^{d-1}(D) = \mathbb{S}^{d-1}(D)/\Gamma_1$. Set $\mathbf{v} = v.\Gamma_1$ and $[\Delta_{\mathbf{v}}] = [\Delta_v]$. The latter is well-defined as $[\Delta_{\gamma v}] = [\Delta_v]$ for all $\gamma \in \Gamma_1$. Note also that the projection $\mathbf{v} \in \mathbf{S}^{d-1}(D) \mapsto \frac{\mathbf{v}}{\|\mathbf{v}\|} \in \mathbf{S}^{d-1}$ is well-defined. It follows that the following double coset

$$K \times K\,(k_v, \theta_v)\,\Gamma_1 \times \Gamma_2 \tag{4.1}$$

represents the pair

$$\left(\frac{\mathbf{v}}{\|\mathbf{v}\|}, [\Delta_{\mathbf{v}}]\right) \in \mathbf{S}^{d-1} \times \mathcal{Y}_{d-1}.$$

Note that all the measures appearing in equation (1.2) are Γ_1-invariant so if we consider their projection ν_D of $\tilde{\nu}_D$ to $\mathbf{S}^{d-1} \times \mathcal{Y}_{d-1}$ we have that the convergence (1.2) is equivalent to

$$\nu_D \overset{\text{weak}^*}{\longrightarrow} m_{\mathbf{S}^{d-1}} \otimes m_{\mathcal{Y}_{d-1}} \text{ as } D \to \infty \text{ with } D \in A \tag{4.2}$$

4.1. **Definition of P_v and the measure ν_v.** From now on we will use only one odd prime p so we fix $S = \{\infty, p\}$ and then $\mathbb{Q}_S = \mathbb{R} \times \mathbb{Q}_p$ and $\mathbb{Z}^S = \mathbb{Z}[\frac{1}{p}]$. Fix $v \in \mathbb{S}^{d-1}(D)$. We say $w \sim v$ for $w \in \mathbb{Z}^d$ if there exist $g_p \in \mathbb{G}_1(\mathbb{Z}_p)$ and $\gamma_p \in \mathbb{G}_1(\mathbb{Z}[\frac{1}{p}])$ such that $g_p w = v, \gamma_p w = v$ and $g_p \gamma_p^{-1} \in \mathbb{H}^+_{v,\{p\}}$.

Lemma 4.1. *The relation $\sim$ is an equivalence relation.*

Proof. The key fact we will use is that for any $v \in \mathbb{Z}^d_{\mathrm{prim}}$, $\mathbb{H}^+_{v,\{p\}}$ is a minimal finite index subgroup of $\mathbb{H}_{v,\{p\}}$ (see [BT73, §6.7]). Reflexivity is immediate. For symmetry, assume $w \sim v$ with g_p, γ_p as above. Taking the inverse we have $\gamma_p g_p^{-1} \in \mathbb{H}^+_{v,\{p\}}$. It follows from $g_p^{-1}\mathbb{H}_v g_p = \mathbb{H}_w$ and the key fact above that $g_p^{-1}\mathbb{H}^+_{v,\{p\}} g_p = \mathbb{H}^+_{w,\{p\}}$ showing that $g_p^{-1}\gamma_p \in \mathbb{H}^+_{w,\{p\}}$ establishing symmetry. For transitivity, let $v \in \mathbb{S}^{d-1}(D)$ be given and let w_1, w_2 be two vectors satisfying $v \sim w_i$. We will show that $w_2 \sim w_1$. Let $\gamma_i \in \mathbb{G}_1(\mathbb{Z}[\frac{1}{p}]), g_i \in$

