

MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Report No. 3/2016

DOI: 10.4171/OWR/2016/3

## Lattices and Applications in Number Theory

Organised by  
Renaud Coulangeon, Talence  
Benedict Gross, Cambridge MA  
Gabriele Nebe, Aachen

17 January – 23 January 2016

**ABSTRACT.** This is a report on the workshop on Lattices and Applications in Number Theory held in Oberwolfach, from January 17 to January 23, 2016. The workshop brought together people working in various areas related to the field: classical geometry of numbers, packings, Diophantine approximation, Arakelov geometry, cohomology of arithmetic groups, algebraic modular forms and Hecke operators, algebraic topology. The meeting consisted of a few long talks which included an introductory part to each of the topics in the previous list, and a series of shorter talks mainly devoted to recent developments. The present report contains extended abstracts of all presentations.

*Mathematics Subject Classification (2010):* 11F75, 11H31, 11H55, 14G40, 20H10, 22E57.

### Introduction by the Organisers

The theory of lattices in Euclidean spaces is a very old subject which is still of great interest because of its various connections to other mathematical theories. As is well-known, the “Geometry of Numbers” developed at the end of the nineteenth century by Hermann Minkowski, following the pioneering works of Hermite, had a profound influence on the development of algebraic number theory. One goal of the workshop “Lattices and Applications in Number Theory” was to attest the vitality of this trend in modern number theory and to show how the theory of Euclidean lattices still provide tools for important discoveries. It was also an occasion for researchers from fairly different areas to exchange their ideas.

The meeting brought together 54 mathematicians from 11 countries. There were eleven one-hour talks, aimed at introducing to non-experts the various topics addressed during the week and presenting recent developments as well. Besides,

eight shorter talks (45 minutes) on some recent developments were proposed, and two afternoon sessions of short presentations ( $5 \times 20$  minutes) were organised.

We briefly describe below some of the main topics that were addressed during the workshop, and point out some of the results exposed.

- *Arakelov geometry* is the natural setting for a modern view on the “Geometry of Numbers”, in which Euclidean lattices appear as a particular instance of Hermitian bundles over arithmetic curves. A striking illustration is the very deep theorem of Zhang on successive minima of Hermitian bundles which can be seen as an analogue of Minkowski’s classical theorem about the successive minima of Euclidean lattices. The talks by Gaël Rémond, Éric Gaudron, Jean–Benoît Bost, and Christophe Soulé pertained to this topic. A closed formula for an absolute version (*i.e.* over  $\overline{\mathbb{Q}}$ ) of the Hermite constant was presented in Rémond’s talk.
- *Applications of Voronoi’s algorithm to arithmetic groups*: In a famous paper dating from 1907, Voronoi defined a face-to-face tiling of the cone of positive semidefinite quadratic forms by so-called *perfect domains* and described an algorithm to enumerate these domains up to  $\mathrm{SL}_n(\mathbb{Z})$  equivalence. It was observed in the 1970s (Ash, Soulé) that Voronoi’s tessellation could also be used to compute the (co)homology of  $\mathrm{SL}_n(\mathbb{Z})$ . Since then, and up to very recently, this observation, extended to more general arithmetic groups, gave rise to a substantial amount of work by various researchers. Philippe Elbaz–Vincent explained one of these recent developments in his talk during the meeting (triviality of  $K_8(\mathbb{Z})$  and application to the Vandiver Conjecture). The talks by Dan Yasaki and Joachim Schwermer dealt with related topics. Finally, Roland Bacher explained a construction of families of integral perfect lattices of minimum 4 which as a by-product shows that the number of perfect lattices grows at least exponentially in the dimension.
- In the tradition of Siegel’s works, *classical modular forms* play a central role in many questions involving lattices (representation numbers, mass formulas, classification of genera). This also was illustrated during the workshop, e.g. in Rainer Schulze–Pillot’s and Jeremy Rouse’s talks.
- *Arithmetic groups and algebraic modular forms*: A recent development in the study of arithmetic groups is the theory of algebraic modular forms, initially developed by Benedict Gross, where a connection between modular forms theory and Bruhat–Tits buildings of algebraic groups is studied. The intermediate objects again are lattices, which generalise naturally to integral forms of algebraic groups. Also other notions like genera and mass formulas have been transferred to more general arithmetic groups (dating back to works by Borel, Harish–Chandra and Kneser, and more recently in the fundamental works by Gopal Prasad). A comprehensive introduction to the subject was provided in the talk by Joshua Lansky and David Pollack. Other talks pertaining to this topic were those of Jessica Fintzen and Sebastian Schönnebeck.

Other crucial topics, not falling within the previous categories, were also addressed: packing and energy minimization problems and related applications of semidefinite optimization, counting arguments for dense lattices in certain families, but also algebraic topology and the algebraic theory of quadratic forms.

All speakers were considerate of the great variety of topics related to lattice theory in this conference and addressed their talks to this broad audience. This concept and the open and stimulating atmosphere of the location lead to many discussions. It was also very fruitful for the many young participants.

*Acknowledgement:* The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, “US Junior Oberwolfach Fellows”.



## Workshop: Lattices and Applications in Number Theory

### Table of Contents

Gaël Rémond (joint with Éric Gaudron)	
<i>Siegel fields</i> .....	93
Éric Gaudron (joint with Gaël Rémond)	
<i>Adelic quadratic spaces</i> .....	95
Joachim Schwermer	
<i>On the special linear group <math>SL_2</math> over orders in division algebras defined over some number field</i> .....	97
Jessica Fintzen	
<i>On the Moy–Prasad filtration and supercuspidal representations</i> .....	99
Ling Long (joint with Alyson Deines, Jenny Fuselier, Holly Swisher, Fang–Ting Tu)	
<i>The period lattices of the generalized Legendre curves</i> .....	102
Joshua M. Lansky, David J. Pollack	
<i>Algebraic modular forms</i> .....	105
Jean-Benoît Bost	
<i>Theta invariants, infinite dimensional Euclidean lattices and Diophantine geometry</i> .....	106
Christophe Soulé	
<i>Arithmetic surfaces and successive minima</i> .....	110
Dan Yasaki	
<i>Perfect forms over CM quartic fields</i> .....	111
Takao Watanabe	
<i>Fundamental domains of arithmetic quotients of reductive groups</i> .....	112
Mathieu Dutour-Sikirić	
<i>Practical computation of Hecke operators</i> .....	113
Markus Kirschmer	
<i>One-class genera of positive definite Hermitian forms</i> .....	114
Sebastian Schönneck	
<i>Simultaneous computation of Hecke operators</i> .....	116
Philippe Elbaz-Vincent	
<i>Perfect forms of rank <math>\leq 8</math>, triviality of <math>K_8(\mathbb{Z})</math> and the Kummer/Vandiver conjecture</i> .....	117

Henry Cohn (joint with Matthew de Courcy–Ireland)	
<i>The Gaussian core model in high dimensions</i> .....	120
Lenny Fukshansky (joint with Albrecht Böttcher, Stephan Ramon Garcia, Hiren Maharaj)	
<i>Lattices from Abelian groups</i> .....	121
Rainer Schulze-Pillot	
<i>Representation numbers and their averages</i> .....	124
Jeremy Rouse	
<i>The largest squarefree exception of a quaternary quadratic form</i> .....	127
Martin Widmer	
<i>Weakly admissible lattices and primitive lattice points</i> .....	129
John Voight	
<i>Discriminants and the monoid of quadratic rings</i> .....	132
Stefan Kühnlein (joint with Lenny Fukshansky, Rebecca Schwerdt)	
<i>Counting ideal lattices in <math>\mathbb{Z}^d</math></i> .....	134
Philippe Moustrou	
<i>On the density of cyclotomic lattices constructed from codes</i> .....	134
Tomoyoshi Ibukiyama	
<i>Vanishing criterion of automorphic forms on tube domains</i> .....	135
Martin Westerholt-Raum	
<i>Analytic properties of some indefinite theta series</i> .....	138
Jean Lannes (joint with H.-W. Henn)	
<i>From Grothendieck’s Chern classes to lattices of dimension 14 and     determinant 2</i> .....	139
Achill Schürmann (joint with Henry Cohn, Renaud Coulangeon, Abhinav Kumar, Christian Reiher)	
<i>Energy minimization and formal duality of periodic point configurations</i>	141
Maria Dostert (joint with Cristóbal Guzmán, Fernando Mário de Oliveira Filho, Frank Vallentin)	
<i>New upper bounds for the density of translative packings of superballs</i> ..	144
Roland Bacher	
<i>Some integral perfect lattices of minimum 4</i> .....	147
Eva Bayer-Fluckiger (joint with Uriya First)	
<i>Rationally isomorphic Hermitian forms</i> .....	147

## Abstracts

### Siegel fields

GAËL RÉMOND

(joint work with Éric Gaudron)

The aim of our paper [2] is to extend Minkowski's theorem/Siegel's lemma to infinite algebraic extensions of  $\mathbb{Q}$ . To formulate the problem, we replace the classical setting of metrized lattice by the framework of adelic spaces.

**Definition 1.** *Given a subfield  $K \subset \overline{\mathbb{Q}}$ , we define an adelic space to be a finite dimensional  $K$ -vector space  $E$  equipped with a collection of norms  $\|\cdot\|_v$  on  $E_v = E \otimes_K K_v$  for each place  $v$  of  $K$ . The adelic space  $E$  is said to be rigid if there exist an isomorphism  $\varphi: E \rightarrow K^n$  and an adelic matrix  $A \in \mathrm{GL}_n(\mathbb{A}_K)$  such that for each place  $v$  and each  $x \in E_v$  we have  $\|x\|_v = |A_v \varphi_v(x)|_v$ .*

Here  $\varphi_v$  denotes  $\varphi \otimes \mathrm{id}_{K_v}: E_v \rightarrow K_v^n$ , the adèles  $\mathbb{A}_K$  are  $\mathbb{A}_{\mathbb{Q}} \otimes K$  and  $|\cdot|_v$  is the standard norm on  $K_v^n$  given by  $|(y_1, \dots, y_n)|_v = \max(|y_1|_v, \dots, |y_n|_v)$  if  $v$  is finite and  $|(y_1, \dots, y_n)|_v = (|y_1|_v^2 + \dots + |y_n|_v^2)^{1/2}$  otherwise.

When  $K$  is a number field, we define the heights of a point and of the space by the products

$$(1) \quad H(x) = \prod_v \|x\|_v^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]} \quad (x \in E), \quad H(E) = \prod_v |\det A_v|_v^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]}$$

where  $A_v$  are the components of an adelic matrix  $A$  as in the definition. These definitions extend to the general case, using the fact that both  $A$  and  $x$  are defined over a number subfield of  $K$ ; alternatively, one can use a more intrinsic approach through integration over the set of places, see [2, part 2].

We now let  $\Lambda_1(E) = \inf\{H(x) \mid x \in E \setminus \{0\}\}$  be the first minimum of  $E$ . For a number field, Siegel's lemma is the statement that  $\Lambda_1(E)^n \leq (n\delta_{K/\mathbb{Q}})^{n/2} H(E)$  where  $n = \dim E$  and  $\delta_{K/\mathbb{Q}}$  is the root discriminant. Accordingly, we define the following avatar of Hermite's constant for  $K$ .

**Definition 2.** *For  $n \geq 1$ , let  $c_K(n) = \sup\{\Lambda_1(E)^n / H(E) \mid E \text{ rigid adelic space over } K \text{ of dimension } n\}$ .*

Our main definition is then as follows.

**Definition 3.** *The field  $K$  is said to be a Siegel field if  $c_K(n) < +\infty$  for all  $n \geq 1$ .*

Examples of Siegel fields are of course all the number fields but also  $\overline{\mathbb{Q}}$  by the absolute Siegel's lemma of Roy-Thunder [3] or by Zhang [5], who gives the estimate  $c_{\overline{\mathbb{Q}}}(n) \leq \exp(n(H_n - 1)/2)$  where  $H_n = 1 + 1/2 + \dots + 1/n$  is the harmonic number. We provide new examples such as the real algebraic numbers  $\mathbb{R} \cap \overline{\mathbb{Q}}$  or the towers of number fields with bounded root discriminant (e. g. class field towers).

Our first result gives examples of fields with no Siegel's lemma.

**Theorem 1.** *If  $[K : \mathbb{Q}] = \infty$  and  $K$  has Northcott property then  $K$  is not a Siegel field.*

Here we say, after Bombieri and Zannier [1], that  $K$  has Northcott property if the number of elements of  $K$  of bounded height is finite. This is certainly true for number fields (and false for  $\overline{\mathbb{Q}}$ ) but [1] provide more examples such as the field  $\mathbb{Q}(\mathbb{Q}^{1/d})$  of all  $d$ th roots of rational numbers (for some fixed  $d \geq 1$ ). Yet other examples come from [4].

We state as an open problem the question of whether there exists a field  $K$  having neither the Siegel nor the Northcott property. Likewise, we would like to know if certain specific interesting fields are Siegel: for example the maximal abelian extension  $\mathbb{Q}^{\text{ab}}$  or the field of totally real numbers (these two do not have Northcott property).

If we assume  $K$  to be a Siegel field, we can prove stronger statements. First we have for free a version of Minkowski's second theorem.

**Proposition 1.** *If  $E$  is a rigid adelic space of dimension  $n$  over  $K$ , we have  $\Lambda_1(E) \cdots \Lambda_n(E) \leq c_K(n)H(E)$ .*

Here we use the classical successive minima defined with a linear condition, that is  $\Lambda_i(E) = \inf\{\max(H(x_1), \dots, H(x_i)) \mid x_1, \dots, x_i \in E, \text{ linearly independent}\}$  but we can in fact obtain a much stronger version if we use Zhang's successive minima  $Z_i(E) = \inf\{\sup_{x \in S} H(x) \mid S \subset E, \dim \overline{S} \geq i\} \geq \Lambda_i(E)$  where  $\overline{S}$  denotes the Zariski closure of  $S$ .

**Theorem 2.** *If  $K$  is a Siegel field with  $[K : \mathbb{Q}] = \infty$ , there exists  $u(K) \in \mathbb{R}$  such that for any rigid adelic space  $E$  of dimension  $n$ , we have  $Z_1(E) \cdots Z_n(E) \leq u(K)^n c_K(n)H(E)$ .*

In fact, this statement implies Theorem 1 because the mere finiteness of  $Z_2(E)$  (any  $E$ ) implies that  $K$  can not have the Northcott property. The proofs of both the Proposition and Theorem 2 rely on a modification of the norms: rather easily and for archimedean places in the first case, in a more intricate way and at finite places in the second. In fact, the construction involved in the proof of the latter even gives more and allows to state the following exact computation of the Hermite constant of  $\overline{\mathbb{Q}}$  (Zhang's bound is in fact optimal).

**Theorem 3.** *We have  $c_{\overline{\mathbb{Q}}}(n) = \exp(n(H_n - 1)/2)$ .*

## REFERENCES

- [1] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of  $\mathbb{Q}$* , Rend. Mat. Acc. Lincei 12, 2001, p. 5–14.
- [2] É. Gaudron and G. Rémond, *Corps de Siegel*, J. reine angew. Math., to appear, 61 pages, DOI: 10.1515/crelle-2014-0096
- [3] D. Roy and J. Thunder, *An absolute Siegel's lemma*, J. reine angew. Math., 476, 1996, p. 1–26. Addendum and erratum. *ibid.* 508. 1999. p. 47–51.



- [4] M. Widmer, *On certain infinite extensions of the rationals with Northcott property*, *Monatsh. Math.*, 162, 2011, p. 341–353.  
 [5] S. Zhang, *Positive line bundles on arithmetic varieties*, *J. Amer. Math. Soc.*, 8, 1995, p. 187–221.

## Adelic quadratic spaces

ÉRIC GAUDRON

(joint work with Gaël Rémond)

We examine the links between linear and quadratic equations through the search of algebraic solutions of small heights.

The starting point is a theorem by Cassels (1955, [1]) and Davenport (1957, [3]) which asserts that if  $q: \mathbb{Q}^n \rightarrow \mathbb{Q}$  is a non-zero isotropic quadratic form with integral coefficients  $(a_{i,j})_{i,j}$  then there exists a vector  $x = (x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{0\}$  such that  $q(x) = 0$  and

$$\sum_{i=1}^n x_i^2 \leq \left( 2\gamma_{n-1}^2 \sum_{i,j} a_{i,j}^2 \right)^{(n-1)/2}$$

( $\gamma_{n-1}$  is the Hermite constant). Our aim is to give a generalization of this statement in the context of rigid adelic spaces (introduced in the preceding talk by Gaël Rémond).

Let  $K$  be an algebraic extension of  $\mathbb{Q}$  and  $n$  be a positive integer. We denote by  $c_K(n)$  the supremum over all rigid adelic spaces  $E$  over  $K$  of the real numbers

$$\inf \{ H_E(x)^n H(E)^{-1}; x \in E \setminus \{0\} \}$$

( $H_E(x)$  and  $H(E)$  are the heights of  $x$  and  $E$  with respect to the metrics on  $E$ ). According to [6], the field  $K$  is called a *Siegel field* if  $c_K(n) < +\infty$  for all  $n \geq 1$ . We have  $c_{\mathbb{Q}}(n) = \gamma_n^{n/2}$ ,

$$c_K(n) \leq \left( n |\Delta_{K/\mathbb{Q}}|^{1/[K:\mathbb{Q}]} \right)^{n/2}$$

if  $K$  is a number field of absolute discriminant  $\Delta_{K/\mathbb{Q}}$  and

$$c_{\overline{\mathbb{Q}}}(n) = \exp \left\{ \frac{n}{2} \left( \frac{1}{2} + \dots + \frac{1}{n} \right) \right\}$$

(see [6]).

