WHAT IS... THE SHAPE OF A LATTICE?

ANDREAS WIESER

Abstract. This are the notes for my talk given in the *What is..?*-seminar in Zurich on 25. October 2018.

In this talk we introduce the shape of a lattice (here a discrete subgroup of Euclidean space) which roughly captures the form of a fundamental parallelotope in it. We will particularly focus on primitive integral lattices and then address old and new questions surrounding such lattices and their shapes. The main (equidistribution) conjecture we discuss answers amongst other things the question whether or not the orientations of such lattices yield any information about their shapes and vice versa.

Let me begin by first explaining what a lattice is (for the purposes of this talk).

Definition 1.1. A *lattice* $\Lambda \subset \mathbb{R}^n$ is a discrete subgroup.

One can prove that any lattice Λ is of the form

$$\Lambda = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_k$$

for $v_1, \ldots, v_k \in \mathbb{R}^n$. The minimal such number k is called the *rank* of Λ.

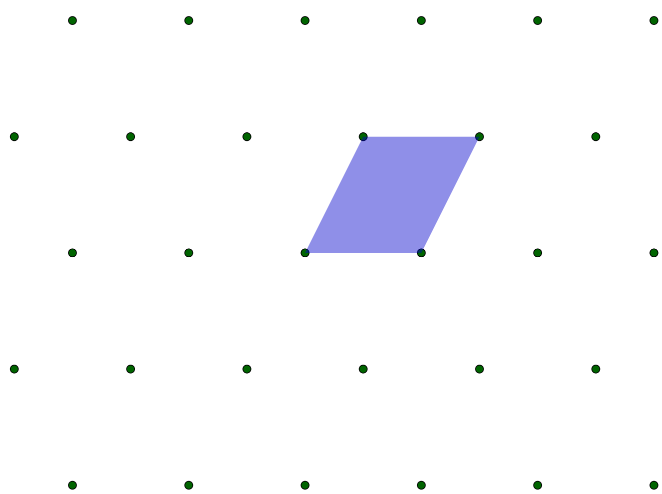


Figure 1. A lattice Λ of rank $k = 2$ viewed as a subset of the subspace $\Lambda_{\mathbb{R}}$ spanned by Λ.

The volume of the drawn parallelogram is what one usually calls the *covolume* of the lattice. Another quantity which one can attach to a lattice is the *discriminant* which is the determinant of the matrix

$$\begin{pmatrix} \langle v_1, v_1\rangle & \cdots & \langle v_1, v_k\rangle \\ \vdots & & \vdots \\ \langle v_k, v_1\rangle & \cdots & \langle v_k, v_k\rangle \end{pmatrix}$$

or in other words just the square of the covolume.

1.1. **Parametrizing lattices of full rank.** Let us for a moment now focus on lattices of full rank, i.e. with rank equal to n. By what we had before, any such lattice Λ can be written as $\Lambda = g\mathbb{Z}^n$ where $g \in \mathrm{GL}_n(\mathbb{R})$. Note that $|\det(g)| = \mathrm{covol}(\Lambda)$. We say that Λ is *unimodular*, if it has covolume 1 or equivalently if $\Lambda = g\mathbb{Z}^n$ for $g \in \mathrm{SL}_n(\mathbb{R})$. The space of unimodular lattices is defined as

$$X_n = \{\Lambda : \Lambda \text{ unimodular}\} \simeq \mathrm{SL}_n(\mathbb{R}) \big/ \mathrm{SL}_n(\mathbb{Z}).$$

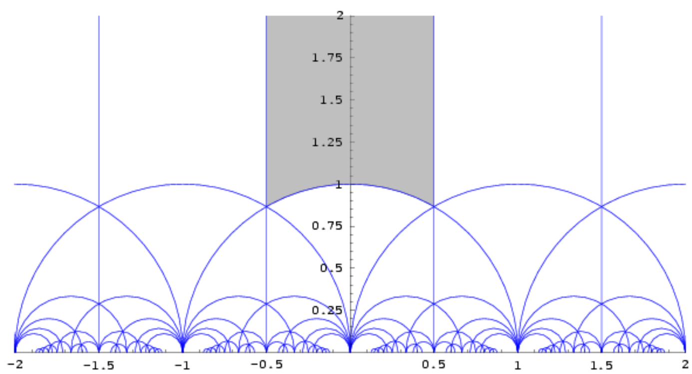
Dynamics and ergodic theory on this quotient has been very successful in encoding statements from number theory (e.g. from Diophantine approximation). The reason why one is able to prove many things using ergodic theory on this quotient is that $\mathrm{SL}_n(\mathbb{Z})$ is a lattice in $\mathrm{SL}_n(\mathbb{R})$ i.e. there is a finite $\mathrm{SL}_n(\mathbb{R})$-invariant measure on X_n.