$\mathbb{G}_1(\mathbb{Z}_p)$, be the elements arising from the definition of $v \sim w_i$. Then, $w_2 = \gamma_1^{-1}\gamma_2 w_1 = g_1^{-1} g_2 w_1$. Transitivity follows as

$$g_2^{-1} g_1 (\gamma_2^{-1}\gamma_1)^{-1} = g_2^{-1}\left(g_1\gamma_1^{-1}\gamma_2 g_2^{-1}\right) g_2 \in g_2^{-1}\mathbb{H}^+_{v,\{p\}} g_2 = \mathbb{H}^+_{w_2,\{p\}}$$

where the latter equality again follows from the key fact. □

The equivalence relation $\sim$ satisfies that if $w \sim v$ and $\gamma \in \Gamma_1$ then $\gamma w \sim \gamma v$, and so it descends to an equivalence relation on $\mathbf{S}^{d-1}(D)$. We set $P_v \overset{\text{def}}{=} \{\mathbf{w} : \mathbf{w} \sim \mathbf{v}\}$ and $R_v = \left\{\left(\frac{\mathbf{w}}{\|\mathbf{w}\|}, [\Delta_{\mathbf{w}}]\right) : \mathbf{w} \in P_v\right\}$. We finally define $\nu_v = \nu_D|_{R_v}$. In the next section we will relate ν_v to the measure $\mu_{v,S}$.

5. Deducing Theorem 1.2 from Theorem 3.2.

5.1. **Restriction to the principal genus.** Consider the open orbit $\mathcal{U}' \overset{\text{def}}{=} \mathbb{G}(\mathbb{R}\times\mathbb{Z}_p)\mathbb{G}(\mathbb{Z}[\frac{1}{p}]) \subset \mathcal{Y}_S$. The set $\mathcal{U}'$ is also closed by [PR94, Theorem 5.1]. By [PR94, §8.2] $\mathbb{G}_S^+ < \mathbb{G}_S$ is a clopen finite-index subgroup. Finally, we consider the clopen set $\mathcal{U} = \mathcal{U}' \cap \left(\mathbb{G}_S^+\mathbb{G}(\mathbb{Z}[\frac{1}{p}])\right)$. Thus, with v_n as in Theorem 3.2, we have that

$$\eta_{v_n} \overset{\text{def}}{=} \mu_{v_n,S}|_{\mathcal{U}} \overset{\text{weak}^*}{\longrightarrow} \eta \overset{\text{def}}{=} \mu|_{\mathcal{U}} \text{ as } n\to\infty \tag{5.1}$$

We have a projection map π from $\mathcal{U}'$, considered as a subset of $\mathcal{Y}^S$, to $\mathcal{Y}^\infty = \mathbb{G}(\mathbb{R})/\mathbb{G}(\mathbb{Z})$ obtained by dividing from the left by $\{e\}\times\mathbb{G}(\mathbb{Z}_p)$. Noting that $G^+_{\{\infty\}} = \mathbb{G}(\mathbb{R})$ (this follows from Lemma 3.6 and the fact that SL_{d-1} is simply-connected), it follows that $\pi_*(\eta)$ is a probability measure which is invariant under $\mathbb{G}(\mathbb{R})$, that is, it is the uniform probability measure on $\mathbb{G}(\mathbb{R})/\mathbb{G}(\mathbb{Z})$. Therefore, under the assumptions of Theorem 3.2 we have

$$\pi_*(\eta_{v_n}) \overset{\text{weak}^*}{\longrightarrow} m_{\mathbb{G}(\mathbb{R})/\mathbb{G}(\mathbb{Z})}. \tag{5.2}$$

In addition, we have the projection map:

$$\rho : G_1\times G_2/\Gamma_1\times\Gamma_2 \to K\times K\setminus G_1\times G_2/\Gamma_1\times\Gamma_2 \tag{5.3}$$

Below we will show that the measures $(\rho\circ\pi)_*\eta_v$ and ν_{Q_v} are closely related.

5.2. **Description of η_v as union of orbits.** Fix $v \in \mathbb{S}^{d-1}(D)$ and note that $\mathbb{H}_v(\mathbb{Z}_p) = \mathbb{H}_v(\mathbb{Q}_p)\cap\mathbb{G}_1(\mathbb{Z}_p)$. Let $\pi_1 : \mathcal{Y}^S \to \mathcal{Y}_1^S \overset{\text{def}}{=} \mathbb{G}_{1,S}/\mathbb{G}_1(\mathbb{Z}^S)$ be the natural projection. For $h \in \mathbb{H}^+_{v,\{p\}}$ the double coset $\mathbb{H}_v(\mathbb{Z}_p)h\mathbb{H}_v(\mathbb{Z}[\frac{1}{p}])$ is either contained in $\pi_1(\mathcal{U})$, in which case we set $s(h) = 0$, or it is disjoint from $\pi_1(\mathcal{U})$, in which case we set $s(h) = \text{other}$. We will not need this, but wish to note that the symbol 0 corresponds here to our quadratic form $Q_0(x_1,\ldots,x_d) = x_1^2+\cdots+x_d^2$ and 'other' for the other quadratic forms in the spin genus of Q_0. For $s\in\{0,\text{other}\}$ choose a set M_s satisfying the following equality (as subsets of $\mathbb{H}_v(\mathbb{Q}_p)$):