An *adelic quadratic space*  $(E, q)$  over  $K$  is a rigid adelic space  $E/K$  endowed with a quadratic form  $q: E \rightarrow K$ . In this framework, several problems can be raised (here, small = of small height):

- 1) Existence of a small isotropic vector,
- 2) Existence of a small maximal totally isotropic subspace,
- 3) Existence of a basis of  $E$  composed of small isotropic vectors.

There exist between 25 and 30 articles in the literature dealing with these questions (essentially when  $K$  a number field or  $\overline{\mathbb{Q}}$ ). A common divisor to these works is the notion of Siegel's lemma. We shall provide solutions to these three problems, which are optimal with respect to the height of  $q$ .

The following statement gives an answer to the problem 2.

**Theorem 1.** *Assume  $q$  is isotropic. Then, for all  $\varepsilon > 0$ , there exists a maximal totally isotropic subspace  $F$  of  $E$  of dimension  $d \geq 1$  and height*

$$H(F) \leq (1 + \varepsilon)c_K(n - d) (2H(q))^{(n-d)/2} H(E).$$

Here  $H(q)$  is the height of  $q$  built from local operators norms (see [7]). For instance, in the context of Cassels and Davenport Theorem, one can prove that  $H(q) \leq (\sum_{i,j} a_{i,j}^2)^{1/2}$ . Theorem 1 generalizes and improves theorems by Schlickewei (1985,  $K = \mathbb{Q}$ , [9]), Vaaler (1987,  $K$  number field, [10]) and Fukshansky (2008,  $K = \overline{\mathbb{Q}}$ , [5]). Using a Siegel's lemma in such a subspace  $F$ , we obtain an answer to Problem 1:

**Lemma 1** (Quadratic Siegel's lemma). *If  $q$  is isotropic then, for all  $\varepsilon > 0$ , there exists  $x \in E \setminus \{0\}$  such that  $q(x) = 0$  and*

$$H_E(x) \leq (1 + \varepsilon) \left( c_K(n) (2H(q))^{(n-d)/2} H(E) \right)^{1/d}.$$

The proof of Theorem 1 follows from an estimate of the height of a suitable  $q$ -orthogonal symmetric of an almost minimal height subspace  $F$  (chosen among maximal totally isotropic subspaces of  $E$ ) and from a Siegel's lemma used with the quotient  $E/F$ . To be interesting, Theorem 1 must be applied in a Siegel field ( $c_K(n - d) < \infty$ ). But the converse is true: it can be also proved that to be a Siegel field is a necessary condition when a quadratic Siegel's lemma exists (take  $q(x) = \ell(x)^2$  with  $\ell: E \rightarrow K$  a linear form and use [6, § 4.8]).

Now, let us tackle the problem of a small isotropic basis of an adelic quadratic space  $(E, q)$  over a Siegel field  $K$ . Assume that there exists a nondegenerate isotropic vector in  $E$ . It is well known then that there exists a basis  $(e_1, \dots, e_n)$  of  $E$  such that  $q(e_i) = 0$  for all  $1 \leq i \leq n$ . Our goal is to have also the heights of  $e_i$ 's *small*. An obvious approach rests on an induction process, choosing  $e_i \in E \setminus K.e_1 \oplus \dots \oplus K.e_{i-1}$  with small height and  $q(e_i) = 0$ . That leads us to the following variant of the quadratic Siegel's lemma:

- 1a) Let  $I$  be an ideal of the ring of polynomials of  $E$  and denote by  $Z(I)$  the set of zeros  $\{x \in E; \forall P \in I, P(x) = 0\}$ . How to bound

$$\inf \{H_E(x); q(x) = 0 \text{ and } x \notin Z(I)\} ?$$

(Quadratic Siegel's lemma avoiding an algebraic set.)

To simplify, we state our result only for the standard adelic space  $E = K^n$ .

**Theorem 2.** *Let  $q: K^n \rightarrow K$  be a quadratic form and let  $I$  be an ideal of  $K[X_1, \dots, X_n]$  generated by polynomials of (total) degree  $\leq M$ . Assume (i)  $q \neq 0$*

and (ii)  $\exists x \notin Z(I)$ ;  $q(x) = 0$ . Then there exists a constant  $c(n, K) \geq 1$ , which depends only on  $n$  and  $K$ , such that the vector  $x$  in condition (ii) can also be chosen with height

$$H_{K^n}(x) \leq c(n, K)M^3 H(q)^{(n-d+1)/2}$$

where  $d$  is the dimension of maximal totally isotropic subspaces of  $(K^n, q)$ .

The constant  $c(n, K)$  can be made fully explicit (see [7, § 7]). This statement generalizes and improves previous results by Masser (1998,  $K = \mathbb{Q}$ ,  $Z(I)$  hyperplane, [8]), Fukshansky (2004,  $K$  number field,  $Z(I)$  union of hyperplanes, [4]) and Chan, Fukshansky & Henshaw (2014, [2]). Moreover the exponent  $(n - d + 1)/2$  of  $H(q)$  is best possible: take  $E = \mathbb{Q}^n$ ,  $a, d \geq 1$  integers,  $Z(I) = \{x_d = 0\}$  and

$$q(x) = 2x_{d+1}x_d - a^2x_d^2 - (x_{d+2} - ax_{d+1})^2 - \cdots - (x_n - ax_{n-1})^2.$$

We have  $H(q) = O_{a \rightarrow +\infty}(a^2)$  and if  $x$  is isotropic then  $|x_n| \geq a^{n-d+1}|x_d|/4$ . The proof of Theorem 2 relies on an avoiding Siegel's lemma and a geometric lemma. From Theorem 2 can easily be deduced a small-height isotropic basis of  $E$ .

Complete proofs and further results are given in [7].

#### REFERENCES

- [1] J. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. **51** (1955), 262–264.
- [2] W.K. Chan, L. Fukshansky and G. Henshaw, *Small zeros of quadratic forms outside a union of varieties*, Trans. Amer. Math. Soc. **366** (2014), 5587–5612.
- [3] H. Davenport, *Note on a theorem of Cassels*, Proc. Cambridge Philos. Soc. **53** (1957), 539–540.
- [4] L. Fukshansky, *Small zeros of quadratic forms with linear conditions*, J. Number Theory **108** (2004), 29–43.
- [5] L. Fukshansky, *Small zeros of quadratic forms over  $\overline{\mathbb{Q}}$* , Int. J. Number Theory **4** (2008), 503–523.
- [6] É. Gaudron and G. Rémond, *Corps de Siegel*, J. reine angew. Math. to appear, 61 pages. DOI: 10.1515/crelle-2014-0096
- [7] É. Gaudron and G. Rémond, *Espaces adéliques quadratiques*, 34 pages, preprint available on <http://math.univ-bpclermont.fr/~gaudron>
- [8] D. Masser, *How to solve a quadratic equation in rationals*, Bull. London Math. Soc. **30** (1998), 24–28.
- [9] H.P. Schlickewei, *Kleine Nullstellen homogener quadratischer Gleichungen*, Monatsh. Math. **100** (1985), 35–45.
- [10] J. Vaaler, *Small zeros of quadratic forms over number fields*, Trans. Amer. Math. Soc. **302** (1987), 281–296.

### On the special linear group $SL_2$ over orders in division algebras defined over some number field

JOACHIM SCHWERMER

Given an algebraic number field  $k$ , its ring of integers  $\mathcal{O}_k$ , let  $D$  be a finite-dimensional central division algebra defined over  $k$ . If  $\ell/k$  is a field extension we denote by  $D_\ell$  the  $\ell$ -algebra  $D \otimes_k \ell$ . Let  $GL(2, D)$  be the connected reductive

algebraic  $k$ -group whose group of  $\ell$ -rational points is the general linear group  $\mathrm{GL}_2(D_\ell) = \{x \in M_2(D_\ell) \mid \mathrm{nr}d_{M_2(D_\ell)}(x) \neq 0\}$ . Then the special linear group  $\mathrm{SL}(2, D)$ , defined as the kernel of the  $k$ -homomorphism  $\mathrm{GL}(2, D) \rightarrow G_m$  induced by the reduced norm, is a connected, almost simple, simply-connected algebraic  $k$ -group of  $k$ -rank 1. We denote by  $G_\infty$  the group of real points of the algebraic  $\mathbb{Q}$ -group obtained by restriction of scalars from  $\mathrm{SL}(2, D)$ , and we denote by  $X_\infty$  the corresponding symmetric space. An  $\mathcal{O}_k$ -order  $\Lambda$  in  $D$  gives rise to an arithmetically defined subgroup  $\Gamma_\Lambda$  in  $\mathrm{SL}_2(D)$ . It can be viewed as a discrete subgroup in the real Lie group  $G_\infty$ . The group  $\Gamma_\Lambda$  acts properly on  $X_\infty$ , and, if  $\Gamma_\Lambda$  is torsion-free, the orbit space is a non-compact locally symmetric space but of finite volume.

Generally we are interested in the geometry of these spaces  $X_\infty/\Gamma_\Lambda$ , their cohomology and the corresponding theory of automorphic forms [7]. In this talk we focused on the geometry of these spaces at infinity and the question how to determine the number  $cs(\Gamma_\Lambda)$  of  $\Gamma_\Lambda$ -conjugacy classes of minimal parabolic  $k$ -subgroups of  $\mathrm{SL}(2, D)$ . This number plays an important role in various compactifications of  $X_\infty/\Gamma_\Lambda$ , for example, the so-called Borel-Serre compactification. If the underlying division algebra is the field  $k$  itself then, in the case of the maximal order  $\mathcal{O}_k$ , the number  $cs(\Gamma_{\mathcal{O}_k})$  coincides geometrically with the number of cusps, given as the cardinality of the coset space obtained by the natural action of  $\Gamma_{\mathcal{O}_k}$  on the projective space  $\mathbb{P}_k^1$ . As shown, e.g., in [6], there is a bijection

$$\mathbb{P}_k^1/\Gamma_{\mathcal{O}_k} \xrightarrow{\sim} \mathcal{C}\ell(\mathcal{O}_k)$$

with the class group of  $k$ , thus,  $cs(\Gamma_{\mathcal{O}_k})$  is the class number  $h_k$  of  $k$ .

Suppose that  $\Lambda$  is a maximal  $\mathcal{O}_k$ -order  $\Lambda$  in  $D$ . Following Fröhlich [1], we denote by  $LF_1(\Lambda)$  the set of isomorphism classes of locally free left  $\Lambda$ -modules of rank 1. In an adelic approach, this set can be parametrized by the double cosets

$$LF_1(\Lambda) \xrightarrow{\sim} U_\Lambda \backslash D_{\mathbb{A}}^*/D^*$$

where  $U_\Lambda$  denotes the units of  $\Lambda$  embedded into the adelic points of the algebraic group  $\mathrm{SL}(1, D)$ . The cardinality of this set is finite. Furthermore, it is independent of the choice of the maximal  $\mathcal{O}_k$ -order  $\Lambda$  in  $D$ , thus it is denoted by  $h_D$ . Now, due to the Ph.D. thesis work of the Vienna students Christian Lacher [5] and Sophie Koch [2], [3], the following results hold true:

- (1) If  $D$  is not totally definite, then  $cs(\Gamma_\Lambda) = h_D$ , in particular,  $cs(\Gamma_\Lambda)$  is independent of the choice of the maximal order  $\Lambda$  (see [5]).
- (2) If  $D$  is totally definite, i.e.  $D$  ramifies at all archimedean places  $v \in V$  of  $k$  and  $D_v \cong \mathbb{H}$  the Hamilton quaternion algebra, then  $cs(\Gamma_\Lambda)$  is also independent of the choice of the maximal order  $\Lambda$  (see [2], [3]).
- (3) If  $D$  is totally definite and the narrow class number of  $k$  satisfies  $h_k^+ = 1$ , then  $cs(\Gamma_\Lambda) = h_D^2$  (see [5]). [This generalizes a result obtained in a classical approach in [4] for totally definite quaternion algebras defined over  $\mathbb{Q}$ .]

The starting point for the proof of these assertions is a general result obtained in [5] which gives a lower bound resp. an upper bound for  $cs(\Gamma_\Lambda)$  by certain arithmetic invariants attached to  $\Lambda$ . However, beyond the results alluded to, in

the general case of a totally definite quaternion division algebras, not subject to the condition in (3), one finds in [2] various examples where  $cs(\Gamma_\Lambda)$  is not a multiple of  $h_D$ .

We concluded the talk by briefly describing the topological nature [as fibre bundles] of the boundary components of the Borel-Serre compactification of the spaces  $X_\infty/\Gamma_\Lambda$  in question.

#### REFERENCES

- [1] A. Fröhlich, *Locally free modules over arithmetic orders*, J. f.d. reine u. angew. Mathematik, **274-275** (1975), 112–124.
- [2] S. Koch, *On the special linear group over orders in quaternion division algebras - arithmetic and geometry*, Ph.D. Thesis, University Vienna 2013.
- [3] S. Koch, *On the special linear group over orders in quaternion division algebras*, submitted.
- [4] V. Krafft, D. Osenberg, *Eisensteinreihen für einige arithmetisch definierte Untergruppen von  $SL_2(\mathbb{H})$* , Math. Zeitschrift. **204** (1990), 425–449.
- [5] C. Lacher, *Geometrie der affin-algebraischen reduzierten Norm-1 Gruppe einer zentral einfachen Algebra endlicher Dimension mit einem algebraischen Zahlkörper als Zentrum*, Ph.D. Thesis, University Vienna 2005.
- [6] C.L. Siegel, *Lectures on Advanced Analytic Number theory*, Lecture Notes, Tata Institute of Fundamental Research, Bombay 1961.
- [7] J. Schwermer, *Geometric cycles, arithmetic groups and their cohomology*, Bull. Amer. Math. Soc. **47** (2010), 187–279.

### On the Moy–Prasad filtration and supercuspidal representations

JESSICA FINTZEN

Let  $k$  be a nonarchimedean local field with residual characteristic  $p > 0$ . Let  $K$  be a maximal unramified extension of  $k$  with residue field  $\overline{\mathbb{F}}_p$ , and let  $G$  be a reductive group over  $K$ . In [2, 3], Bruhat and Tits defined a building  $\mathcal{B}(G, K)$  associated to  $G$ . For each point  $x$  in  $\mathcal{B}(G, K)$ , they constructed a compact subgroup  $G_x$  of  $G(K)$ , called parahoric subgroup. In [8, 9], Moy and Prasad defined a filtration of these parahoric subgroups by smaller subgroups

$$G_x = G_{x,0} \supseteq G_{x,r_1} \supseteq G_{x,r_2} \supseteq \dots,$$

where  $0 < r_1 < r_2 < \dots$  are real numbers depending on  $x$ . For simplicity, we assume that  $r_1, r_2, \dots$  are rational numbers. The quotient  $G_{x,0}/G_{x,r_1}$  can be identified with the  $\overline{\mathbb{F}}_p$ -points of a reductive group  $\mathbf{G}_x$ , and  $G_{x,r_i}/G_{x,r_{i+1}}$  ( $i > 0$ ) can be identified with an  $\overline{\mathbb{F}}_p$ -vector space  $\mathbf{V}_{x,r_i}$  on which  $\mathbf{G}_x$  acts.

If  $G$  is defined over  $k$ , this filtration was used to associate a depth to complex representations of  $G(k)$ , which can be viewed as a first step towards a classification of these representations. In 1998, Adler ([1]) used the Moy–Prasad filtration to construct supercuspidal representations of  $G(k)$ , and Yu ([12]) generalized his construction three years later. Kim ([6]) showed that for large primes  $p$  Yu’s construction yields all supercuspidal representations. However, the construction does not give rise to all supercuspidal representations for small primes.

In 2014, Reeder and Yu ([10]) gave a new construction of supercuspidal representations of smallest positive depth, which they called epipelagic representations. A vector in the dual  $\check{\mathbf{V}}_{x,r_1} = (G_{x,r_1}/G_{x,r_2})^\vee$  of the first Moy–Prasad filtration quotient is called stable in the sense of geometric invariant theory if its orbit under  $\mathbf{G}_x$  is closed and its stabilizer in  $\mathbf{G}_x$  is finite. The only input for the new construction of supercuspidal representations in [10] is such a stable vector. Assuming that  $G$  is a semisimple group that splits over a tamely ramified field extension, Reeder and Yu gave a necessary and sufficient criterion for the existence of stable vectors for sufficiently large primes  $p$ . In [5], we removed the assumption on the prime  $p$  for absolutely simple split reductive groups  $G$ , which yielded new supercuspidal representations for split groups. One application of the results in [4] presented during the talk is a criterion for the existence of stable vectors for all primes  $p$  for a much larger class of semisimple groups. This class includes semisimple groups that split over a tamely ramified field extension, i.e. those considered by [10] for large primes  $p$ , but it also includes arbitrary simply connected or adjoint semisimple groups. As a consequence we obtain supercuspidal representations of non-split  $p$ -adic reductive groups, in particular for small  $p$  now.

Our method of proof assumes the result for large primes and semisimple groups that split over a tamely ramified extension, and we transfer it to arbitrary residue field characteristics and a larger class of groups  $G$ . This is done via a comparison of the Moy–Prasad filtrations for different primes  $p$ .

More precisely, we show for a large class of reductive groups over finite extensions of  $\mathbb{Q}_p^{ur}$  (or  $\mathbb{F}_p((t))^{ur}$ ), which we call good groups (see Definition 3.1 in [4]), that the Moy–Prasad filtration is in a certain sense (made precise below) independent of the residue field characteristic  $p$ . The class of good groups contains reductive groups that split over a tamely ramified field extension as well as simply connected and adjoint semisimple groups and arbitrary restriction of scalars of any of these. The restriction to this large subclass of reductive groups is necessary as the main result in [4] (Theorem 1 below) fails in general. Given a good reductive group  $G$  over  $K$ , a rational point  $x$  of the Bruhat-Tits building  $\mathcal{B}(G, K)$  and an arbitrary prime  $q$  coprime to a certain integer  $N$  that depends on the splitting field of  $G$  (for details see Definition 3.1 in [4]), we construct a finite extension  $K_q$  of  $\mathbb{Q}_q^{ur}$ , a reductive group  $G_q$  and a point  $x_q$  in  $\mathcal{B}(G_q, K_q)$ . To this data, one can attach as above a Moy–Prasad filtration. The corresponding reductive quotient  $\mathbf{G}_{x_q}$  is a reductive group over  $\overline{\mathbb{F}}_q$  that acts on the quotients  $\mathbf{V}_{x_q, r_i}$ , which are identified with  $\overline{\mathbb{F}}_q$ -vector spaces. We then have the following theorem.