The shape of a lattice of rank k will be an element of

$$\mathcal{X}_k = \mathrm{SO}(k) \big\backslash X_k$$

i.e. the space of lattices up to rotation[1].

To visualize $\mathcal{X}_2$, note that $\mathrm{SL}_2(\mathbb{R}) \,/\, \mathrm{SO}(2)$ can be identified with the hyperbolic plane via Moebius transformations. Thus, $\mathcal{X}_2$ is the hyperbolic plane folded up under the $\mathrm{SL}_2(\mathbb{Z})$-action by Moebius transformations. A fundamental domain is given as in the following picture.



1.2. **Definition of the shape.** Let $\Lambda < \mathbb{R}^n$ be a lattice of rank k. We fix a rotation $r \in \mathrm{SO}(n)$ with the property that $r.\Lambda_{\mathbb{R}} = \mathbb{R}^k \times \{0\}^{n-k} = \mathbb{R}^k$, that is, we rotate the k-dimensional subspace in which Λ lies to a fixed reference subspace that we simply call $\mathbb{R}^k$. Since $r.\Lambda < \mathbb{R}^k$ is a lattice of full rank, we may stretch it evenly in all directions to obtain a unimodular lattice in X_k.

[1]In some cases, the shape will in fact be an element of $\mathrm{O}(k) \setminus \mathrm{PGL}_k(\mathbb{R}) \,/\, \mathrm{PGL}_k(\mathbb{Z})$ but we will ignore this issue here.

Definition 1.2 (Shape)**.** The *shape* of the lattice Λ is the point

$$[\Lambda] = \mathrm{SO}(k)\frac{1}{\mathrm{covol}(\Lambda)^{\frac{1}{k}}}r\Lambda \in \mathrm{SO}(k)\Big\backslash X_k = \mathcal{X}_k.$$

Taking the quotient with $\mathrm{SO}(k)$ asserts that there is no dependency on the choice of r in the definition of the shape[2].

1.3. **Distribution of planes and shapes.** Let us now fix a lattice of full rank and consider only rank k sublattices of that lattice. For concreteness we take the integer lattice $\mathbb{Z}^n$ and call a lattice $\Lambda < \mathbb{R}^n$ *integral* if $\Lambda \subset \mathbb{Z}^n$. Note that the discriminant of an integer lattice is always a positive integer.

Such an integral lattice Λ is *primitive* if it is not contained in any larger sublattice of $\mathbb{Z}^n$ of the same rank. Equivalently, Λ is primitive if

$$\Lambda = \Lambda_{\mathbb{R}} \cap \mathbb{Z}^n.$$

For any positive integer d we define the finite set

$$\mathcal{R}_d^{k,n} = \{\Lambda : \text{primitive integral lattice of rank } k \text{ and discriminant } d\}.$$

One can now ask various questions of very different flavour for $\mathcal{R}_d^{k,n}$. For instance

When is $\mathcal{R}_d^{k,n}$ non-empty?

To the author's knowledge there is no complete answer to this question. There are however some cases in which there is an answer:

- $\mathcal{R}_d^{1,3}$ is non-empty if and only if $d \not\equiv 0, 4, 7 \bmod 8$. This is in essence Legendre's theorem on sums of three squares proven in full by Gauss [Gau86].
- $\mathcal{R}_d^{2,4}$ is non-empty if and only if $d \not\equiv 0, 7, 12, 15 \bmod 16$ – see for example [AEW19].
- $\mathcal{R}_d^{2,n}$ for $n \geq 5$ is always non-empty (Mordell [Mor32]).

In general, such a question is strongly connected Siegel's mass formula which aims at counting representations of forms in few by forms in many variables. This also yields the question

If non-empty, how large is $\mathcal{R}_d^{k,n}$?

Let us however not dwell on that and ask how these solutions (if you will) are distributed.