$$\bigcup_{h\in\mathbb{H}^+_{v,\{p\}},\, s(h)=s} \mathbb{H}_v(\mathbb{Z}_p)h\mathbb{H}_v(\mathbb{Z}[\tfrac{1}{p}]) = \bigsqcup_{h\in M_s} \mathbb{H}_v(\mathbb{Z}_p)h\mathbb{H}_v(\mathbb{Z}[\tfrac{1}{p}])$$

where the later denotes a disjoint union. The sets $M_0, M_{\mathrm{other}}, M_{\mathrm{full}} \overset{\mathrm{def}}{=} M_0 \cup M_{\mathrm{other}}$ are finite by [PR94, Theorem 5.1]. Using that $\mathbb{H}^+_{v,\{p\}} \subset \mathbb{G}^+_{1,\{p\}}$ and the definition of $\mathcal{U}$ we have

$$\left\{h \in \mathbb{H}^+_{v,\{p\}} : s(h) = 0\right\} = \mathbb{H}^+_{v,\{p\}} \cap \mathbb{G}_1(\mathbb{Z}_p)\mathbb{G}_1(\mathbb{Z}[\tfrac{1}{p}]).$$

By Lemma 3.6, $\mathbb{L}^+_{v,\{\infty\}} = \mathbb{L}_v(\mathbb{R})$. Recall $\theta_v = a_v k_v g_v$ and note that $(k_v, \theta_v)\,\mathbb{L}_v(\mathbb{R}) = \Theta_K\,(k_v, \theta_v)$. Using this we can express the orbit $\mathbf{O}_{v,S}$ from (3.2) in a different form: set $l(h) = g_v^{-1} h g_v$ and let us allow to re-order entries of products as needed so that

$$\Theta_K \times \mathbb{L}^+_{v,\{p\}} = \left\{(k, h, k, l(h)) : k \in K, h \in \mathbb{H}^+_{v,\{p\}}\right\} \subset \mathbb{G}_S. \tag{5.4}$$

In this notation we get

$$\mathbf{O}_{v,S} = \Theta_K \times \mathbb{L}^+_{v,\{p\}}(k_v, e_p, \theta_v, e_p)\mathbb{G}(\mathbb{Z}[\tfrac{1}{p}]).$$

We also set $\mathbb{L}^+(\mathbb{Z}_p) = \mathbb{L}^+_{v,\{p\}} \cap \mathbb{G}(\mathbb{Z}_p)$ and obtain

$$\mathbf{O}_v = \bigsqcup_{h \in M_{\mathrm{full}}} \Theta_K \times \mathbb{L}^+(\mathbb{Z}_p)(k_v, h, \theta_v, l(h))\mathbb{G}(\mathbb{Z}[\tfrac{1}{p}]),$$

where we used the same identification as in (5.4). Thus, the restricted measure η_v (see (5.1)) is a $\Theta_K \times \mathbb{L}^+(\mathbb{Z}_p)$-invariant probability measure on

$$\mathbf{O}_v \cap \mathcal{U} = \bigsqcup_{h \in M_0} \Theta_K \times \mathbb{L}^+(\mathbb{Z}_p)(k_v, h, \theta_v, l(h))\mathbb{G}(\mathbb{Z}[\tfrac{1}{p}]). \tag{5.5}$$

We note that the last equality could also have been used as the definition of the finite set $M_0 \subset \mathbb{H}^+_{v,\{p\}}$ of representatives.