**Theorem 1** ([4]). *For each  $i \in \mathbb{Z}_{>0}$ , there exists a split reductive group scheme  $\mathcal{H}$  over  $\overline{\mathbb{Z}}[1/N]$  acting on a free  $\overline{\mathbb{Z}}[1/N]$ -module  $\mathcal{V}$  satisfying the following. For every prime  $q$  coprime to  $N$ , there exist isomorphisms  $\mathcal{H}_{\overline{\mathbb{F}}_q} \simeq \mathbf{G}_{x_q}$  and  $\mathcal{V}_{\overline{\mathbb{F}}_q} \simeq \mathbf{V}_{x_q, r_i}$  such that the induced representation of  $\mathcal{H}_{\overline{\mathbb{F}}_q}$  on  $\mathcal{V}_{\overline{\mathbb{F}}_q}$  corresponds to the above mentioned representation of  $\mathbf{G}_{x_q}$  on  $\mathbf{V}_{x_q, r_i}$ . Moreover, there are isomorphisms  $\mathcal{H}_{\overline{\mathbb{F}}_p} \simeq \mathbf{G}_x$  and  $\mathcal{V}_{\overline{\mathbb{F}}_p} \simeq \mathbf{V}_{x, r_i}$  such that the induced representation of  $\mathcal{H}_{\overline{\mathbb{F}}_p}$  on  $\mathcal{V}_{\overline{\mathbb{F}}_p}$  is*

the representation of  $\mathbf{G}_x$  on  $\mathbf{V}_{x,r_i}$ . In other words, we have commutative diagrams

$$\begin{array}{ccc}
 \mathcal{H}_{\overline{\mathbb{F}}_p} \times \mathcal{V}_{\overline{\mathbb{F}}_p} & \longrightarrow & \mathcal{V}_{\overline{\mathbb{F}}_p} \\
 \downarrow \simeq \times \simeq & & \downarrow \simeq \\
 \mathbf{G}_x \times \mathbf{V}_{x,r_i} & \longrightarrow & \mathbf{V}_{x,r_i}
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathcal{H}_{\overline{\mathbb{F}}_q} \times \mathcal{V}_{\overline{\mathbb{F}}_q} & \longrightarrow & \mathcal{V}_{\overline{\mathbb{F}}_q} \\
 \downarrow \simeq \times \simeq & & \downarrow \simeq \\
 \mathbf{G}_{x_q} \times \mathbf{V}_{x_q,r_i} & \longrightarrow & \mathbf{V}_{x_q,r_i} \quad .
 \end{array}$$

This theorem allows to compare the Moy–Prasad filtration representations for different primes.

We also give a new description of the Moy–Prasad filtration representations for reductive groups that split over a tamely ramified field extension of  $K$ . Let  $m$  be the order of  $x$ . We define an action of the group scheme  $\mu_m$  of  $m$ -th roots of unity on a reductive group  $\mathcal{G}_{\overline{\mathbb{F}}_p}$  over  $\overline{\mathbb{F}}_p$ , and denote by  $\mathcal{G}_{\overline{\mathbb{F}}_p}^{\mu_m,0}$  the connected component of the fixed point group scheme. In addition, we define a related action of  $\mu_m$  on the Lie algebra  $\text{Lie}(\mathcal{G}_{\overline{\mathbb{F}}_p})(\overline{\mathbb{F}}_p)$ , which yields a decomposition  $\text{Lie}(\mathcal{G}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p)) = \bigoplus_{i=1}^m \text{Lie}(\mathcal{G}_{\overline{\mathbb{F}}_p})_i(\overline{\mathbb{F}}_p)$ . Then we prove in [4] that the action of  $\mathbf{G}_x$  on  $\mathbf{V}_{x,r_i}$  corresponds to the action of  $\mathcal{G}_{\overline{\mathbb{F}}_p}^{\mu_m,0}$  on one of the graded pieces  $\text{Lie}(\mathcal{G})_j(\overline{\mathbb{F}}_p)$  of the Lie algebra of  $\mathcal{G}_{\overline{\mathbb{F}}_p}$ . This was previously known by [10] for sufficiently large primes  $p$ , and representations of the latter kind have been studied by Vinberg [11] in characteristic zero and generalized to positive characteristic coprime to  $m$  by Levy [7]. To be precise, we even prove a global version of the above mentioned result. See Theorem 4.1 in [4] for details. We also show that the same statement holds true for all good reductive groups after base change of  $\mathcal{H}$  and  $\mathcal{V}$  to  $\overline{\mathbb{Q}}$ , see Corollary 4.4 in [4].

This allows us to classify the points of the building  $\mathcal{B}(G, K)$  whose first Moy–Prasad filtration quotient contains stable vectors, which then yields supercuspidal representations (Corollary 5.5 in [4]). Similarly, the existence of semistable vectors is independent on the residue field characteristic (Theorem 5.1 in [4]).

REFERENCES

- [1] Jeffrey D. Adler. Refined anisotropic  $K$ -types and supercuspidal representations. *Pacific J. Math.*, 185(1):1–32, 1998.
- [2] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. *Inst. Hautes Études Sci. Publ. Math.*, (41):5–251, 1972.
- [3] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. II. Schémas en groupes. Existence d’une donnée radicielle valuée. *Inst. Hautes Études Sci. Publ. Math.*, (60):197–376, 1984.
- [4] Jessica Fintzen. On the Moy-Prasad filtration and stable vectors, 2015. Preprint, available at <http://arxiv.org/pdf/1511.00726v1.pdf>.
- [5] Jessica Fintzen and Beth Romano. Stable vectors in Moy-Prasad filtrations, 2015. Preprint, available at <http://arxiv.org/pdf/1510.00357v1.pdf>.
- [6] Ju-Lee Kim. Supercuspidal representations: an exhaustion theorem. *J. Amer. Math. Soc.*, 20(2):273–320 (electronic), 2007.
- [7] Paul Levy. Vinberg’s  $\theta$ -groups in positive characteristic and Kostant-Weierstrass slices. *Transform. Groups*, 14(2):417–461, 2009.

- [8] Allen Moy and Gopal Prasad. Unrefined minimal  $K$ -types for  $p$ -adic groups. *Invent. Math.*, 116(1-3):393–408, 1994.
- [9] Allen Moy and Gopal Prasad. Jacquet functors and unrefined minimal  $K$ -types. *Comment. Math. Helv.*, 71(1):98–121, 1996.
- [10] Mark Reeder and Jiu-Kang Yu. Epipelagic representations and invariant theory. *J. Amer. Math. Soc.*, 27(2):437–477, 2014.
- [11] È. B. Vinberg. The Weyl group of a graded Lie algebra. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(3):488–526, 709, 1976.
- [12] Jiu-Kang Yu. Construction of tame supercuspidal representations. *J. Amer. Math. Soc.*, 14(3):579–622 (electronic), 2001.

## The period lattices of the generalized Legendre curves

LING LONG

(joint work with Alyson Deines, Jenny Fuselier, Holly Swisher, Fang–Ting Tu)

Given  $i, j, k, N \in \mathbb{N}$ ,  $\lambda \in \overline{\mathbb{Q}}$  (the algebraic closure of  $\mathbb{Q}$ ), the generalized Legendre curve  $X_\lambda^{[N;i,j,k]}$  is the smooth model of the curve

$$C_\lambda^{[N;i,j,k]} : y^N = x^i(1-x)^j(1-\lambda x)^k.$$

We use  $J_\lambda^{[N;i,j,k]}$  to denote the Jacobian variety of  $X_\lambda^{[N;i,j,k]}$ . These curves have been studied by Wolfart [8], Archinard [3] and others. They satisfy very nice properties: their period lattices can be computed explicitly using classical Gauss hypergeometric functions and their local zeta functions can be computed using hypergeometric functions over finite fields which are defined in a few versions by Greene [5], Katz [6], McCarthy [7] respectively. Below we modify their definition slightly so that they are more parallel to the classical setting (for details see [4]). Part of our motivation is study 2-dimensional abelian varieties with quaternionic multiplication (QM) in the sense that their endomorphism algebras contain a quaternion algebra. In particular, we are interested in when one can construct such abelian varieties from the factors of  $J_\lambda^{[N;i,j,k]}$ . Below we consider the cases  $N = 3, 4, 6$  in which the primitive part of  $J_\lambda^{[N;i,j,k]}$ , denoted by  $J_\lambda^{\text{prim}}$ , is 2-dimensional.

Classical hypergeometric functions are an important class of special functions with many applications in mathematics and physics. Their properties are built on essentially two functions: the gamma function  $\Gamma(x)$  and the beta function: for  $\text{Re}(a) > 0, \text{Re}(b) > 0$ ,

$$B(a, b) = \int_0^1 x^{a-1}(1-x)^{b-1} dx = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

Now we define Gauss hypergeometric function using an idea of Euler. When  $\text{Re}(c) > \text{Re}(b) > 0$ , we first define the period function

$${}_2P_1 \left[ \begin{matrix} a & b \\ & c \end{matrix} ; \lambda \right] := \int_0^1 x^{b-1}(1-x)^{c-b-1}(1-\lambda x)^{-a} dx.$$



Then

$${}_2P_1 \left[ \begin{matrix} a & b \\ & c \end{matrix} ; 0 \right] = \int_0^1 x^{b-1}(1-x)^{c-b-1} dx = B(b, c-b).$$

Now let

$${}_2F_1 \left[ \begin{matrix} a & b \\ & c \end{matrix} ; \lambda \right] := B(b, c-b)_2^{-1} P_1 \left[ \begin{matrix} a & b \\ & c \end{matrix} ; \lambda \right] = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k \lambda^k}{(c)_k k!},$$

where  $(a)_k := a(a+1)\cdots(a+k-1) = \frac{\Gamma(a+k)}{\Gamma(a)}$ . Gauss hypergeometric functions  ${}_2F_1 \left[ \begin{matrix} a & b \\ & c \end{matrix} ; \lambda \right]$  satisfy many nice symmetries, see [1].

Let  $p$  be an odd prime,  $\mathbb{F}_q$  be a finite field of size  $q = p^e$ . Use  $\widehat{\mathbb{F}_q^\times}$  to denote the set of all multiplicative characters on  $\mathbb{F}_q^\times$ . For each  $\chi \in \widehat{\mathbb{F}_q^\times}$ , we use  $\overline{\chi}$  to denote its complex conjugation. Let  $\varepsilon$  be the trivial character. For each  $\chi \in \widehat{\mathbb{F}_q^\times}$ , including  $\varepsilon$ , we assume  $\chi(0) = 0$ . Let  $\Psi$  be a non-trivial additive character of  $\mathbb{F}_q$ . Define the Gauss sum of  $\chi \in \widehat{\mathbb{F}_q^\times}$  as  $g(\chi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\Psi(x)$ . The Jacobi sum of  $A, B \in \widehat{\mathbb{F}_q^\times}$  is defined as  $J(A, B) = \sum_{x \in \mathbb{F}_q} A(x)B(1-x)$ . It is well-known to the experts that Gauss sums (resp. Jacobi sums) are finite field analogues of the gamma (resp. beta) function. To be more explicit, there is a dictionary between the complex and finite field settings, see [4]. Below we assume  $q \equiv 1 \pmod N$ .

$\frac{1}{N}$	$\leftrightarrow$	a primitive character $\eta_N$ of order $N$
$a = \frac{i}{N}, b = \frac{j}{N}$	$\leftrightarrow$	$A, B \in \widehat{\mathbb{F}_q^\times}, A = \eta_N^i, B = \eta_N^j$
$x^a$	$\leftrightarrow$	$A(x)$
$-a$	$\leftrightarrow$	$\overline{A}$
$\Gamma(a)$	$\leftrightarrow$	$g(A)$
$B(a, b)$	$\leftrightarrow$	$J(A, B)$
$\int_0^1 dx$	$\leftrightarrow$	$\sum_{x \in \mathbb{F}}$

Base on the above dictionary, we define the finite field period functions by:

$${}_2\mathbb{P}_1 \left[ \begin{matrix} A & B \\ & C \end{matrix} ; \lambda; q \right] := \sum_{x \in \mathbb{F}_q} B(x)C\overline{B}(1-x)\overline{A}(1-\lambda x),$$

with

$${}_2\mathbb{P}_1 \left[ \begin{matrix} A & B \\ & C \end{matrix} ; 0; q \right] = J(B, C\overline{B})$$

Now we define the finite field hypergeometric functions.

$${}_2\mathbb{F}_1 \left[ \begin{matrix} A & B \\ & C \end{matrix} ; \lambda; q \right] := J(B, C\overline{B})^{-1} {}_2\mathbb{P}_1 \left[ \begin{matrix} A & B \\ & C \end{matrix} ; \lambda; q \right].$$

These  ${}_2\mathbb{F}_1$  functions satisfy many properties parallel to the classical  ${}_2F_1$  functions.

Coming back to the generalized Legendre curves  $X_\lambda^{[N; i, j, k]}$ , we assume  $0 \leq i, j, k < N, N \nmid i + j + k, \lambda \in \overline{\mathbb{Q}} \setminus \{0, 1\}$  so that the corresponding curve is an  $N$ -cold cyclic cover of  $BCP^1$  which ramifies at  $0, 1, \infty, 1/\lambda$ . Wolfhart gave an explicit

way to compute the period lattice using hypergeometric functions. Meanwhile, to compute the number of points on  $X_\lambda^{[N;i,j,k]}$  over  $\mathbb{F}_q$ , we will need character sums of the form  $\eta(x^i(1-x)^j(1-\lambda x)^k)$  with  $\eta^N = \varepsilon$ , which can be written explicitly as period functions  ${}_2\mathbb{P}_1$  over finite fields. Thus the period functions provide a way to compute the Galois representations associate with  $J_\lambda^{[N;i,j,k]}$  of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\lambda, e^{2\pi i/N}))$ . The symmetries of classical hypergeometric functions can be transferred to the Galois representations of  $X_\lambda^{[N;i,j,k]}$ . On the other hand, one has

**Lemma 1.**

$${}_2\mathbb{P}_1 \left[ \begin{matrix} A & B \\ C & \end{matrix} ; \lambda \right] = \overline{C}(\lambda) C \overline{AB}(\lambda - 1) \frac{J(B, C\overline{B})}{J(A, C\overline{A})} {}_2\mathbb{P}_1 \left[ \begin{matrix} \overline{A} & \overline{B} \\ \overline{C} & \end{matrix} ; \lambda \right],$$

In terms of Galois representation, when  $\lambda \in \mathbb{Q}$ , this Lemma relates the 2-dimensional Galois representations corresponding the left hand side with its complex conjugation. In the application of finding 2-dimensional abelian varieties with QM, we will like the factor  $\frac{J(B, C\overline{B})}{J(A, C\overline{A})}$  on the right corresponds to a finite order character of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\lambda, \zeta_N))$ . By the Hasse conjecture proved by Yamamoto [10], the corresponding beta quotient has to be an algebraic number. The converse also holds due to a transcendental theorem of Wüstholz [9] on periods of abelian varieties.

**Theorem 1** ([2]). *Let  $N = 3, 4, 6$ ,  $0 < i, j, k < N$ ,  $N \nmid i + j + k$ . Then for each  $\lambda \in \overline{\mathbb{Q}}$ , the endomorphism algebra of  $J_\lambda^{\text{prim}}$  contains a quaternion algebra over  $\mathbb{Q}$  if and only if*

$$B \left( \frac{N-i}{N}, \frac{N-j}{N} \right) / B \left( \frac{k}{N}, \frac{2N-i-j-k}{N} \right) \in \overline{\mathbb{Q}}.$$

## REFERENCES

- [1] George E. Andrews, Richard Askey, and Ranjan Roy. *Special functions*, volume 71 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1999.
- [2] Alyson Deines, Jenny G. Fuselier, Ling Long, Holly Swisher, and Fang Ting Tu. Generalized Legendre Curves and Quaternionic Multiplication. *Journal of Number Theory (in press)*, *arXiv:1412.6906*, 2014.
- [3] Natália Archinard. Hypergeometric abelian varieties. *Canad. J. Math.*, 55(5):897–932, 2003.
- [4] Jenny G. Fuselier, Ling Long, Ravi Ramakrishna, Holly Swisher, and Fang Ting Tu. Hypergeometric functions over finite fields. *arXiv:1510.02575*, 2015.
- [5] John Greene. Hypergeometric functions over finite fields. *Trans. Amer. Math. Soc.*, 301(1):77–101, 1987.
- [6] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.
- [7] Dermot McCarthy. Transformations of well-poised hypergeometric functions over finite fields. *Finite Fields Appl.*, 18(6):1133–1147, 2012.
- [8] Jürgen Wolfart. Werte hypergeometrischer Funktionen. *Invent. Math.*, 92(1):187–216, 1988.

- [9] G. Wüstholz. Algebraic groups, Hodge theory, and transcendence. In *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Berkeley, Calif., 1986), pages 476–483. Amer. Math. Soc., Providence, RI, 1987.
- [10] Koichi Yamamoto. On a conjecture of Hasse concerning multiplicative relations of Gaussian sums. *J. Combinatorial Theory*, 1:476–489, 1966.