Conjecture 1.3 (Equidistribution of planes and shapes)**.** *Let $n \geq 3$ and $k \leq n$ with $n - k \geq 2$. If $k \geq 2$ the set*

$$\mathcal{J}_d^{k,n} = \{(\Lambda_{\mathbb{R}}, [\Lambda], [\Lambda^\perp \cap \mathbb{Z}^n]) : \Lambda \in \mathcal{R}_d^{k,n}\}$$

equidistributes to the uniform probability measure on $\mathrm{Gr}_{k,n}(\mathbb{R}) \times \mathcal{X}_k \times \mathcal{X}_{n-k}$. If $k = 1$, the analogous statement holds for the pairs $(\Lambda_{\mathbb{R}}, [\Lambda^\perp \cap \mathbb{Z}^n])$.

This means that, whenever you give yourself, say, a nice measurable set A of half the volume in $\mathrm{Gr}_{2,4}(\mathbb{R})$ in the limit you will still find all kinds of shapes under the given restriction on the subspace. Conversely, one can fix an approximate shape the lattice should have and also an approximate shape its orthogonal complement should have and one will always find for large enough discriminants a lattice with these given approximate shapes.

To the author's knowledge, the progress to the conjecture is the following:

---

[2] Up to a slight issue with orientation; this is the same problem as the one mentioned in the footnote on page 2.

- Maass [Maa56], [Maa59] in the 50's and W. Schmidt [Sch98] in the 90's: the pairs $(\Lambda_{\mathbb{R}}, [\Lambda])$ equidistribute when Λ varies over the primitive integral lattices of rank k with discriminant $\leq d$ (!).
- Aka, Einsiedler, Shapira [AES16b], [AES16a]: $k = 1$ where for $n = 3$ additional congruence conditions on d need to be assumed.
- Aka, Einsiedler, W. [AEW19]: $k = 2$ and $n = 4$ also under additional congruence assumptions. Here, the result is in fact much stronger as it also considers 2 further natural shapes that one can attach to each lattice.

The remaining cases will be treated in an upcoming preprint by Menny Aka and the author (also under additional congruence conditions). It is worthwhile remarking that in all of the above cases the congruence conditions are an artefact of the dynamical proofs.

1.3.1. *About the dynamical proofs and the congruence condition.* The theorems in [AES16b],[AES16a] and [AEW19] each follow from an equidistribution result for orbits in a locally homogeneous product space[3]

$$Y_1 \times Y_2 \times Y_3$$

under the stabilizer subgroup of subspaces $L = \mathrm{span}_{\mathbb{R}}(\Lambda)$

$$\mathbb{H}_L = \{g \in \mathrm{SO}_n : g.L = L\}.$$

Over the reals, we have an action of a compact group $\mathbb{H}_L(\mathbb{R}) \simeq \mathrm{SO}_k(\mathbb{R}) \times \mathrm{SO}_{n-k}(\mathbb{R})$ (up to finite index), which cannot yield any interesting dynamical behaviour. The way to avoid this, one considers instead the group of $\mathbb{Q}_p$-points! If Q is a positive-definite rational quadratic form, the group $\mathrm{SO}_Q(\mathbb{R})$ is compact, but $\mathrm{SO}_Q(\mathbb{Q}_p)$ might not be. In either of the works mentioned above, the imposed congruence condition asserts that for a given discriminant D satisfying this congruence condition, the stabilizer subgroup of any plane of this discriminant is isotropic. In order to obtain an action of $\mathbb{H}_L(\mathbb{Q}_p)$ one passes to an extension.

References

[AES16a] M. Aka, M. Einsiedler, and U. Shapira, *Integer points on spheres and their orthogonal grids*, J London Math Soc **93** (2016), no. 1, 143–158.

[AES16b] ———, *Integer points on spheres and their orthogonal lattices*, Invent. Math. **206** (2016), no. 2, 379–396.

[AEW19] M. Aka, M. Einsiedler, and A. Wieser, *Planes in four space and four associated CM points*, arXiv:1901.05833 (2019).

[Gau86] C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A.W.Grootendorst and with a preface by Waterhouse.

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

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

[Mor32] L.J. Mordell, *On the representations of a binary quadratic form as a sum of squares of linear forms*, Mathematische Zeitschrift **35** (1932), no. 1, 1–15.

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

[3] More precisely, Y_1 is an S-arthmetic extension of $\mathrm{SO}(n) \setminus \mathrm{SO}_n(\mathbb{Z})$ and Y_2, Y_3 are S-arthmetic extensions of $\mathrm{SL}_k(\mathbb{R}) \setminus \mathrm{SL}_k(\mathbb{Z})$ resp. $\mathrm{SL}_{n-k}(\mathbb{R}) \setminus \mathrm{SL}_{n-k}(\mathbb{Z})$.