5.3. **The support of the measure $\pi_*(\eta_v)$.** By definition each $h \in M_0$ belongs to $\mathbb{G}_1(\mathbb{Z}_p)\mathbb{G}_1(\mathbb{Z}[\frac{1}{p}])$. So we can write $h = c_1(h)\gamma_1(h)^{-1}$ where $c_1(h) \in \mathbb{G}_1(\mathbb{Z}_p)$ and $\gamma_1(h) \in \mathbb{G}_1(\mathbb{Z}[\frac{1}{p}])$. Using the fact that $\mathbb{G}_2$ has class number 1, we can write $l(h) = c_2(h)\gamma_2(h)^{-1}$ where $c_2(h) \in \mathbb{G}_2(\mathbb{Z}_p)$ and $\gamma_2(h) \in \mathbb{G}_2(\mathbb{Z}[\frac{1}{p}])$.

Proposition 5.1. *The measure $\pi_*(\eta_v)$ is a Θ_K-invariant probability measure on*

$$\bigsqcup_{h \in M_0} \mathcal{O}_h \overset{\mathrm{def}}{=} \bigsqcup_{h \in M_0} \Theta_K(k_v\gamma_1(h), a_v k_v g_v \gamma_2(h))\Gamma. \tag{5.6}$$

Proof. The proposition follows immediately by plugging the decompositions $h = c_1(h)\gamma_1(h)^{-1}$ and $l(h) = c_2(h)\gamma_2(h)^{-1}$ into (5.5) while recalling two facts. The first is that the map π is dividing by $\{e\} \times \mathbb{G}(\mathbb{Z}_p)$ from the left. The second fact is that $(\gamma_1(h), \gamma_1(h), \gamma_2(h), \gamma_2(h)) \in \mathbb{G}(\mathbb{Z}[\frac{1}{p}])$. $\square$

Let us note that $\Theta_K(k_v\gamma_1(h), a_v k_v g_v \gamma_2(h))\Gamma$ does not depend on the choice of the representative of the double coset $\mathbb{H}^+_{v,\{p\}}(\mathbb{Z}_p)h\mathbb{H}(\mathbb{Z}[\frac{1}{p}])$ and also not on the choice of the above decompositions. In fact, let us first assume that $h = c_1\gamma_1^{-1} = c_1'(\gamma_1')^{-1}$ are two decompositions as above. This gives that

$c_1^{-1}c_1' = \gamma_1^{-1}\gamma_1'$ belongs to $\mathbb{G}_1(\mathbb{Z}_p) \cap \mathbb{G}_1(\mathbb{Z}[\frac{1}{p}]) = \mathbb{G}_1(\mathbb{Z}) = \Gamma_1$, which implies the first half of the claimed independence in the $\mathbb{G}_1$-factor. If now $h = c_1\gamma_1^{-1}$ as above, $g_p \in \mathbb{H}_v(\mathbb{Z}_p)$, and $\beta \in \mathbb{H}_v(\mathbb{Z}[\frac{1}{p}])$, then $g_p h\beta = (g_p c_1)(\gamma_1^{-1}\beta)$ and we associate to this point the double coset $Kk_v\beta^{-1}\gamma_1\Gamma_1$. Using $k_v\beta^{-1}k_v^{-1} \in K$ the latter equals $Kk_v\gamma_1\Gamma_1$, which is the claimed independence for the components in $\mathbb{G}_1$. The proof for the component in $\mathbb{G}_2$ is similar.

We will now relate the set appearing in the above proposition with the set P_v introduced in §4.1.

Proposition 5.2. *For $h \in M_0$ set $\varphi(h) = Kk_v\gamma_1(h)\Gamma_1$. Then φ is a bijection from M_0 to $\{Kk_u\Gamma_1 : \mathbf{u} \in P_v\}$. Noting that $\varphi(h)$ corresponds to $u = \gamma_1(h)^{-1}v$ we further claim that $Ka_vk_vg_v\gamma_2(h)\Gamma_2 = [\Delta_{\mathbf{u}}]$.*