### Algebraic modular forms

JOSHUA M. LANSKY, DAVID J. POLLACK

We review the theory of algebraic modular forms on connected reductive algebraic  $\mathbb{Q}$ -groups  $G$  such that  $G(\mathbb{R})$  is compact modulo center. Early instances of such modular forms were studied by Eichler, Ihara, Hashimoto, and Ibukiyama, among others. Following Gross's general framework [1], we define the space of algebraic modular forms  $M(V, K)$  of weight  $V$  and level  $K = \prod K_p$  to be

$$M(V, K) = \{f : G(\hat{\mathbb{Q}}) \rightarrow V(\mathbb{Q}) \text{ such that } f(\gamma g k) = \gamma f(g) \text{ for } \gamma \in G(\mathbb{Q}), k \in K\},$$

where  $V$  is a  $\mathbb{Q}$ -rational representation of  $G$ , and  $K$  is an open compact subgroup of  $G(\hat{\mathbb{Q}})$ . (Here  $\hat{\mathbb{Q}}$  is the ring of finite adeles of  $\mathbb{Q}$ .) The space  $M(V, K)$  carries an action of the Hecke algebra  $H_K$  of  $K$ -bi-invariant, compactly supported functions on  $G(\hat{\mathbb{Q}})$  given by

$$Tf(g) = \int_{G(\hat{\mathbb{Q}})} T(x)f(gx)dx$$

for  $T \in H_K$ .

The compactness mod center of  $G(\mathbb{R})$  makes  $M(V, K)$  amenable to efficient calculation. Since irreducible  $H_K$ -submodules of  $M(V, K) \otimes \mathbb{C}$  correspond to irreducible automorphic representations of  $G(\mathbb{A})$  having  $K$ -fixed vectors and infinite component  $V \otimes \mathbb{C}$ , such calculations yield information on the automorphic spectrum of  $G$ .

We outline a method for computing a basis for  $M(V, K)$  and the action of  $H_K$  on  $M(V, K)$  (as in [5]). The assumption on  $G(\mathbb{R})$  implies that  $G(\mathbb{Q}) \backslash G(\hat{\mathbb{Q}}) / K$  is finite. Choosing representatives  $g_i$  for these double cosets, and letting  $\Gamma_i = G(\mathbb{Q}) \cap g_i K g_i^{-1}$ , we see

$$M(V, K) \cong \bigoplus V^{\Gamma_i}.$$

Note that once we compute representatives  $g_i$  corresponding to a maximal level  $K$ , it is straightforward to obtain representatives for deeper levels. To find the  $g_i$  at a maximal level requires a separate analysis. For example, see [2] in the case where  $G$  is a compact form of  $\mathrm{GSP}_4$ .

To compute the action of the Hecke algebra on  $M(V, K)$  we need to decompose  $K_p$ -double cosets into single cosets. We derive a solution to this problem in the case in which  $G$  is split over  $\mathbb{Q}_p$  and  $K_p$  is a hyperspecial maximal compact subgroup of  $G(\mathbb{Q}_p)$  (see [5] and, for a more general decomposition, [4]).

## REFERENCES

- [1] B. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.
- [2] K. Hashimoto and T. Ibukiyama, *On class numbers of positive definite binary quaternion Hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), 549–601.
- [3] Y. Ihara, *On certain arithmetical Dirichlet series*, J. Math. Soc. Japan **16** (1964), 214–225.
- [4] J. Lansky, *Decomposition of double cosets in  $p$ -adic groups*, Pacific J. Math. **197** (2001), 97–117.
- [5] J. Lansky and D. Pollack, *Hecke algebras and automorphic forms*, Compositio Math. **130** (2002), 21–48.

## Theta invariants, infinite dimensional Euclidean lattices and Diophantine geometry

JEAN-BENOÎT BOST

**1.** In the classical analogy between number fields and function fields, an Euclidean lattice  $\overline{E} := (E, \|\cdot\|)$  — defined by a free  $\mathbb{Z}$ -module of finite rank  $E$  and some Euclidean norm  $\|\cdot\|$  on the  $\mathbb{R}$ -vector space  $E_{\mathbb{R}} := E \otimes_{\mathbb{Z}} \mathbb{R}$  — appears as the counterpart of a vector bundle  $V$  on a smooth projective curve  $C$  over some field  $k$ .

In this analogy, the arithmetic counterpart of the dimension

$$h^0(C, V) := \dim_k \Gamma(C, V)$$

of the space of sections of  $V$  is the non-negative real number

$$h_{\theta}^0(\overline{E}) := \log \sum_{v \in E} e^{-\pi \|v\|^2}.$$

This correspondence goes back to the classical German school of number theory. Indeed, it is conspicuous when comparing the proof of the meromorphic continuation and functional equation for the zeta function of a number field by Hecke ([Hec17]) and for the zeta function of a function field  $k(C)$  (when  $k$  is a finite field) by F. K. Schmidt ([Sch31]).

More recently, the invariant  $h_{\theta}^0(\overline{E})$  has been investigated in the perspective of Arakelov geometry, notably by Roessler ([Roe93]), van der Geer and Schoof ([vdGS00]) and Groenewegen ([Gro01]).

Another arithmetic counterpart of the dimension  $h^0(C, V)$ , already introduced in substance by Weil ([Wei39]) and considered more systematically by Arakelov and his followers (see for instance [Man85] and [Szp85]), is defined as:

$$h_{\text{Ar}}^0(\overline{E}) := \log |\{v \in E \mid \|v\| \leq 1\}|.$$

More generally, for any  $t \in \mathbb{R}_+^*$ , we let:

$$h_{\text{Ar}}^0(\overline{E}, t) := \log |\{v \in E \mid \|v\|^2 \leq t\}|.$$

This talk is devoted to the properties of the invariant  $h_{\theta}^0$  and of its extension to certain infinite dimensional generalizations of Euclidean lattices. One may refer to [Bos15] for more details and proofs.

**2.** It is possible to compare the two arithmetic counterparts  $h_{\theta}^0(\overline{E})$  and  $h_{\text{Ar}}^0(\overline{E})$  of the geometric invariant  $h^0(C, V)$ .

**Theorem 1.** *For any Euclidean lattice  $\overline{E}$  of positive rank  $\text{rk}E$ , we have:*

$$(1) \quad -\pi \leq h_\theta^0(\overline{E}) - h_{\text{Ar}}^0(\overline{E}) \leq (\text{rk}E/2) \cdot \log \text{rk}E + \log(1 - 1/2\pi)^{-1}.$$

The first inequality in (1) is straightforward. The proof of the second one relies on the techniques introduced by Banaszczyk in his work on transference inequalities in geometry of numbers ([Ban93]).

To any Euclidean lattice  $\overline{E}$ , we may attach its *theta function*, namely the function  $\theta_{\overline{E}}$  on  $\mathbb{R}_+^*$  defined by:

$$\theta_{\overline{E}}(t) := \sum_{v \in E} e^{-\pi t \|v\|^2}.$$

By the very definition of  $h_\theta^0(\overline{E})$ , we have:

$$h_\theta^0(\overline{E}) := \log \theta_{\overline{E}}(1).$$

Conversely, for any  $\delta \in \mathbb{R}$ , we may define consider the Euclidean lattice

$$\overline{E} \otimes \overline{\mathcal{O}}(\delta) := (E, e^{-\delta} \|\cdot\|)$$

deduced from  $\overline{E}$  by scaling its norm by the factor  $e^{-\delta}$ . Then (the logarithm of) the theta function  $\theta_{\overline{E}}$  may be seen as an arithmetic counterpart of the Hilbert function of a vector bundle:

$$\log \theta_{\overline{E}}(t) = h_\theta^0(\overline{E} \otimes \overline{\mathcal{O}}(-(1/2) \log t)).$$

**Theorem 2.** *For any Euclidean lattice  $\overline{E}$  and any  $t \in \mathbb{R}_+^*$ , the limit*

$$\tilde{h}_{\text{Ar}}^0(\overline{E}, t) := \lim_{n \rightarrow +\infty} \frac{1}{n} h_{\text{Ar}}^0(\overline{E}^{\oplus n}, t)$$

*exists and satisfies:*

$$\tilde{h}_{\text{Ar}}^0(\overline{E}, t) = \sup_{n \geq 1} \frac{1}{n} h_{\text{Ar}}^0(\overline{E}^{\oplus n}, t) < +\infty.$$

*The function  $\tilde{h}_{\text{Ar}}^0(\overline{E})$  and  $\log \theta_{\overline{E}}$  on  $\mathbb{R}_+^*$  are real analytic, and respectively concave and convex. They are related by Legendre duality:*

$$\text{for every } x \in \mathbb{R}_+^*, \tilde{h}_{\text{Ar}}^0(\overline{E}, x) = \inf_{\beta > 0} [\pi \beta x + \log \theta_{\overline{E}}(\beta)]$$

*and*

$$\text{for every } \beta \in \mathbb{R}_+^*, \log \theta_{\overline{E}}(\beta) = \sup_{x > 0} [\tilde{h}_{\text{Ar}}^0(\overline{E}, x) - \pi \beta x].$$

When  $\overline{E}$  is the “trivial” Euclidean lattice  $(\mathbb{Z}, |\cdot|)$ , Theorem 2 may be derived from the results of Odlyzko and Mazo [MO90].

To establish its general version, in [Bos15] we first prove a generalization of Cramér’s theorem in the theory of large deviation that is valid, not only on a probability space, but on some measured space with possibly infinite total mass. Theorem 2 is a consequence of this generalized Cramér’s theorem applied to the set  $E$  equipped with the counting measure.

This extension of Cramér’s theorem is closely related to the formalism of statistical thermodynamics. This relation actually suggests some properties of the

invariants  $\tilde{h}_{\text{Ar}}^0(\overline{E}, t)$ . For instance, the following corollary may be understood as an avatar of the second law of thermodynamics:

**Corollary 1.** *For any two Euclidean lattices  $\overline{E}_1$  and  $\overline{E}_2$ , we have:*

$$\tilde{h}_{\text{Ar}}^0(\overline{E}_1 \oplus \overline{E}_2, t) = \max_{\substack{t_1, t_2 > 0 \\ t_1 + t_2 = t}} \left( \tilde{h}_{\text{Ar}}^0(\overline{E}_1, t_1) + \tilde{h}_{\text{Ar}}^0(\overline{E}_2, t_2) \right).$$

**2.** The infinite dimensional generalizations of Euclidean lattices we are interested in, with a view towards Diophantine geometry, are the *pro-Euclidean lattices*. They naturally occur as projective limits of countable systems of Euclidean lattices

$$(2) \quad \overline{E}_\bullet : \overline{E}_0 \xleftarrow{q_0} \overline{E}_1 \xleftarrow{q_1} \dots \xleftarrow{q_{i-1}} \overline{E}_i \xleftarrow{q_i} \overline{E}_{i+1} \xleftarrow{q_{i+1}} \dots$$

Here, for every  $i \in \mathbb{N}$ , we have denoted by  $\overline{E}_i$  some Euclidean lattice  $(E_i, \|\cdot\|_i)$  and by  $q_i$  a surjective morphism of  $\mathbb{Z}$ -modules

$$q_i : E_{i+1} \longrightarrow E_i$$

such that the norm  $\|\cdot\|_i$  on  $V_{i,\mathbb{R}}$  coincides with the the quotient norm deduced from the norm  $\|\cdot\|_{i+1}$  on  $E_{i+1,\mathbb{R}}$  by means of the surjective  $\mathbb{R}$ -linear map

$$q_{i,\mathbb{R}} := q_i \otimes Id_{\mathbb{R}} : E_{i+1,\mathbb{R}} \longrightarrow E_{i,\mathbb{R}}.$$

A *pro-Euclidean lattice* may actually be defined directly, without explicit mention of projective systems of Euclidean lattices, as a triple

$$\widehat{E} := (\widehat{E}, E_{\mathbb{R}}^{\text{Hilb}}, \|\cdot\|)$$

consisting in the following data:

- an abelian topological group  $\widehat{E}$ , isomorphic to  $\mathbb{Z}^n$  (for some  $n \in \mathbb{N}$ ) equipped with the discrete topology, or to  $\mathbb{Z}^{\mathbb{N}}$  equipped with the product topology of the discrete topology on each factor  $\mathbb{Z}$ ;
- a dense real vector subspace  $E_{\mathbb{R}}^{\text{Hilb}}$  of the topological real vector space  $\widehat{E}_{\mathbb{R}} := \widehat{E} \widehat{\otimes}_{\mathbb{Z}} \mathbb{R}$ , defined as the completed tensor product of  $\widehat{E}$  by  $\mathbb{R}$ ;
- a norm  $\|\cdot\|$  on  $E_{\mathbb{R}}^{\text{Hilb}}$  that makes  $(E_{\mathbb{R}}^{\text{Hilb}}, \|\cdot\|)$  a real Hilbert space; this Hilbert space topology on  $E_{\mathbb{R}}^{\text{Hilb}}$  is moreover required to be finer than the topology induced by the topology of  $\widehat{E}_{\mathbb{R}}$ .

To any projective system  $\overline{E}_\bullet$  as (2) above, one attaches a pro-Euclidean lattice

$$\varprojlim \overline{E}_\bullet := (\widehat{E}, E_{\mathbb{R}}^{\text{Hilb}}, \|\cdot\|)$$

by defining  $\widehat{E}$  as the pro-discrete  $\mathbb{Z}$ -module  $\widehat{E} := \varprojlim_i E_i$  and  $(E_{\mathbb{R}}^{\text{Hilb}}, \|\cdot\|)$  as the projective limit, in the category of real normed vector spaces, of the projective system:

$$(E_{0,\mathbb{R}}, \|\cdot\|_0) \xleftarrow{q_{0,\mathbb{R}}} (E_{1,\mathbb{R}}, \|\cdot\|_1) \xleftarrow{q_{1,\mathbb{R}}} \dots \xleftarrow{q_{i-1,\mathbb{R}}} (E_{i,\mathbb{R}}, \|\cdot\|_i) \xleftarrow{q_{i,\mathbb{R}}} (E_{i+1,\mathbb{R}}, \|\cdot\|_{i+1}) \xleftarrow{q_{i+1,\mathbb{R}}} \dots$$

To any pro-Euclidean lattice  $\widehat{E} := (\widehat{E}, E_{\mathbb{R}}^{\text{Hilb}}, \|\cdot\|)$ , we may attach some infinite dimensional generalizations of the invariant  $h_\theta^0(\overline{E})$  previously defined for finite

dimensional Euclidean lattices. Notably we may consider the invariant in  $[0, +\infty]$  defined as:

$$h_\theta^0(\widehat{E}) := \log \sum_{v \in \widehat{E} \cap E_{\mathbb{R}}^{\text{Hilb}}} e^{-\pi \|v\|^2}.$$

**Theorem 3.** *For any projective system of Euclidean lattices  $\overline{E}_\bullet$  as in (2) above, if there exists some  $\delta \in \mathbb{R}_+^*$  such that*

$$\sum_{i \in \mathbb{N}} h_\theta^0(\overline{\ker q_i} \otimes \overline{\mathcal{O}}(\delta)) < +\infty,$$

then the pro-Euclidean lattice  $\varprojlim \overline{E}_\bullet$  satisfies

$$h_\theta^0(\varprojlim \overline{E}_\bullet) = \lim_{i \rightarrow +\infty} h_\theta^0(\overline{E}_i) < +\infty.$$

In Diophantine geometry, notably in transcendence theory, one often encounters problems and constructions that involve some formal geometry over a number field, or over its ring of integers, together with some complex analysis. The pro-Euclidean lattices and their  $\theta$ -invariants  $h_\theta^0$  are precisely devised to investigate the combination of such formal and analytic data.

## REFERENCES

- [Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.*, 296(4):625–635, 1993.
- [Bos15] J.-B. Bost. Theta invariants of Euclidean lattices an infinite-dimensional hermitian vector bundles over arithmetic curves. *ArXiv: 1512.08946 [math.NT]*, 2015.
- [Gro01] R. P. Groenewegen. An arithmetic analogue of Clifford’s theorem. *J. Théor. Nombres Bordeaux*, 13(1):143–156, 2001. 21st Journées Arithmétiques (Rome, 2001).
- [Hec17] E. Hecke. Über die Zetafunktion beliebiger algebraischer Zahlkörper. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.*, 1917:77–89, 1917.
- [Man85] Yu. I. Manin. New dimensions in geometry. In *Workshop Bonn 1984 (Bonn, 1984)*, volume 1111 of *Lecture Notes in Math.*, pages 59–101. Springer, Berlin, 1985.
- [MO90] J. E. Mazo and A. M. Odlyzko. Lattice points in high-dimensional spheres. *Monatsh. Math.*, 110(1):47–61, 1990.
- [Roe93] D. Roessler. The Riemann-Roch theorem for arithmetic curves. Diplomarbeit, ETH Zürich, 1993.
- [Sch31] F. K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik  $p$ . *Math. Z.*, 33:1–32, 1931.
- [Szp85] L. Szpiro. Degrés, intersections, hauteurs. *Astérisque*, (127):11–28, 1985.
- [vdGS00] G. van der Geer and R. Schoof. Effectivity of Arakelov divisors and the theta divisor of a number field. *Selecta Math. (N.S.)*, 6(4):377–398, 2000.
- [Wei39] A. Weil. Sur l’analogie entre les corps de nombres algébriques et les corps de fonctions algébriques. *Rev. Sci.*, 77:104–106, 1939.

## Arithmetic surfaces and successive minima

CHRISTOPHE SOULÉ

1) Let  $F$  be a number field,  $O_F$  its ring of integers, and  $S = \text{Spec}(O_F)$ . Consider a semi-stable curve  $f : X \rightarrow S$  with generic fiber  $X_F$ , a geometrically connected curve over  $K$ , of genus  $g \geq 2$ . Let  $\omega = \omega_{X/S}$  be the relative dualizing sheaf of  $X$  over  $S$ . We endow  $\omega$  with its Arakelov metric [1]. Consider also an hermitian line bundle  $\bar{L} = (L, h)$  over  $X$ . We let  $d = \deg(L)$  be the degree of the restriction of  $L$  to  $X_F$ . We assume that  $d \geq 2g - 1$ . The  $O_F$ -module  $\Lambda = H^0(X, L)$  is projective of rank  $N = d + 1 - g$ . It is equipped with the  $L^2$ -metric: if  $s$  and  $t$  are two sections of  $L$  over  $X(\mathbb{C})$ ,

$$\langle s, t \rangle_{L^2} = \int_{X(\mathbb{C})} h(s(x), t(x)) dv,$$

where  $dv$  is the probability measure on  $X(\mathbb{C})$  defined by  $\omega$ .