Proof. Fix $h \in M_0$ and recall that h stabilizes v. We first need to show that $u = \gamma_1(h)^{-1}v \in \mathbb{Z}^{d-1}$: indeed, we have

$$\mathbb{Z}[\tfrac{1}{p}]^d \ni \gamma_1(h)^{-1}v = c_1(h)^{-1}hv = c_1(h)^{-1}v \in \mathbb{Z}_p^d$$

so $u \in \mathbb{Z}^d$ as $\mathbb{Z}[\frac{1}{p}] \cap \mathbb{Z}_p = \mathbb{Z}$. Now, the elements $c_1(h), \gamma_1(h)$ satisfy

$$c_1(h)u = c_1(h)\gamma_1(h)^{-1}v = hv = v \text{ and } \gamma_1(h)u = v.$$

As $c_1(h)\gamma_1(h)^{-1} = h \in \mathbb{H}^+_{v,\{p\}}$ this shows that $u \sim v$ and therefore $Kk_v\gamma_1(h)\Gamma_1$ belongs to $\{Kk_u\Gamma_1 : \mathbf{u} \in P_v\}$.

To see that φ is onto, fix $u \sim v$ and let $h_u = g_p\gamma_p^{-1} \in \mathbb{H}^+_{v,\{p\}}$ arising from the definition of $\sim$ in §4.1. Then $\gamma_p u = v$ and $s(h_u) = 0$. Let $\bar{h} \in M_0$ be such that $\mathbb{H}_v(\mathbb{Z}_p)h_u\mathbb{H}_v(\mathbb{Z}[\frac{1}{p}]) = \mathbb{H}_v(\mathbb{Z}_p)\bar{h}\mathbb{H}_v(\mathbb{Z}[\frac{1}{p}])$. We have explained above that $Kk_u\Gamma_1 = Kk_v\gamma_p\Gamma_1 = Kk_v\gamma_1(\bar{h})\Gamma_1$.

For injectivity, let $h_1, h_2 \in M_0$ and set $\alpha_i = \gamma_1(h_i), k_i = c_1(h_i)$, $i = 1, 2$. Assuming $\varphi(h_1) = \varphi(h_2)$, there exist a $\gamma \in \Gamma_1$ such that $Kk_v\alpha_1\gamma = Kk_v\alpha_2$. Thus $\alpha_1\gamma\alpha_2^{-1}$ stabilize v so $\alpha_1\gamma\alpha_2^{-1} \in \mathbb{H}_v(\mathbb{R}) \cap \mathbb{G}(\mathbb{Z}[\frac{1}{p}]) = \mathbb{H}_v(\mathbb{Z}[\frac{1}{p}])$. Also $(k_2\gamma^{-1}k_1^{-1})v = (h_2\alpha_2\gamma^{-1}\alpha_1^{-1}h_1^{-1})v = v$ so $k_2\gamma^{-1}k_1^{-1} \in \mathbb{H}_v(\mathbb{Q}_p) \cap \mathbb{G}(\mathbb{Z}_p) = \mathbb{H}_v(\mathbb{Z}_p)$. As $(k_2\gamma^{-1}k_1^{-1})h_1(\alpha_1\gamma\alpha_2^{-1}) = h_2$ we see that

$$\mathbb{H}_v(\mathbb{Z}_p)h_1\mathbb{H}_v(\mathbb{Z}[\tfrac{1}{p}]) = \mathbb{H}_v(\mathbb{Z}_p)h_2\mathbb{H}_v(\mathbb{Z}[\tfrac{1}{p}]).$$

For the second assertion, fix $h \in M_0$ and let $u = \gamma_1(h)^{-1}v$. We will use the abbreviations $\gamma_i = \gamma_i(h), c_i = c_i(h)$ for $i = 1, 2$ which satisfy by definition that $h = c_1\gamma_1^{-1}$ and $l(h) = g_v^{-1}hg_v = c_2\gamma_2^{-1}$. We need to show that

$$Ka_vk_vg_v\gamma_2\Gamma_2 \overset{?}{=} [\Delta_u] = Ka_uk_ug_u\Gamma_2. \tag{5.7}$$