We are interested in studying the  $O_F$ -lattice  $\bar{\Lambda} = (\Lambda, \langle \cdot, \cdot \rangle_{L^2})$ , as well as its dual:

$$\bar{\Lambda}^* = (H^1(X, \omega \otimes L^{-1})/\text{torsion}, \langle \cdot, \cdot \rangle_{L^2})$$

(Serre duality). For any integer  $k$ ,  $1 \leq k \leq N$  we let

$$\mu_k(\bar{\Lambda}) := \text{Inf} \{ \mu \in \mathbb{R} / \exists e_1, \dots, e_k \in \Lambda,$$

linearly independent in  $\Lambda \otimes F$ , and such that  $\log \|e_i\| \leq \mu$  for every  $i = 1, \dots, k$  \}.

We define similarly  $\mu_k(\bar{\Lambda}^*)$ .

On the other hand, if  $\bar{M}_1$  and  $\bar{M}_2$  are two hermitian line bundles on  $X$ , we denote by  $\bar{M}_1 \cdot \bar{M}_2 \in \mathbb{R}$ , the arithmetic intersection number of  $\bar{M}_1$  and  $\bar{M}_2$ , a number introduced by Arakelov [1] and, in this generality, by Deligne.

Our goal is to bound the successive minima  $\mu_k(\bar{\Lambda})$  and  $\mu_k(\bar{\Lambda}^*)$  by means of arithmetic intersection numbers.

2) It follows from the definitions that

$$\mu_1(\bar{\Lambda}) \leq \mu_2(\bar{\Lambda}) \leq \dots \leq \mu_N(\bar{\Lambda}).$$

Furthermore, the second Minkowski's theorem (extended to number fields by Bombieri and Vaaler) asserts that  $\mu_1(\bar{\Lambda}) + \dots + \mu_N(\bar{\Lambda})$  is (essentially) equal to  $-\widehat{\deg}(\bar{\Lambda})$ , the opposite of the arithmetic degree .

The arithmetic Riemann-Roch theorem computes  $\widehat{\deg}(\bar{\Lambda})$  in terms of arithmetic intersection numbers (at least if  $H^1(X, L)$  is torsion-free):

$$\widehat{\deg}(\bar{\Lambda}) = \frac{\bar{L}^2}{2} - \frac{\bar{\omega} \cdot \bar{L}}{2} + \frac{\bar{\omega}^2}{12} + C_\infty,$$

where  $C_\infty$  is an analytic constant.

3) The numbers  $\mu_k(\bar{\Lambda})$  and  $\mu_{N+1-k}(\bar{\Lambda}^*)$  are essentially equal, so the following result can be viewed as an upper bound for  $\mu_k(\bar{\Lambda})$ .



**Theorem 1.** [2, 3]: Let  $\bar{L} = \bar{\omega}^{\otimes n+1}$ ,  $n \geq 1$ . Assume  $k < (g-1)n$ . Then

$$\mu_k(\bar{\Lambda}^*) \geq \frac{k+n}{4g(g-1)} \frac{\bar{\omega}^2}{[F:\mathbb{Q}]} - C(g, n).$$

4) Assume  $d = \deg(L)$  is even and let

$$n = d - 2g + 2.$$

**Theorem 2.** [4]

$$\mu_{\frac{d}{2}+1}(\bar{\Lambda}^*) \geq \frac{(\bar{\omega} - \bar{L})^2}{2n[F:\mathbb{Q}]} - C(g, d).$$

5) Assume  $d \geq 2g + 1$ . Let

$$\mu(\bar{\Lambda}) = \frac{\mu_1(\bar{\Lambda}) + \dots + \mu_N(\bar{\Lambda})}{N}.$$

**Theorem 3.** [5]

$$\frac{\bar{L}^2}{[F:\mathbb{Q}]} + 2d\mu(\bar{\Lambda}) \geq \frac{2dg(d-2g)}{d^2 + d - 2g^2} (\mu(\bar{\Lambda}) - \mu_1(\bar{\Lambda})) - C_\infty.$$

#### REFERENCES

- [1] Arakelov, S.Ju. Intersection theory of divisors on an arithmetic surface. Math. USSR, Izv. 8(1974), 1167-1180 (1976), translation from Izv. Akad. Nauk SSSR, Ser. Mat. 38, 1179-1192 (1974)
- [2] Soulé, C. A vanishing theorem on arithmetic surfaces. Invent. Math. 116, No.1-3, 577-599 (1994)
- [3] Soulé, C. Secant varieties and successive minima. J. Algebr. Geom. 13, No.2, 323-341 (2004)
- [4] Soulé, C. Semi-stable extensions on arithmetic surfaces, in Moduli Spaces and Arithmetic Geometry (Kyoto 2004), Advanced Studies in Pure Maths., 45, 283-295 (2006)
- [5] Soulé, C. Successive minima on arithmetic varieties, Compo.Math. 96, 85-98 (1995).

### Perfect forms over CM quartic fields

DAN YASAKI

Let  $F$  number field, with ring of integers  $\mathcal{O}$ , and let  $n$  be a positive integer. A *perfect* form over  $F$  is form that is uniquely determined by its arithmetic minimum and set of minimal vectors. For fixed  $F$  and  $n$ , there are finitely many perfect  $n$ -ary forms up to the equivalence of  $\mathrm{GL}_n(\mathcal{O})$ . Work of Voronoi [8], generalized by Ash [1] and Koecher [6], gives an algorithm for computing explicit representatives for each equivalence class. The representatives give rise to a decomposition of the symmetric space  $X$  associated to the real points of the restriction of scalars of the general linear group over  $F$ . One first identifies  $X$  with a cone  $C$  of forms up to homothety. Then there is a collection  $\Sigma$  of polyhedral cones so that

$$\bigcup_{\sigma \in \Sigma} \sigma \cap C = C,$$

and  $\Sigma$  gives a reduction theory in the following sense.

- (1) There are finitely many  $\mathrm{GL}_n(\mathcal{O})$ -orbits in  $\Sigma$ .
- (2) Each  $y \in C$  is contained in a unique open cone in  $\Sigma$ .
- (3) For each  $\sigma \in \Sigma$  with  $\sigma \cap C \neq \emptyset$ , the stabilizer of  $\sigma$  is finite.

The codimension 0 cones in  $\Sigma$  can be described in terms of perfect forms over  $F$ . The collection  $\Sigma$  induces a tessellation of  $X$ .

The tessellation allows one to compute the Voronoi complex that can be used to explicitly compute certain spaces of cuspidal automorphic forms on  $\mathrm{GL}_2$ . For  $n = 2$  and  $F = \mathbb{Q}$ , the tessellation is the well-known triangulation of the upper half-plane given by the  $\mathrm{SL}_2(\mathbb{Z})$ -orbit of the ideal triangle with vertices at 0, 1, and  $\infty$ . Similar tessellations have been computed by Cremona and his students [2, 3, 7] for hyperbolic 3-space for the purposes of computing Bianchi modular forms, the case where  $F$  is a complex quadratic field.

There has not been many computations done for CM quartic fields. See [4, 9] for  $\mathbb{Q}(\zeta_5)$  and [5] for  $\mathbb{Q}(\zeta_{12})$ . The current project classifies perfect forms up to equivalence for 26 different CM quartic fields as a first step to explore cuspidal automorphic forms on  $\mathrm{GL}_2$  over these other fields.

#### REFERENCES

- [1] A. Ash, *Deformation retracts with lowest possible dimension of arithmetic quotients of self-adjoint homogeneous cones*, Math. Ann. **225** (1977), no. 1, 69–76.
- [2] J. Bygott, *Modular forms and modular symbols over imaginary quadratic fields*, Ph.D. thesis, Exeter, 1999.
- [3] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324.
- [4] P. E. Gunnells, F. Hajir, and D. Yasaki, *Modular forms and elliptic curves over the field of fifth roots of unity*, Exp. Math. **22** (2013), no. 2, 203–216, With an appendix by Mark Watkins.
- [5] Andrew Jones, *Modular Elliptic Curves over the Field of Twelfth Roots of Unity*, [arXiv:1505.01812](https://arxiv.org/abs/1505.01812) [math.NT]
- [6] M. Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I*, Math. Ann. **141** (1960), 384–432.
- [7] M. Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, Nottingham, 2005.
- [8] G. Voronoï, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. **133** (1908), 97–178.
- [9] D. Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), no. 11, 4132–4142.

### Fundamental domains of arithmetic quotients of reductive groups

TAKAO WATANABE

Let  $G$  be a connected reductive algebraic group defined over a number field  $k$ . Assume  $G$  is  $k$ -isotropic. A domain  $\Omega$  in the adèle group  $G(\mathbb{A})$  is called a fundamental domain (abbreviated as f.d.) for  $G(k)\backslash G(\mathbb{A})$  if  $\Omega$  is contained in the closure  $(\Omega^\circ)^-$  of the interior  $\Omega^\circ$  of  $\Omega$ ,  $G(k)(\Omega^\circ)^- = G(\mathbb{A})$  and  $\gamma\Omega^\circ \cap (\Omega^\circ)^-$  is empty for all  $\gamma \in G(k) \setminus \{e\}$ . Our purpose is to construct a f.d. for  $G(k)\backslash G(\mathbb{A})^1$ , where  $G(\mathbb{A})^1 = \{g \in G(\mathbb{A}) : |\chi(g)|_{\mathbb{A}} = 1 \text{ for } \forall \chi \in \mathrm{Hom}_k(G, G_m)\}$ . Fix a maximal

$k$ -parabolic subgroup  $P \subset G$ . Denote by  $Z$  a maximal central  $k$ -split torus of  $G$  and by  $K$  a maximal compact subgroup of  $G(\mathbb{A})$ . We choose a generator  $\alpha_P \in \text{Hom}_k(P/Z, G_m)$  appropriately and then define the height  $H_P : G(\mathbb{A}) \rightarrow \mathbb{R}_{>0}$  by  $H_P(pk) = |\alpha_P(p)|_{\mathbb{A}}^{-1}$  for  $p \in P(\mathbb{A}), k \in K$ . The arithmetical minimum  $\mathfrak{m}_P(g)$  for  $g \in G(\mathbb{A})^1$  is defined to be  $\min_{x \in X_P} H_P(xg)$ , where  $X_P$  denotes  $P(k) \backslash G(k)$ . Then  $X_P(g) = \{x \in X_P : \mathfrak{m}_P(g) = H_P(xg)\}$  is a finite subset of  $X_P$  by Northcott's theorem. Denote by  $R_1$  the domain  $\{g \in G(\mathbb{A})^1 : X_P(g) = \{\bar{e}\}\}$  in  $G(\mathbb{A})^1$ , where  $\bar{e} \in X_P$  is the trivial class. Let  $R_1^-$  denote the closure of  $R_1$  in  $G(\mathbb{A})^1$ . Our results are stated as follows:

- (1)  $R_1$  is an open  $P(k)$  invariant set,  $G(k)R_1$  is dense in  $G(\mathbb{A})^1$  and  $G(k)R_1^- = G(\mathbb{A})^1$ .
- (2) For  $\gamma \in G(k)$ ,  $\gamma R_1 \cap R_1^-$  is nonempty if and only if  $\gamma \in P(k)$ .
- (3) If  $\Omega_P$  is a f.d. for  $P(k) \backslash R_1^-$ , then  $\Omega_P$  yields a f.d. for  $G(k) \backslash G(\mathbb{A})^1$  and any local maximum of  $\mathfrak{m}_P$  is attained on the boundary  $\partial\Omega_P \cap \partial R_1$ .

In the case of  $G = \text{GL}_n$ , we can construct  $\Omega_P$  explicitly. In particular, if  $P$  is a maximal parabolic subgroup whose Levi subgroup is isomorphic with  $\text{GL}_1 \times \text{GL}_{n-1}$ , then  $\Omega_P$  yields a generalization of Korkine–Zolotarev reduction domain.

#### REFERENCES

- [1] T. Watanabe, *Ryshkov domains of reductive algebraic groups*, Pacific J. Math. **270** (2014), 237–255.
- [2] L. Weng, *Fundamental domains of arithmetic quotients of reductive groups over number fields (with Appendix by Takao Watanabe)*, preprint, 2015.

### Practical computation of Hecke operators

MATHIEU DUTOUR-SIKIRIĆ

The computation of automorphic forms for a group  $\Gamma$  is a major problem in number theory. The only known computational way to approach the higher rank cases is by computing the action of Hecke operators on the cohomology (see [1]).

Henceforth, we consider the explicit computation of the cohomology by using cellular complexes invariant under the group. For the group  $\text{GL}_n(\mathbb{Z})$  there are many possible invariant complexes:

- The perfect form theory (Voronoi I) for lattice packings (full face lattice known for  $n \leq 7$ , perfect domains known for  $n \leq 8$ )
- The central cone compactification (Igusa & Namikawa) (Known for  $n \leq 6$ )
- The  $L$ -type reduction theory (Voronoi II) for the Delaunay tessellations (Known for  $n \leq 5$ )
- The  $C$ -type reduction theory (Ryshkov & Baranovski) for edges of Delaunay tessellations (Known for  $n \leq 5$ )
- The Minkowski reduction theory it uses the successive minima of a lattice to reduce it (Known for  $n \leq 7$ ) not face-to-face.
- Venkov's reduction theory also known as Igusa's fundamental cone (finiteness proved by Crisalli and Venkov)

Thus the Voronoi I decomposition known as perfect form is the most appropriate from the computational viewpoint. For an element  $g$  in  $GL_n(\mathbb{Q})$  we can consider the action on the perfect form cellular complex. For rank 1 extreme rays the action can be done trivially. For higher dimensional faces, this is more complex and requires the solution of linear system over the full cellular complex. This approach generalizes the one of [2] and can in principle be applied to a ring of integers.

The solution of such large systems becomes problematic. As it turns out we need methods for finding sparse solution of linear systems. Here we use the approach of Compressed Sensing where this problem is named “basis pursuit” and implemented the approach of [3] in C++.

For the exceptional symplectic group  $Sp_4(\mathbb{Z})$  there exist a special complex on which the group acts (see [4] for details). We then explain how the element of  $Sp_4(\mathbb{Q})$  can be made to act on this complex and allow to find the Hecke operators.

#### REFERENCES

- [1] W. Stein, *Modular forms, a computational approach*, Graduate Series in Mathematics, 2007.
- [2] P.E. Gunnells, *Computing Hecke Eigenvalues Below the Cohomological Dimension*, Experimental Mathematics 9-3 (2000) 351–367.
- [3] D.L. Donoho, A. Maleki, A. Montanari, *Message Passing Algorithms for Compressed Sensing*, PNAS **106** (2009) 18914–18919.
- [4] R. MacPherson and M. McConnell, *Explicit reduction theory for Siegel modular threefolds*, Invent. Math. **111** (1993) 575–625.

### One-class genera of positive definite Hermitian forms

MARKUS KIRSCHMER

Let  $E/K$  be a CM-extension of number fields with non-trivial Galois automorphism  $\bar{\phantom{x}}: E \rightarrow E$ . Let  $V$  be a vector space over  $E$  of rank  $m \geq 3$  equipped with a definite hermitian form  $\Phi: V \times V \rightarrow E$ , i.e.

- $\Phi(ax + x', y) = a\Phi(x, y) + \Phi(x', y)$  for all  $a \in E$  and  $x, x', y \in V$ .
- $\Phi(x, y) = \overline{\Phi(y, x)}$  for all  $x, y \in V$ .
- $\Phi(x, x)$  is totally positive for all non-zero  $x \in V$ .

Let  $\mathfrak{o}, \mathcal{O}$  be the maximal orders of  $K$  and  $E$  respectively. Two lattices in  $(V, \Phi)$ , i.e. finitely generated  $\mathcal{O}$ -submodules of  $V$  of full rank, are said to be in the same genus if their completions are isometric everywhere. The *genus*  $\text{gen}(L)$  of a lattice  $L$  consists of finitely many isometry classes, say represented by  $L_1, \dots, L_{h(L)}$ . The goal of this talk is to describe a method to enumerate the lattices  $L$  with class number  $h(L) \leq B$  for some small integer  $B$ . In particular, for  $B = 1$  this yields the one-class genera i.e. the lattices for which the local-global principle holds. The method depends on (1) some reduction maps and (2) Siegel’s mass formula.

Given a prime ideal  $\mathfrak{P}$  of  $\mathcal{O}$ , we define the map  $\rho_{\mathfrak{P}}$  on the set of lattices in  $V$  by  $L \mapsto L + (\mathfrak{P}^{-1}L \cap \mathfrak{P}L^{\#})$  where  $L^{\#} = \{x \in V \mid \Phi(x, L) \subseteq \mathcal{O}\}$ . These maps have been used by Gerstein in [2] and generalize Watson’s  $p$ -maps [3]. Clearly,

$h(L) \geq h(\rho_{\mathfrak{p}}(L))$  and after rescaling and applying these maps  $\rho_{\mathfrak{p}}(L)$  repeatedly, one can assume that  $L$  is  $\mathfrak{A}$ -squarefree, i.e.

- $\mathfrak{p}L_{\mathfrak{p}}^{\#} \subseteq L_{\mathfrak{p}} \subseteq L_{\mathfrak{p}}^{\#}$  for all prime ideals  $\mathfrak{p}$  of  $\lambda$ .
- $\mathfrak{A} \subseteq \{\Phi(x, y) \mid x, y \in L\} \subseteq \mathcal{O}$  where  $\mathfrak{A}$  is an integral ideal of  $\mathcal{O}$  that only depends on (the narrow class group of)  $K$ .

So the main problem is to enumerate the  $\mathfrak{A}$ -squarefree lattices  $L$  with  $h(L) \leq B$ .

The *mass* of  $L$  is the rational number  $\text{mass}(L) := \sum_{i=1}^{h(L)} \frac{1}{\#\text{Aut}(L_i)}$  where  $\text{Aut}(L_i)$  denotes the stabilizer of  $L_i$  in the unitary group of  $(V, \Phi)$ . Siegel’s celebrated mass formula shows that  $\text{mass}(L)$  can be expressed as follows:

$$\text{mass}(L) = 2^{1-m[K:\mathbb{Q}]} \cdot \prod_{i=1}^m \mathcal{L}(\chi^i, 1-i) \cdot \prod_{\mathfrak{p}} \lambda(L_{\mathfrak{p}}).$$

Here  $\chi$  be the non-trivial character of  $\text{Gal}(E/K)$  and  $\mathcal{L}(\chi^i)$  is the  $L$ -series with character  $\chi^i$ . The local factors  $\lambda(L_{\mathfrak{p}})$  are known in almost all cases, c.f. [1] for details. In the talk we will see how to compute the local factors for squarefree lattices which are not already known.

Siegel’s mass formula and the analytic class number formula show that

$$(*) \quad B \geq \#\mu(E) \cdot \text{mass}(L) \geq c_m \cdot \text{disc}_K^{(m^2-1)/2} \cdot \underbrace{\text{Nr}_{K/\mathbb{Q}}(\text{disc}_{E/K})^{m'-1/2} \cdot \prod_{\mathfrak{p}} \lambda(L_{\mathfrak{p}})}_{\geq 1}.$$

Here  $\mu(E)$  is the group of roots of unity in  $E$ ,  $m' = m(m - (-1)^m)/4$ ,  $c_m$  is a constant,  $\text{disc}_K$  is the absolute value of the discriminant of  $K$  and  $\text{disc}_{E/K}$  is the relative discriminant of  $E/K$ .

- (1) Eq. (\*) yields an upper bound on  $\text{disc}_K$  and thus all possible base fields  $K$ .
- (2) For  $K$  fixed, eq. (\*) leaves only finitely many possibilities for  $\text{disc}_{E/K}$ . Using class field theory, this gives all possible extensions  $E/K$ .
- (3) For  $E$  and  $K$  fixed, eq. (\*) leaves only finitely many possibilities for  $\{\mathfrak{p} \mid \lambda(L_{\mathfrak{p}}) > 1\}$  since  $\lambda(L_{\mathfrak{p}}) > \text{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{m-1}/2$  if  $\lambda(L_{\mathfrak{p}}) > 1$ . This gives finitely many possibilities for the genus of  $L$ .

### REFERENCES

[1] W. T. Gan and J.-K. Yu, *Group schemes and local densities.*, Duke Math. J., **105** (2000), 497–524.  
 [2] L. Gerstein, *The growth of class numbers of quadartic forms*, Amer. J. Math. **94** (1972), 221–236.  
 [3] G. L. Watson, *The class number of a positive definite quadratic form*, Proceedings of the LMS, **13** (1963), 549–576.

## Simultaneous computation of Hecke operators

SEBASTIAN SCHÖNNENBECK

Let  $G$  be a connected semisimple linear algebraic group defined over  $\mathbb{Q}$  such that  $G(\mathbb{R})$  is compact. We fix an open and compact subgroup  $K \leq G(\mathbb{A}_f)$  and a  $\mathbb{Q}$ -rational representation  $V$  of  $G$  (where  $\mathbb{A}_f$  denotes the finite adeles of  $\mathbb{Q}$ ). Following Gross (cf. [1]) we define the space of algebraic modular forms of level  $K$  and weight  $V$  as follows:

$$M(V, K) := \left\{ f : G(\mathbb{A}_f) \rightarrow V \mid \begin{array}{l} f(g\gamma k) = gf(\gamma) \text{ for } \gamma \in G(\mathbb{A}_f), \\ g \in G(\mathbb{Q}), k \in K \end{array} \right\}.$$

This is a finite-dimensional vector space which comes equipped with an action of the Hecke algebra  $H_K = H(G, K)$  of compactly supported  $K$ -bi-invariant functions on  $G(\mathbb{A}_f)$  (with multiplication given by convolution). With respect to the natural basis of characteristic functions on double cosets of  $K$  this action is given as follows: For  $\gamma \in G(\mathbb{A}_f)$  we decompose  $K\gamma K = \bigsqcup_i \gamma_i K$  and thus get the operator  $T(\gamma) = T(K\gamma K)$  acting via

$$(T(\gamma)f)(x) = \sum_i f(x\gamma_i).$$

As long as the group  $G$  is sufficiently well-behaved it is possible to explicitly compute these double coset decompositions and thus determine the action of  $H_K$  on  $M(V, K)$  (cf. the talk of Joshua Lansky and David Pollack as well as their article [2]). Here we want to present an approach using the adjacency relation in the local affine buildings of  $G$  to compute the action of several Hecke operators at once.

To that end let now  $K_1$  and  $K_2$  be two open and compact subgroups of  $G(\mathbb{A}_f)$ . We fix coset representatives  $K_1 = \bigsqcup_i l_i(K_1 \cap K_2)$  and  $K_2 = \bigsqcup_j m_j(K_1 \cap K_2)$ .

**Definition 1.** (1) We define the transfer operator  $T_2^1 = T(K_1, K_2)$  via

$$T_2^1 : M(V, K_1) \rightarrow M(V, K_2), \quad (T_2^1 f)(x) = \sum_j f(xm_j).$$

(2) We define the Venkov element  $\nu_{1,2} = \nu(K_1, K_2)$  with respect to  $K_1$  and  $K_2$  as

$$\nu(K_1, K_2) = \sum_{i,j} \mathbf{1}_{l_i m_j K_1} \in H_{K_1}.$$

Note that one can equivalently think of  $T(K_1, K_2)$  as a kind of Hecke operator corresponding to the double coset  $K_2 \text{id} K_1$ .

**Lemma 1.** *The following holds:*

- (1) *The operators  $T(K_1, K_2)$  and  $T(K_2, K_1)$  are adjoint to each other with respect to suitably defined scalar products on the spaces  $M(V, K_1)$  and  $M(V, K_2)$ .*
- (2)  *$T(K_2, K_1)T(K_1, K_2)$  acts as the Hecke operator  $T(\nu(K_1, K_2))$  on the space  $M(V, K_1)$ .*

In applications it is often far less expensive to compute the operator  $T(K_1, K_2)$  than the action of an arbitrary Hecke operator in  $H_{K_1}$ . Hence if we have control over the double cosets appearing in  $\nu(K_1, K_2)$  (and their coefficients) we can potentially use this method to determine the action of the Hecke algebra. Our main result is, that we can explicitly write down the decomposition in certain situations:

**Theorem 1.** *Let  $G$  be simply connected,  $K_i = \prod_p K_{i,p}$  products of local factors with  $K_{1,p} = K_{2,p}$  for all  $p \neq q$  and  $K_{1,q}, K_{2,q}$  parahoric subgroups of  $G(\mathbb{Q}_q)$ , which contain a common Iwahori subgroup  $I$ . Let  $\widetilde{W}$  be the extended affine Weyl group and  $W_i \leq \widetilde{W}$  with  $K_{i,q} = IW_iI$ ,  $W_{1,2} = W_1 \cap W_2$  and  $[W_{1,2} \backslash W_2 / W_{1,2}]$  a system of representatives of elements of shortest lengths. Then the following holds:*

$$\nu_{1,2} = \sum_{\kappa \in [W_{1,2} \backslash W_2 / W_{1,2}]} [I(W_1 \cap {}^\kappa W_1)I : I(W_1 \cap {}^\kappa W_1 \cap W_2)I] \mathbf{1}_{K_1 \kappa K_1}.$$

A similar result still holds if  $G$  is no longer simply connected.

For simply connected groups of type  $C_n$  the method turns out to be particularly powerful and the action of the whole (local) Hecke algebra can be computed using transfer operators.

**Theorem 2.** *Let  $G$  be of type  $C_n$  simply connected,  $K_1$  as above with  $K_{1,q}$  hyperspecial. If  $K_{i,q}$ ,  $2 \leq i \leq n+1$ , runs through the  $n$  further conjugacy classes of maximal parahoric subgroups, then the corresponding elements  $\nu(K_1, K_i)$  form a minimal generating system for the local Hecke algebra  $H_{K_{1,q}}$ .*

Since  $T_2^1 T_1^2$  also constitutes a Hecke operator (acting on  $M(V, K_2)$ ) using this method in the  $C_n$  case we get  $2n$  Hecke operators (plus some additional information) out of  $n$  computations.

## REFERENCES

- [1] Benedict H. Gross, *Algebraic Modular Forms*, Israel J. Math., 113 (1999), 61–93.
- [2] Joshua Lansky and David Pollack, *Hecke algebras and automorphic forms*, Compositio Math., 130 (2002), 21–48.

## Perfect forms of rank $\leq 8$ , triviality of $K_8(\mathbb{Z})$ and the Kummer/Vandiver conjecture

PHILIPPE ELBAZ-VINCENT

The author is partially supported by the LabEx PERSYVAL-Lab (ANR-11-LABX-0025-01) and the ANR ARRAND.

The following work builds on previous joint work with H. Gangl and C. Soulé [4] and ongoing works with M. Dutour Sikiric and J. Martinet.

For any positive integer  $n$  we let  $\mathcal{S}_n$  be the class of finite abelian groups the order of which has only prime factors less than or equal to  $n$ .

1. VORONOÏ THEORY

Let  $N \geq 2$  be an integer. We let  $C_N$  be the set of positive definite real quadratic forms in  $N$  variables. Given  $h \in C_N$ , let  $m(h)$  be the finite set of minimal vectors of  $h$ , i.e. vectors  $v \in \mathbb{Z}^N$ ,  $v \neq 0$ , such that  $h(v)$  is minimal. A form  $h$  is called *perfect* when  $m(h)$  determines  $h$  up to scalar: if  $h' \in C_N$  is such that  $m(h') = m(h)$ , then  $h'$  is proportional to  $h$ . Denote by  $C_N^*$  the set of non-negative real quadratic forms on  $\mathbb{R}^N$  the kernel of which is spanned by a proper linear subspace of  $\mathbb{Q}^N$ , by  $X_N^*$  the quotient of  $C_N^*$  by positive real homotheties, and by  $\pi : C_N^* \rightarrow X_N^*$  the projection. Let  $X_N = \pi(C_N)$  and  $\partial X_N^* = X_N^* - X_N$ . Let  $\Gamma$  be either  $GL_N(\mathbb{Z})$  or  $SL_N(\mathbb{Z})$ . The group  $\Gamma$  acts on  $C_N^*$  and  $X_N^*$  on the right by the formula

$$h \cdot \gamma = \gamma^t h \gamma, \quad \gamma \in \Gamma, \quad h \in C_N^*,$$

where  $h$  is viewed as a symmetric matrix and  $\gamma^t$  is the transpose of the matrix  $\gamma$ . Voronoï proved that there are only finitely many perfect forms modulo the action of  $\Gamma$  and multiplication by positive real numbers [10](Thm. p.110). The following table gives the current state of the art on the enumeration of perfect forms.

rank	1	2	3	4	5	6	7	8	9
#classes	1	1	1	2	3	7	33	10916	$\geq 500000$

The classification of perfect forms of rank 8 was achieved by Dutour Sikirić, Schürmann and Vallentin in 2005 [2]. We refer to the book of Martinet [7] for more details on the results up to rank 7. Given  $v \in \mathbb{Z}^N - \{0\}$  we let  $\hat{v} \in C_N^*$  be the form defined by

$$\hat{v}(x) = (v | x)^2, \quad x \in \mathbb{R}^N,$$

where  $(v | x)$  is the scalar product of  $v$  and  $x$ . The *convex hull in  $X_N^*$*  of a finite subset  $B \subset \mathbb{Z}^N - \{0\}$  is the subset of  $X_N^*$  which is the image under  $\pi$  of the quadratic forms  $\sum_j \lambda_j \hat{v}_j \in C_N^*$ , where  $v_j \in B$  and  $\lambda_j \geq 0$ . For any perfect form  $h$ , we let  $\sigma(h) \subset X_N^*$  be the convex hull of the set  $m(h)$  of its minimal vectors. Voronoï proved in [10](§§8-15), that the cells  $\sigma(h)$  and their intersections, as  $h$  runs over all perfect forms, define a cell decomposition of  $X_N^*$ , which is invariant under the action of  $\Gamma$ . We endow  $X_N^*$  with the corresponding CW-topology.

According to [1](VII.7), there is a spectral sequence  $E_{pq}^r$  converging to the equivariant homology groups  $H_{p+q}^\Gamma(X_N^*, \partial X_N^*; \mathbb{Z})$  of the homology pair  $(X_N^*, \partial X_N^*)$ , and such that

$$E_{pq}^1 = \bigoplus_{\sigma \in \Sigma_p^*} H_q(\Gamma_\sigma, \mathbb{Z}_\sigma),$$

where  $\mathbb{Z}_\sigma$  is the orientation module of the cell  $\sigma$  and  $\Sigma_p^*$  is a set of representatives, modulo  $\Gamma$ , of the  $p$ -cells  $\sigma$  in  $X_N^*$  which meet  $X_N$ . Since  $\sigma$  meets  $X_N$ , its stabilizer  $\Gamma_\sigma$  is finite and, by [4], when  $q$  is positive, the group  $H_q(\Gamma_\sigma, \mathbb{Z}_\sigma)$  lies in  $\mathcal{S}_{N+1}$ . When  $\Gamma_\sigma$  happens to contain an element which changes the orientation of  $\sigma$ , the group  $H_0(\Gamma_\sigma, \mathbb{Z}_\sigma)$  is killed by 2, otherwise  $H_0(\Gamma_\sigma, \mathbb{Z}_\sigma) \cong \mathbb{Z}_\sigma$ . The resulting complex  $(E_{\bullet,0}^1, d_\bullet^1)$  (see [4]) will be denoted by  $\text{Vor}_\Gamma$ , and we call it the *Voronoi complex*. In [4],  $\text{Vor}_\Gamma$  has been computed for  $\Gamma = GL_N(\mathbb{Z}), SL_N(\mathbb{Z})$  up to  $N = 7$ . Due



to the number of perfect forms in rank 8, it is not possible to use this method. Fortunately, in order to get the information on  $K_8(\mathbb{Z})$ , we only need to know the 8-cells of the Voronoi complex associated to  $GL_8(\mathbb{Z})$ .

2. THE 8-DIMENSIONAL CELLS OF  $VOR_{GL_8(\mathbb{Z})}$

Using his previous work [6], Martinet has shown that one can compute all the possible sublattices of finite index associated to “well-rounded” cells. The lattices  $L$  with perfection ranks equal to  $n$  contain a unique sublattice  $L'$  generated by minimal vectors of  $L$ , and  $L'$  has a unique basis up to permutation and changes of signs. Hence the classification of minimal classes (modulo the action of  $GL_8(\mathbb{Z})$ ) coincide with the following index classification.

$i =$	1	2	3	4	$2^2$	5	6	7	8	$4 \cdot 2$	total
$n = 8$	1	4	2	4	1	1	0	0	0	0	13

Hence, there are 13 classes (modulo  $GL_8(\mathbb{Z})$ ) of 8-dimensional cells (see also the Table 1 of [3]). We can find those classes by generating randomly 8-dimensional cells from the simplicial perfect forms of rank 8 and computing their relative spectrum (see [4]). It turns out that they all have their orientations changed by their stabilizers.

**Proposition 1.** *The group  $H_8(VOR_{GL_8(\mathbb{Z})})$  is trivial modulo  $S_2$ .*

3. APPLICATION TO  $K_8(\mathbb{Z})$  AND THE KUMMER/VANDIVER CONJECTURE

Let  $Q$  (resp.  $Q_N$ ) be the category defined by Quillen [8] made of free  $\mathbb{Z}$ -modules of finite rank (resp. of rank at most  $N$ ). If  $BQ$  is the classifying space of  $Q$ , we get (by the very definition)  $K_m(\mathbb{Z}) = \pi_{m+1}(BQ)$ . We also have the Hurewicz map  $h_m : K_m(\mathbb{Z}) \rightarrow H_{m+1}(BQ, \mathbb{Z})$ , and  $H_N(BQ) \cong H_N(BQ_N)$ . Quillen (*op. cit.*) proved that there are long exact sequences

$$\begin{aligned} \cdots \rightarrow H_m(BQ_{N-1}, \mathbb{Z}) \rightarrow H_m(BQ_N, \mathbb{Z}) \rightarrow H_{m-N}(GL_N(\mathbb{Z}), St_N) \\ \rightarrow H_{m-1}(BQ_{N-1}, \mathbb{Z}) \rightarrow \cdots, \end{aligned}$$

and, according to Lee and Szczarba [5],  $H_0(GL_N(\mathbb{Z}), St_N) = 0$  when  $N \geq 1$ . From the computations of [4] and the results of the previous section, we get

**Proposition 2.** *The group  $H_9(BQ)$  is trivial modulo  $S_7$ .*

Pushing further the techniques used in [4] on the Hurewicz map  $h_8$ , we get

**Proposition 3.** *The  $p$ -torsion of the kernel of  $h_8$  is bounded by 5.*

Finally, using the fact that the  $p$ -torsion part of  $K_8(\mathbb{Z})$  is trivial if  $p$  is a regular prime (see [11]).