Note first that $a_v = a_u$ and that $k_v\gamma_1$ is a legitimate choice of k_u. With these choices (and using the identity of K on both sides), (5.7) will follow once we show $g_u^{-1}\gamma_1^{-1}g_v\gamma_2 \in \Gamma_2$. The element $g_u^{-1}\gamma_1^{-1}g_v\gamma_2$ is certainly a determinant 1 element which map $\mathbb{R}^{d-1}$ to itself. Furthermore, the last entry of its last column is positive by the orientation requirement in the definition of g_v and

g_u. Therefore, it will be enough to show that this element maps $\mathbb{Z}^d$ to itself. We use again that $\mathbb{Z}[\frac{1}{p}] \cap \mathbb{Z}_p = \mathbb{Z}$ to obtain

$$\mathbb{Z}[\tfrac{1}{p}]^d \supset g_u^{-1}\gamma_1^{-1}g_v\gamma_2\mathbb{Z}^d = g_u^{-1}c_1^{-1}\left(c_1\gamma_1^{-1}\right)g_v\left(\gamma_2 c_2^{-1}\right)c_2\mathbb{Z}^d = \\ = g_u^{-1}c_1^{-1}hg_vg_v^{-1}h^{-1}g_vc_2\mathbb{Z}^d = g_u^{-1}c_1^{-1}g_vc_2\mathbb{Z}^d \subset \mathbb{Z}_p^d.$$

□

5.4. **Weights of $(\rho\circ\pi)_*\eta_v$ and ν_v.** Fix a sequence (v_n) of vectors satisfying the conditions of Theorem 3.2 and set $\mu_n \overset{\text{def}}{=} (\rho\circ\pi)_*\eta_{v_n}$ (with π as in (5.2) and ρ as in (5.3)) and $\nu_n \overset{\text{def}}{=} \nu_{v_n}$. It follows from Propositions 5.1–5.2 that $R_{v_n} = \mathrm{Supp}(\nu_\mathrm{n}) = \mathrm{Supp}(\mu_\mathrm{n})$. Let λ_n denote the normalised counting measure on R_{v_n}. In this section we show

$$\mu_n - \lambda_n \overset{n\to\infty}{\longrightarrow} 0 \text{ and } \nu_n - \lambda_n \overset{n\to\infty}{\longrightarrow} 0, \tag{5.8}$$

That is, the measures μ_n and ν_n are equal to λ_n up-to a negligible error. For $\mathbf{u}\in\mathbf{S}^{d-1}$ let $S(\mathbf{u}) = |\mathrm{Stab}_{\Gamma_1}(u)|$ for some $u\in\mathbf{u}$ and $E = \tilde{E}\times\mathcal{Y}_{d-1}$ where

$$\tilde{E} \overset{\text{def}}{=} \left\{\mathbf{u}\in\mathbf{S}^{d-1} : \text{ for } u\in\mathbf{u},\ S(\mathbf{u})>1\right\} \subset \mathbf{S}^{d-1}.$$

The convergences in (5.8) follow from the following two lemmata:

Lemma 5.3. *Fix $n\in\mathbb{N}$ and let $v = v_n$. Set $M_n = \max_{x\in R_v}\mu_n(x)$ and $N_n = \max_{x\in R_v}\nu_n(x)$ and $a = |\Gamma_1|$. For every $x\in R_v$, $\frac{M_n}{a}\le\mu_n(x)\le M_n$ and $\frac{N_n}{a}\le\nu_n(x)\le N_n$. Furthermore, equality holds in the right hand side of both inequalities when $x\in R_v\setminus E$.*

Lemma 5.4. *We have that*

$$|R_{v_n}\cap E|/|R_{v_n}| \overset{n\to\infty}{\longrightarrow} 0. \tag{5.9}$$

Proof of Lemma 5.3. Let $x(u) = \left(\frac{\mathbf{u}}{\|\mathbf{u}\|},[\Delta_\mathbf{u}]\right)$ and $S(x(u)) \overset{\text{def}}{=} S(\frac{\mathbf{u}}{\|\mathbf{u}\|})$. By the definition of ν_n, we have for $x(u)\in R_{v_n}$ that $\nu_n(x(u)) = \frac{|\Gamma_1|}{|R_{v_n}|S(x(u))}$. So the lemma follows for ν_n. For μ_n first note that, using (5.5) we have

$$\mu_n(x(u)) = \eta_{v_n}(\Theta_K\times\mathbb{L}^+(\mathbb{Z}_p)(k_v,h,\theta_v,l(h))\mathbb{G}(\mathbb{Z}[\tfrac{1}{p}]))$$

where $h = h(x(u))$ is the unique (by Prop. 5.2) element corresponding to $x(u)$ in M_0. Therefore, we will be done once we show that the stabilizer of the above orbit, namely,

$$\left|\left(\Theta_K\times\mathbb{L}^+(\mathbb{Z}_p)\right)\cap\alpha_h\mathbb{G}(\mathbb{Z}[\tfrac{1}{p}]))\alpha_h^{-1}\right| \tag{5.10}$$

is bounded by $S(x(u))$, where $\alpha_h \overset{\text{def}}{=} (k_v,h,\theta_v,l(h))$. To this end, notice that as $\Theta_K\times\mathbb{L}^+(\mathbb{Z}_p)$ embeds diagonally into the product $\mathbb{G}_1\times\mathbb{G}_2$, the third and the fourth coordinate of an element in this stabilizer are determined by the first and the second. As we are only interested in getting an upper bound it is enough to consider the stabilizer in $\mathbb{G}_1$. Using that $Kk_v = k_v\mathbb{H}_v(\mathbb{R})$ and $\mathbb{H}^+(\mathbb{Z}_p) \overset{\text{def}}{=} \mathbb{H}^+_{v,\{p\}} \cap \mathbb{G}_1(\mathbb{Z}_p) \subset \mathbb{G}_1(\mathbb{Z}_p)$ it is enough to bound

$$\left|(\mathbb{H}_v(\mathbb{R}) \times \mathbb{G}_1(\mathbb{Z}_p)) \cap (e,h)\mathbb{G}_1(\mathbb{Z}[\tfrac{1}{p}])(e,h^{-1})\right|.$$

Using the decomposition $h = c\gamma \overset{\text{def}}{=} c(h)\gamma(h)^{-1}$ and that $c \in \mathbb{G}_1(\mathbb{Z}_p)$ the latter is bounded by

$$\left|(\mathbb{H}_v(\mathbb{R}) \times \gamma\mathbb{G}_1(\mathbb{Z}_p)\gamma^{-1}) \cap \mathbb{G}_1(\mathbb{Z}[\tfrac{1}{p}])\right|. \tag{5.11}$$

As $\gamma \in \mathbb{G}_1(\mathbb{Z}[\frac{1}{p}])$ we have $\gamma\mathbb{G}_1(\mathbb{Z}_p)\gamma^{-1} \cap \mathbb{G}_1(\mathbb{Z}[\frac{1}{p}]) = \gamma\mathbb{G}_1(\mathbb{Z})\gamma^{-1}$. Therefore

$$\left|\mathbb{H}_v(\mathbb{R}) \cap \gamma\mathbb{G}_1(\mathbb{Z})\gamma^{-1}\right| = \left|\gamma^{-1}\mathbb{H}_v(\mathbb{R})\gamma \cap \mathbb{G}_1(\mathbb{Z})\right| = S(x(u))$$

bounds (5.11). □

Proof of Lemma 5.4 . We have that $\mu_n(E) = \mu_n(\tilde{E} \times \mathcal{Y}_{d-1}) \overset{n\to\infty}{\longrightarrow} 0$ since by (5.2) we have $\limsup_{n\to\infty} (\pi_1)_* \mu_n(\tilde{E}) \leq m_{\mathbf{S}^{d-1}}(\tilde{E}) = 0$. Here $\pi_1 : \mathbf{S}^{d-1} \times \mathcal{Y}_{d-1} \to \mathbf{S}^{d-1}$ is the projection map. Using Lemma 5.3 we have

$$\mu_n(E) = \frac{\mu_n(E \cap R_{v_n})}{\mu_n(R_{v_n})} \geq \frac{\frac{M_n}{a}|E \cap R_{v_n}|}{M_n|R_{v_n}|} \geq \frac{1}{a}\frac{|E \cap R_{v_n}|}{|R_{v_n}|} \tag{5.12}$$

which gives (5.9).