**Theorem 1.** *The group  $K_8(\mathbb{Z})$  is trivial.*

Let  $\mathbb{Q}(\zeta_p)$  be the cyclotomic extension of  $\mathbb{Q}$  obtained by adding  $p$ -th roots of unity and  $C$  be the  $p$ -Sylow subgroup of the class group of  $\mathbb{Q}(\zeta_p)$ . The group  $\Delta = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times$  acts upon  $C$  via the Teichmüller character  $\omega : \Delta \rightarrow (\mathbb{Z}/p)^\times$ , with  $g(x) = x^{\omega(g)}$  and  $x^p = 1$ . For all  $i \in \mathbb{Z}$  let

$$C^{(i)} = \{x \in C \text{ such that } g(x) = \omega(g)^i x \text{ for all } g \in \Delta\}.$$

The subgroup  $C^+$  of  $C$  fixed by the complex conjugation  $\mathbb{Q}(\zeta_p)$  is the direct sum of the groups  $C^{(i)}$  for  $i$  even and  $0 \leq i \leq p-3$ . The Kummer/Vandiver conjecture states (see [9]) that the groups  $C^{(i)}$  vanish for  $i$  even and  $0 \leq i \leq p-3$ . From the triviality of  $K_8(\mathbb{Z})$  we deduce.

**Corollary 1.** *The groups  $C^{(p-5)}$  are zero for all odd prime  $p$ .*

#### REFERENCES

- [1] **Brown, K.;** *Cohomology of Groups*, Graduate Texts in Mathematics **87**, Springer-Verlag, New York, 1994.
- [2] **Dutour Sikiric, M.; Schürmann, A.; Vallentin, F.;** *Classification of eight dimensional perfect forms*, Electron. Res. Announc. Amer. Math. Soc. **13** (2007), 21–32.
- [3] **Dutour Sikiric, M.; Hulek, K.; Schürmann, A.;** *Smoothness and singularities of the perfect form compactification of Ag*, Algebraic Geometry **2**(5) (2015) 642–653.
- [4] **Elbaz-Vincent, Ph.; Gangl, H.; Soulé, C.;** *Perfect forms and the cohomology of modular groups*, Advances in Math. **245** (2013), 587–624.
- [5] **Lee, R.; Szczarba, R. H.;** *On the torsion in  $K_4(\mathbb{Z})$  and  $K_5(\mathbb{Z})$* , Duke Math. J. **45** (1978), 101–129.
- [6] **Martinet, J.;** *Sur l'indice d'un sous-réseau*, in Réseaux Euclidiens, designs sphériques et formes modulaires, Monogr. Enseign. Math. **37** (2001), 163–211.
- [7] **Martinet, J.;** *Perfect Lattices in Euclidean Spaces*, Springer-Verlag, Grundlehren der Mathematischen Wissenschaften **327**, Heidelberg, 2003.
- [8] **Quillen, D.;** Higher algebraic  $K$ -theory. I. Algebraic  $K$ -theory, I: Higher  $K$ -theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972), pp. 85–147. Lecture Notes in Math., **341**, Springer, Berlin 1973.
- [9] **Soulé, C.;**  *$K$ -theory and values of zeta functions*, in Proceedings of the Workshop and Symposium: Algebraic  $K$ -theory and its applications, ICTP 1997, H. Bass, A. Kuku, C. Pedrini ed., World Scientific 1999, 255–283.
- [10] **Voronoi, G.;** *Nouvelles applications des paramètres continus à la théorie des formes quadratiques I*, J. Crelle **133** (1907), 97–178.
- [11] **Weibel, C.;** *The algebraic  $K$ -theory of rings of integers in local and global fields*. chapter 5 (pp. 139–184) in the book Handbook of  $K$ -theory, Springer-Verlag, 2005.

## The Gaussian core model in high dimensions

HENRY COHN

(joint work with Matthew de Courcy–Ireland)

In the Gaussian core model, point particles interact via a Gaussian pair potential [3]. Given a configuration  $\mathcal{C}$  of particles in  $\mathbb{R}^n$ , the *energy* of a particle  $x \in \mathcal{C}$  is given by

$$E_\alpha(x, \mathcal{C}) = \sum_{y \in \mathcal{C} \setminus \{x\}} e^{-\alpha|x-y|^2}.$$

The *energy*  $E_\alpha(\mathcal{C})$  of  $\mathcal{C}$  is the average of  $E_\alpha(x, \mathcal{C})$  over all  $x \in \mathcal{C}$ . The *density* of  $\mathcal{C}$  is the number of particles per unit volume in space. Energy and density are well-defined for periodic configurations, among others.

What are the ground states of this system? In other words, if we fix the density of  $\mathcal{C}$  to be 1 (so that the particles do not simply recede to infinity), how low can  $E_\alpha(\mathcal{C})$  reach? In low dimensions many intricate phenomena occur [2], but little is known about high dimensions.

What is known follows from an averaging argument. Specifically, the Siegel mean value theorem implies that the expected energy of a random lattice of determinant 1 is  $(\pi/\alpha)^{n/2}$ . Thus, the ground state energy is no higher than this bound. For example, the simplest case is  $\alpha = \pi$ , in which case the ground state energy is at most 1.

We prove that for fixed  $\alpha < 4\pi/e$ , the ground state energy of the Gaussian core model for density 1 and potential function  $r \mapsto e^{-\alpha r^2}$  is asymptotic to  $(\pi/\alpha)^{n/2}$  as  $n \rightarrow \infty$  (in the sense that their ratio tends to 1). Thus, the averaging argument based on the Siegel mean value theorem is asymptotically sharp for  $\alpha < 4\pi/e$ , and random lattices are the ground states. We do not know whether it is sharp for larger values of  $\alpha$ .

The proof uses the linear programming bounds from Section 9 of [1], as well as analogies with Beurling-Selberg extremal problems in analytic number theory.

#### REFERENCES

- [1] H. Cohn and A. Kumar, *Universally optimal distribution of points on spheres*, J. Amer. Math. Soc. **20** (2007), no. 1, 99–148.
- [2] H. Cohn, A. Kumar, and A. Schürmann, *Ground states and formal duality relations in the Gaussian core model*, Phys. Rev. E (3) **80** (2009), no. 6, 061116, 7 pp.
- [3] F. H. Stillinger, *Phase transitions in the Gaussian core system*, J. Chem. Phys. **65** (1976), no. 10, 3968–3974.

### Lattices from Abelian groups

LENNY FUKSHANSKY

(joint work with Albrecht Böttcher, Stephan Ramon Garcia, Hiren Maharaj)

Function field lattices were originally introduced by Rosenbloom and Tsfasman in [7], where they were studied for their good asymptotic packing density properties. This construction is reviewed in [10] as follows. Let  $F$  be an algebraic function field (of a single variable) with the finite field  $\mathbb{F}_q$  as its full field of constants. Let  $\mathcal{P} = \{P_0, P_1, P_2, \dots, P_{n-1}\}$  be the set of rational places of  $F$ . Corresponding to each place  $P_i$ , let  $v_i$  denote the corresponding normalized discrete valuation and let  $\mathcal{O}_{\mathcal{P}}^*$  be the set of all nonzero functions  $f \in F$  whose divisor has support contained in the set  $\mathcal{P}$ . Then  $\mathcal{O}_{\mathcal{P}}^*$  is an Abelian group,  $\sum_{i=1}^n v_i(f) = 0$  for each  $f \in \mathcal{O}_{\mathcal{P}}^*$ , and we let  $\deg f := \sum_{v_i(f) > 0} v_i(f) = \frac{1}{2} \sum_{i=0}^{n-1} |v_i(f)|$ . Define the homomorphism  $\phi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* \rightarrow \mathbb{Z}^n$  (here  $n = |\mathcal{P}|$ , the number of rational places of  $F$ )

by  $\phi_{\mathcal{P}}(f) = (v_0(f), v_1(f), \dots, v_{n-1}(f))$ . Then  $L_{\mathcal{P}} := \text{Image}(\phi_{\mathcal{P}})$  is a finite-index sublattice of the root lattice  $A_{n-1}$ .

We discuss an algebraic construction of lattices which generalizes the function field lattices. Given a finite Abelian group  $G$  and a subset  $S = \{g_0 := 0, g_1, \dots, g_{n-1}\}$  of  $G$ , we define the sublattice  $L_G(S)$  of  $A_{n-1}$  by

$$(1) \quad L_G(S) = \left\{ \mathbf{X} = (x_0, \dots, x_{n-1}) \in A_{n-1} : \sum_{j=1}^{n-1} x_j g_j = 0 \right\}.$$

The general problem we consider is the following.

*Investigate geometric properties of lattices  $L_G(S)$ . Specifically, what are their minimal norms and determinants? How many minimal vectors do these lattices have? Are they well-rounded? Generated by their minimal vectors? Have bases of minimal vectors? What can be said about their automorphism groups?*

The answers to these questions certainly depend on the group  $G$  and the set  $S$ . As the result of the abstract construction of function field lattices outlined above, we obtain  $L_{\mathcal{P}} = L_G(S)$ , where  $S = \{[P_i - P_0] : 0 \leq i \leq n-1\}$  is a set of divisor classes and  $G$  is the subgroup of the divisor class group  $\text{Cl}^0(F)$  generated by  $S$ . Thus, in this case  $S$  is not simply a subset of  $G$ , but a generating set for  $G$ , and lattices defined in (1) are a generalization of function field lattices. In [5], [1], [3] we addressed the questions raised above in several situations:

- The field  $F$  is the function field of an elliptic curve of a finite field, in which case  $G = S$  and the groups that can appear this way are always of the form  $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$  (with further restrictions on the pairs  $(m_1, m_2)$ ) as characterized by Rück [8].
- The Abelian group  $G$  is arbitrary, but the set  $S$  coincides with all of  $G$ ; this is a generalization of function field lattices from elliptic curves.
- The field  $F$  is a Hermitian function field, in which case the generating set  $S$  is a proper subset of the group  $G$ .

Here we state our results. For an Abelian group  $G$ , write  $L_G$  for the lattice  $L_G(G)$ . The automorphism group  $\text{Aut}(L_G)$  can be identified with a finite subgroup of  $\text{GL}_{n-1}(\mathbb{Z})$ . We also identify  $S_{n-1}$ , the group of permutations on  $n-1$  letters, with the corresponding subgroup of  $\text{GL}_{n-1}(\mathbb{Z})$  consisting of permutation matrices.

**Theorem 1** ([1]). *Let  $G$  be an Abelian group of order  $n$ . Then:*

- (1) For every  $G$ ,  $\det L_G = n^{3/2}$ .
- (2)  $|L_G| = \begin{cases} \sqrt{8} & \text{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \text{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \text{for every other } G. \end{cases}$
- (3) For  $G = \mathbb{Z}/4\mathbb{Z}$ , the lattice  $L_G$  is not well-rounded.
- (4) For every  $G \neq \mathbb{Z}/4\mathbb{Z}$ , the lattice  $L_G$  has a basis of minimal vectors.
- (5) For every  $G$ ,  $\text{Aut}(L_G) \cap S_{n-1} \cong \text{Aut}(G)$ .

As mentioned above, the lattices coming from elliptic curves via the Rosenbloom-Tsfasman construction were considered in [5] and [9], and they are a special case of

the lattices  $L_G$  in Theorem 1. In addition to these results, we also have a formula for the number of minimal vectors in lattices  $L_G$ .

**Theorem 2.** *Assume that  $n \geq 4$  and let  $\kappa$  denote the order of the subgroup  $G_2 := \{x \in G : 2x = 0\}$  of  $G$ . Then the number of minimal vectors in  $L_G$  is*

$$(2) \quad \frac{n}{\kappa} \cdot \frac{(n - \kappa)(n - \kappa - 2)}{4} + \left(n - \frac{n}{\kappa}\right) \cdot \frac{n(n - 2)}{4}.$$

The result of Theorem 2 was established for lattices from elliptic curves in [5], but the argument is the same for any lattice of the form  $L_G$ . Furthermore, we obtained bounds for the covering radii of the lattices  $L_G$ . Recall that the *covering radius* of a lattice  $L$  is defined as

$$(3) \quad \mu(L) = \inf \left\{ r \in \mathbb{R}_{>0} : \bigcup_{\mathbf{x} \in L} (B(r) + \mathbf{x}) = \text{span}_{\mathbb{R}} L \right\},$$

where  $B(r)$  is the ball of radius  $r$  centered at the origin in  $\text{span}_{\mathbb{R}} L$ . In [9], Min Sha, building on our previous results from [5], proved that

$$(4) \quad \mu(L_G) \leq \mu(A_{n-1}) + \sqrt{2},$$

where

$$\mu(A_m) = \begin{cases} \frac{1}{2} \sqrt{m + 1} & \text{if } m \text{ is odd,} \\ \frac{1}{2} \sqrt{m + 1 - 1/(m + 1)} & \text{if } m \text{ is even;} \end{cases}$$

see [4, Chap. 4, Sec. 6.1]. In [1], we derived an improvement of (4) for the case when  $G$  is a cyclic group:

$$(5) \quad \mu(L_{\mathbb{Z}/n\mathbb{Z}}) < \frac{1}{2} \sqrt{(n - 1) + 4 \log(n - 2) + 7 - 4 \log 2 + 10/(n - 1)}.$$

We also have some partial results on the properties of the lattices  $L_G(S)$  in the more general situation when  $S$  is a proper subset of  $G$  containing the identity. Suppose  $|G| = n$ ,  $|S| = m \leq n$ . Define  $\text{Aut}(G, S) := \{\sigma \in \text{Aut}(G) : \sigma(g) \in S \ \forall g \in S\}$ . Notice that every element of  $\text{Aut}(G)$  fixes 0 and permutes the other elements of  $G$ , which allows us to identify  $\text{Aut}(G)$  with a subgroup of  $S_{n-1}$ , the group of permutations on  $n - 1$  letters. Think of  $S_{m-1}$  as the subgroup of  $S_{n-1}$  consisting of all permutations of the corresponding subset  $S \setminus \{0\}$  of  $m - 1$  letters. Each element of  $\text{Aut}(G, S)$  induces a permutation of  $S$ , and hence gives rise to an element of  $S_{m-1}$ . Let us write  $\text{Aut}(G, S)^*$  for the group of permutations of  $S$  which are extendable to automorphisms of  $G$ . In other words, every element of  $\text{Aut}(G, S)^*$  is a restriction  $\sigma|_S : S \rightarrow S$  of some element  $\sigma \in \text{Aut}(G, S)$  and every element of  $\text{Aut}(G, S)$  arises as an extension  $\hat{\tau} : G \rightarrow G$  of some element  $\tau \in \text{Aut}(G, S)^*$ .

**Theorem 3** ([3]).  *$\text{Aut}(G, S)^*$  is isomorphic to a subgroup of  $\text{Aut}(L_G(S)) \cap S_{m-1}$ . If  $S$  is a generating set for  $G$ , then  $\text{Aut}(G, S)^* \cong \text{Aut}(L_G(S)) \cap S_{m-1}$ .*

More concretely, if the lattice  $L_G(S)$  comes from a Hermitian curve

$$(6) \quad y^q + y = x^{q+1}$$

over a finite field  $\mathbb{F}_{q^2}$ , where  $q$  is a prime power, we obtained some further results.

**Theorem 4** ([3]). *If  $L_G(S)$  comes from a Hermitian curve as in (6), then:*

- (1)  $|L_G(S)| = \sqrt{2q}$  and  $\det L_G(S) = \sqrt{q^3 + 1}(q + 1)^{q^2 - q}$ .
- (2) *The lattice  $L_G(S)$  is generated by minimal vectors.*
- (3) *The lattice  $L_G(S)$  contains at least  $q^7 - q^5 + q^4 - q^2$  minimal vectors.*

Additional observations on these lattices involve a connection to spherical designs. Let  $n \geq 2$ . A collection of points  $\mathbf{y}_1, \dots, \mathbf{y}_m$  on the unit sphere  $\Sigma_{n-2}$  in  $\mathbb{R}^{n-1}$  is called a *spherical  $t$ -design* for some integer  $t \geq 1$  if  $\int_{\Sigma_{n-2}} f(\mathbf{X}) d\nu(\mathbf{X}) = \frac{1}{m} \sum_{k=1}^m f(\mathbf{y}_k)$  for every polynomial  $f(\mathbf{X}) = f(X_1, \dots, X_{n-1})$  with real coefficients of degree  $\leq t$ , where  $\nu$  is the surface measure normalized so that  $\nu(\Sigma_{n-2}) = 1$ . For  $n = 2$ , this means that  $f(-1) \cdot \frac{1}{2} + f(1) \cdot \frac{1}{2} = \frac{1}{m} \sum_{k=1}^m f(y_k)$  with  $y_1, \dots, y_m \in \{-1, 1\}$ . Recall that a full-rank lattice in  $\mathbb{R}^{n-1}$  is called *strongly eutactic* if its set of minimal vectors (normalized to lie on the unit sphere) forms a spherical 2-design. Strongly eutactic lattices are of great importance in extremal lattice theory (see [6]). The lattices  $L_G$  coming from Abelian groups are full-rank sublattices of  $A_{n-1}$  and may hence be viewed as full-rank lattices in  $\mathbb{R}^{n-1}$ . For these lattices, we have the following result.

**Theorem 5** ([2]). *The lattice  $L_G$  is strongly eutactic if and only if the Abelian group  $G$  has odd order or  $G = (\mathbb{Z}/2\mathbb{Z})^k$  for some  $k \geq 1$ .*

#### REFERENCES

- [1] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. On lattices generated by finite Abelian groups. *SIAM J. Discrete Math.*, 29(1):382–404, 2015.
- [2] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. Spherical 2-designs and lattices from Abelian groups. *preprint; arXiv:1510.08804*, 2015.
- [3] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. Lattices from Hermitian function fields. *J. Algebra*, 447:560–579, 2016.
- [4] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups*. Springer-Verlag, 1988.
- [5] L. Fukshansky and H. Maharaj. Lattices from elliptic curves over finite fields. *Finite Fields Appl.*, 28:67–78, 2014.
- [6] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.
- [7] M. Y. Rosenbloom and M. A. Tsfasman. Multiplicative lattices in global fields. *Invent. Math.*, 101:687–696, 1990.
- [8] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.
- [9] M. Sha. On the lattices from elliptic curves over finite fields. *Finite Fields Appl.*, 31:84–107, 2015.
- [10] M. A. Tsfasman and S. G. Vladut. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, 1991.