□

This shows (5.8) and thus that

$$\lim_{n\to\infty} \nu_n = \lim_{n\to\infty} \mu_n = m_{\mathbf{S}^{d-1}} \otimes m_{\mathcal{Y}_{d-1}}. \tag{5.13}$$

5.5. **Concluding the proof of Theorem 1.2.** We have to show that the convergence in (4.2) holds. In fact, we have proven a stronger statement. The support of ν_D can be written as a disjoint union of equivalence classes of the form R_v for some $v \in \mathbb{S}^{d-1}(D)$. The convergence in (5.13) shows that *each* sequence of the form (ν_v) for any choice of varying vectors v (under the congruence condition $\|v\|^2 \in \mathbb{D}(p)$ when $d = 4$ or 5), equidistribute to $m_{\mathbf{S}^{d-1}} \otimes m_{\mathcal{Y}_{d-1}}$. This implies Theorem 1.2.

References

[AES14] M. Aka, M. Einsiedler, and U. Shapira, *Integer points on spheres and their orthogonal lattices (with an appendix by Ruixiang Zhang*, preprint (2014).

[BT73] A. Borel and J. Tits, *Homomorphismes "abstraits" de groupes algébriques simples*, Ann. of Math. (2) **97** (1973), 499–571. MR0316587 (47 #5134)

[Dyn00] E. Dynkin, *Maximal subgroups of the classical groups*, Selected Papers of EB Dynkin with Commentary, Amer. Math. Soc, Providence, RI (2000), 37–170.

[Dyn52] E. B. Dynkin, *Maximal subgroups of the classical groups*, Trudy Moskovskogo Matematicheskogo Obshchestva **1** (1952), 39–166.

[EMMV14] M. Einsiedler, G. Margulis, A. Mohammadi, and A. Venkatesh, *Effective equidistribution and property* (τ), preprint (2014).

[EMSS] M. Einsiedler, S. Mozes, S. Shah, and U. Shapira, *Equidistribution of primitive rational points on expanding horospheres*. Preprint.

[EMV09] M. Einsiedler, G. Margulis, and A. Venkatesh, *Effective equidistribution for closed orbits of semisimple groups on homogeneous spaces*, Invent. Math. **177** (2009), no. 1, 137–212.

[ERW14] M. Einsiedler, R. Rühr, and P. Wirth, *Effective equidistribution of shapes of orthogonal lattices*, preprint (2014).

[GO11] A. Gorodnik and H. Oh, *Rational points on homogeneous varieties and equidistribution of adelic periods*, Geom. Funct. Anal. **21** (2011), no. 2, 319–392. With an appendix by Mikhail Borovoi. MR2795511 (2012d:11144)

[Kit99] Y. Kitaoka, *Arithmetic of quadratic forms*, Vol. 106, Cambridge University Press, 1999.

[Maa56] H. Maass, *Spherical functions and quadratic forms*, J. Indian Math. Soc **20** (1956), 117–162.

[Maa59] H. Maass, *Über die Verteilung der zweidimensionalen Untergitter in einem euklidischen Gitter*, Mathematische Annalen **137** (1959), 319–327.

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

[Mar91] G. A Margulis, *Discrete subgroups of semisimple lie groups*, Vol. 17, Springer, 1991.

[MS95] S. Mozes and N. Shah, *On the space of ergodic invariant measures of unipotent flows*, Ergodic Theory and Dynamical Systems **15** (1995), no. 01, 149–159.

[MT94] G. Margulis and G. Tomanov, *Invariant measures for actions of unipotent groups over local fields on homogeneous spaces*, Inventiones mathematicae **116** (1994), no. 1, 347–392.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263 (95b:11039)

[Pro07] C. Procesi, *Lie groups*, Universitext, Springer, New York, 2007. An approach through invariants and representations. MR2265844 (2007j:22016)

[Ra95] M. Ratner, *Raghunathan conjectures for cartesian products of real and p-adic Lie groups*, Duke Mathematical Journal **77** (1995), no. 2, 275–382.

[Sch98] W. M. Schmidt, *The distribution of sublattices of* $\mathbf{Z}^m$, Monatsh. Math. **125** (1998), no. 1, 37–81.

Departement Mathematik, ETH Zürich, Rämistrasse 101, 8092 Zurich, Switzerland

E-mail address: `menashe-hai.akka@math.ethz.ch`

Departement Mathematik, ETH Zürich, Rämistrasse 101, 8092 Zurich, Switzerland

E-mail address: `manfred.einsiedler@math.ethz.ch`

Department of Mathematics, Technion, Haifa, Israel

E-mail address: `ushapira@gmail.com`