### Representation numbers and their averages

RAINER SCHULZE-PILLOT

Let  $(V, Q), (W, Q')$  be positive definite quadratic spaces over  $\mathbb{Q}$  of dimensions  $m, n$  with associated symmetric bilinear forms  $B, B'$  and  $b = 2B, b' = 2B'$ , with  $B(x, x) = Q(x)$ . Let  $\Lambda$  be a  $\mathbb{Z}$ -lattice on  $V$  with Gram matrix  $A$ ,  $N$  a  $\mathbb{Z}$ -lattice on

$W$  with Gram matrix  $T$  with respect to  $B$ ,  $T = (t)$  if  $n = 1$ . The genus of  $\Lambda$  is denoted by  $\text{gen}(\Lambda)$ .

**Definition 1** (Representation numbers).

$$\begin{aligned} r(\Lambda, N) &= \#\{\phi : N \rightarrow \Lambda \mid \phi \text{ an isometric embedding} \} \\ &= \#\{X \in M_{m,n}(\mathbb{Z}) \mid {}^t X A X = T\} \\ &= r(A, T) = r(\Lambda, T). \end{aligned}$$

$r^*(\Lambda, N) = r^*(A, T)$  counts primitive representations, i.e. representations satisfying  $\Lambda \cap \mathbb{Q}\phi(N) = \phi(N)$  resp.  $X$  has elementary divisors 1.

The first part of the talk gave a survey of known results on asymptotic formulae for these representation numbers and of results about existence of representations of  $T$  by  $\Lambda$  for sufficiently large minimum of  $T$ .

The best known asymptotic results are for  $m \geq 2n + 3$  for general  $n$  (Raghavan, Kitaoka [6, 4]) and for  $m = 3, 4$  for  $n = 1$  (Kloosterman [5], Tartakovski [7], Duke/Schulze-Pillot [2], not effective for  $m = 3$ ), the best known existence results are for  $m \geq n + 3$  (Ellenberg, Venkatesh [3]) and are at present not effective.

In particular, results of either type appear to be out of reach at present for  $n > 1$  with  $m - n = 2$ .

Recently, Einsiedler, Lindenstrauss, Michel and Venkatesh announced a different type of result for the case  $m = 4, n = 2$ :

**Theorem 1** (Einsiedler, Lindenstrauss, Michel, Venkatesh, 2012). *Let  $\Lambda$  be an ideal of a maximal order in a definite quaternion algebra  $B$  over  $\mathbb{Q}$ , fix a prime  $p$  not ramified in  $B$  and  $0 < \delta < \frac{1}{2}$ .*

*Let  $-d$  run over negative fundamental discriminants with  $p$  split in  $\mathbb{Q}(\sqrt{-d})$  and  $\mathbb{Q}(\sqrt{-d}) \subseteq B$ , for each such  $d$  fix a set  $\mathcal{S}_d$  of classes of binary quadratic forms of discriminant  $-d$  with  $|\mathcal{S}_d| \geq d^\delta$ .*

*Then for  $d$  sufficiently large all  $\Lambda' \in \text{gen}(\Lambda)$  represent some  $T \in \mathcal{S}_d$ .*

*For  $\mathcal{S}_d(c) = \{T \mid \det(T) = d, c \leq \min(T) \leq d^{\frac{1}{2}-\delta}\}$  and  $c$  large enough, all  $T \in \mathcal{S}_d(c)$  are represented by all  $\Lambda' \in \text{gen}(\Lambda)$ .*

This new approach suggests to consider the following problems:

- (1) Study representations of forms in subsets  $\mathcal{S}_d$  of  $\mathcal{T}_d := \{T \mid \det(T) = d\}$  by individual  $\Lambda$  or by all  $\Lambda' \in \text{gen}(\Lambda)$ .
- (2) How many  $T \in \mathcal{T}_d$  are represented by a given  $\Lambda$ ?
- (3) What is the average  $r_{\text{av}}(\Lambda, d)$  over the  $T \in \mathcal{T}_d$  of  $r(\Lambda, T)$ ?
- (4) Can we compute the asymptotics of this average?

The  $r_{\text{av}}(\Lambda, d)$  are known from the theory of Siegel modular forms: They are the coefficients of the Koecher-Maaß Dirichlet series of the Siegel theta series of  $\Lambda$ .

To compute averages  $r_{\text{av}}(\Lambda, d) := \sum_{\det(T)=d} \frac{r(\Lambda, T)}{\#O(T)}$  over  $T$  with  $\det(T) = d$  fixed connect this to

- pairs of representations of  $d$  by two ternary  $\mathbb{Z}$ -lattices  $L_i, L_j$  associated to  $\Lambda = I_{ij}$  in the case of square determinant. (Böcherer/SP [1])
- representations of  $d$  by a ternary  $\mathfrak{o}_K$ -lattice for non square determinant  $\Delta$ , with  $K = \mathbb{Q}(\sqrt{\Delta})$ .

Since the asymptotic representation behaviour of the ternary lattices involved is known, this gives the asymptotics of  $r_{\text{av}}(\Lambda, T)$ .

In the talk I discussed the latter case, adapting an idea for a reformulation of the former case due to Hiroshi Saito. The former case can then be viewed as the degenerate case  $K = \mathbb{Q} + \mathbb{Q}$ .

A crucial tool is the following simple lemma of Skolem-Noether type which is a consequence of the classical Skolem-Noether theorem:

**Lemma 1.** *Let  $B/K$  be a central simple algebra,  $x \mapsto x^I$  an involution of the second kind with fixed field  $K_0$ . Let  $C_1$  be a commutative  $K_0$ -algebra, let  $\varphi : C_1 \rightarrow B$  an embedding (of  $K_0$ -algebras) such that  $\varphi(C_1)$  and  $K$  are linearly disjoint over  $\underline{K_0}$  (i. e.,  $\varphi(C_1) = K\varphi(C_1) \cong K \otimes_{K_0} C_1$ ), denote by  $C_2$  the centralizer in  $B$  of  $\varphi(C_1)$ . Then  $\{\alpha \in B \mid \alpha\varphi^I = \varphi\alpha, \alpha^I = \alpha\}$  is a  $K_0$ -vector space of dimension  $\dim_K(C_2)$ . In particular, if  $B$  is a division algebra there exists  $\alpha \in B$  with  $\alpha^I = \alpha$  and  $\alpha^{-1}\varphi\alpha = \varphi^I$ .*

For simplicity of notation restrict now to the case of prime determinant.

**Theorem 2.** *Let  $\Delta$  be a prime discriminant,  $D$  the definite quaternion algebra over  $\mathbb{Q}$  ramified (only) at  $p = \Delta$ ,  $K = \mathbb{Q}(\sqrt{\Delta})$ ,  $D_K = D \otimes_{\mathbb{Q}} K$ ,  $V = \{\alpha \in D_K \mid \bar{\alpha}^\tau = \alpha\}$ . Let  $R$  be a symmetric maximal order in  $D_K$  and  $\Lambda = R \cap V$ , put  $L = \{z \in \mathbb{Z}1 + 2R \mid \text{tr}(x) = 0\}$ . Let  $\Lambda_i = y_i R \tau(y_i^{-1})$  with  $y_i \in D_{K, \mathbb{A}}^\times$ ,  $n(y_i) \in \mathbb{Q}_{\mathbb{A}}^\times$  be a lattice in the genus of  $\Lambda$ , put  $L_i = y_i L y_i^{-1}$ .*

*Then for all  $d \in \mathbb{N}$  one has*

$$r_{\text{av}}^*(\Lambda_i, d) = r^*(L_i, d),$$

where  $r^*(L_i, d)$  denotes the number of  $\mathbb{Z}$ -primitive representations of  $d$  by  $L_i$ .

**Theorem 3.** *In the situation of the previous theorem one has*

$$r_{\text{av}}^*(\Lambda_i, d) = r_{\text{av}}^*(\text{span}(L_i), d) + O(d^{1 - \frac{25}{256} + \epsilon})$$

and

$$r_{\text{av}}(\Lambda_i, d) \geq C_2 d^{1 - \epsilon} \text{ for } d > C_1.$$

For  $\delta > 0$  there is a constant  $C_3 = C_3(\delta)$  with:

For all  $d \geq C_3$  with  $-d$  a fundamental discriminant

$\nu_d := \#\{T \mid \det(T) = d, r(\Lambda_i, T) \neq 0\}$  satisfies

$$\nu_d \geq (1 - \delta) \frac{h(-d)}{2^t \mu o_{\text{max}}},$$

where  $\mu = \mu(\text{gen}(\Lambda))$  is the mass of the genus of  $\Lambda$  and  $o_{\text{max}} = o_{\text{max}}(\text{gen}(\Lambda))$  the maximal order of the group of automorphisms of a lattice in the genus of  $\Lambda$ .

In particular: For  $d$  large enough a positive proportion of the classes of binary quadratic forms of discriminant  $-d$  is represented by  $\Lambda$ .



The above results lead to estimates for averages of Fourier coefficients of Siegel cusp forms of degree 2 which are obtained as Yoshida liftings of type one (lifting a pair of elliptic cusp forms) or of type two (lifting a Hilbert cusp form). These estimates are better than what one obtains by summing up estimates for the individual Fourier coefficients.

This raises the question whether similar average estimates are possible for more general Siegel modular forms. In degree 2 such a type of estimate would follow from Böcherer's conjecture and a subconvexity bound for central values of quadratic twists of the spinor zeta function of such a cusp form.

#### REFERENCES

- [1] S. Böcherer, R. Schulze-Pillot: *On a theorem of Waldspurger and on Eisenstein series of Klingen type*, *Math. Annalen* **288** (1990), 361–388
- [2] W. Duke, R. Schulze-Pillot: *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*. *Invent. Math.* **99** (1990), 49–57.
- [3] J. Ellenberg, A. Venkatesh: *Local-global principles for representations of quadratic forms*. *Invent. Math.* **171** (2008), 257–279.
- [4] Y. Kitaoka: *Modular forms of degree  $n$  and representation by quadratic forms. II*. *Nagoya Math. J.* **87** (1982), 127–146.
- [5] H.D. Kloosterman: *Asymptotische Formeln für die Fourierkoeffizienten ganzer Modulformen*. *Abh. Math. Sem. Hamburg* **5** (1927), 337–352 .
- [6] S. Raghavan: *Modular forms of degree  $n$  and representation by quadratic forms*. *Ann. of Math. (2)* **70** (1959) 446–477
- [7] W. Tartakowsky: *Die Gesamtheit der Zahlen, die durch eine positive quadratische Form  $F(x_1, x_2, \dots, x_s)$  ( $s \geq 4$ ) darstellbar sind*. I, II. *Bull. Ac. Sc. Leningrad* **7 2** (1929); 111–122, 165–196 (1929)
- [8] H. Yoshida: *Siegel's modular forms and the arithmetic of quadratic forms*, *Invent. Math.* **60** (1980), 193–248.

### The largest squarefree exception of a quaternary quadratic form

JEREMY ROUSE

The study of integers represented by positive-definite quadratic forms has a long history, beginning with Fermat's two-square theorem, and the four-square theorem of Lagrange. Tartakowski showed that if  $Q$  is a positive-definite quadratic form in four variables and  $n$  is a positive integer which is primitively represented by  $Q$  modulo  $k$  for all  $k$ , then  $n$  is represented by  $Q$  provided  $n$  is sufficiently large. The focus of the present work is to discuss how large  $n$  must be in terms of the invariants of  $Q$ . Applications of such include the universality theorems of Conway-Schneeberger, Bhargava [1], and Bhargava-Hanke [2].

Suppose that  $Q = \frac{1}{2}\vec{x}^T A \vec{x}$  is a positive-definite quaternary quadratic form, where  $A$  is a matrix with integer entries and even diagonal entries. Let  $D(Q) = \det(A)$  and  $N(Q)$  be the smallest positive integer  $N$  so that  $NA^{-1}$  has integer entries and even diagonal entries. Using the circle method, Browning and Dietmann proved [3] that if  $n \gg D(Q)^{10+\epsilon}$ , and  $n$  satisfies appropriate local conditions, then

$n$  is represented by  $Q$ . This is an improvement over the earlier work of Schulze-Pillot [4] where the bound  $n \gg N(Q)^{14+\epsilon}$  is given. The main result of the present talk is the following.

**Theorem 1.** *Let  $\epsilon > 0$ . Then there is a constant  $C_\epsilon$  so that if  $D(Q)$  is a fundamental discriminant,  $n$  is locally represented by  $Q$ , and  $n \geq C_\epsilon D(Q)^{2+\epsilon}$ , then  $n$  is represented by  $Q$ .*

The above result is ineffective in that the constant  $C_\epsilon$  cannot be explicitly given if  $\epsilon$  is small. The source of the ineffectivity is lower bounds for values of  $L$ -functions. However, for a given  $Q$ , only finitely many  $L$ -functions are involved and they can be effectively enumerated.

The method of proof is to consider the theta series  $\theta_Q(z) = \sum_{n=0}^{\infty} r_Q(n)q^n$ . This is a weight 2 modular form for  $\Gamma_0(N(Q))$  and a certain quadratic character  $\chi_{D(Q)}$ . This theta series decomposes as

$$\begin{aligned}\theta_Q(z) &= E(z) + C(z) \\ &= \sum_{n=0}^{\infty} a_E(n)q^n + \sum_{n=1}^{\infty} a_C(n)q^n.\end{aligned}$$

We have the lower bound  $a_E(n) \gg \frac{n^{1-\epsilon}}{\sqrt{D(Q)}}$  provided  $n$  is squarefree and locally represented. We can decompose  $C(z)$  as

$$C(z) = \sum_{i=1}^s c_i g_i(d_i z)$$

where the  $g_i(z)$  are normalized Hecke eigenforms. The coefficients of such a form are bounded by  $d(n)\sqrt{n}$  and so we have  $|a_C(n)| \leq C_Q d(n)\sqrt{n}$ , where  $C_Q = \sum_{i=1}^s |c_i/\sqrt{d_i}|$ .

To bound  $C_Q$ , one uses the Petersson inner product. This is a tool that was used in the work of Fomenko [5]. We develop lower-bounds for the value at  $s = 1$  of  $L(\text{Ad}^2 g_i, s)$ , which is (up to an explicit constant) equal to  $\langle g_i, g_i \rangle$ . In addition, we develop a formula for the Petersson norm of  $C(z)$  that is a quickly converging infinite series and also only involves the Fourier coefficients of  $C(z)$  at infinity. This enables us to prove that  $\langle C, C \rangle$  is bounded (independent of  $D(Q)$ ), and this gives  $C_Q \ll D(Q)^{1/2+\epsilon}$ . This yields the stated result above.

In conclusion here are two open problems. First, what is the right conjecture about the largest  $n$  that is locally represented but not represented? Is it true that such an  $n$  is  $\ll D(Q)^{1+\epsilon}$ ? Second, it would be very interesting to prove that any  $n \gg D(Q)^{2+\epsilon}$  is represented for a larger class of quadratic forms.

The talk is based on the contents of [6].

#### REFERENCES

- [1] M. Bhargava, *On the Conway-Schneeberger fifteen theorem*, Quadratic forms and their applications (Dublin, 1999), Contemp. Math., vol. 272, Amer. Math. Soc., Providence, RI, 2000, pp. 27–37. MR 1803359 (2001m:11050)

- [2] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-Theorem*, Preprint.
- [3] Timothy Browning and Rainer Dietmann. *On the representation of integers by quadratic forms*, Proc. Lond. Math. Soc. (3), 96(2):389–416, 2008.
- [4] Rainer Schulze-Pillot. *On explicit versions of Tartakovski's theorem*, Arch. Math. (Basel), 77(2):129–137, 2001.
- [5] O. M. Fomenko, *Estimates of Petersson's inner product with an application to the theory of quaternary quadratic forms*, Dokl. Akad. Nauk SSSR **152** (1963), 559–562. MR 0158874 (28 #2096)
- [6] Jeremy Rouse. *Quadratic forms representing all odd positive integers*, Amer. J. Math., 136(6):1693–1745, 2014.

## Weakly admissible lattices and primitive lattice points

MARTIN WIDMER

We generalise Skriganov's notion of (weak) admissibility for lattices to include standard lattices occurring in Diophantine approximation and algebraic number theory (e.g. ideal lattices), and we shall present a counting result for primitive lattice points in sets such as aligned boxes. The motivation for this comes from classical results due to Chalk and Erdős [4] as well as more recent work of Dani, Laurent, and Nogueira [2, 3] on inhomogeneous Diophantine approximation by primitive points.

Consider the tuple  $\mathcal{S} = (\mathbf{m}, \boldsymbol{\beta})$  where  $\mathbf{m} = (m_1, \dots, m_n) \in \mathbb{N}^n$ ,  $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in (0, \infty)^n$ , and  $n \in \mathbb{N} = \{1, 2, 3, \dots\}$ . We write

$$\underline{\mathbf{x}} = (\mathbf{x}_1, \dots, \mathbf{x}_n) \quad (\mathbf{x}_i \in \mathbb{R}^{m_i})$$

for the elements in

$$\mathbf{E} := \mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_n},$$

and  $|\cdot|$  to denote the Euclidean norm. We set

$$N := \dim \mathbf{E} = \sum_{i=1}^n m_i,$$

$$t := \sum_{i=1}^n \beta_i,$$

and we assume that  $N > 1$ . We write

$$\text{Nm}_{\boldsymbol{\beta}}(\underline{\mathbf{x}}) = \prod_{i=1}^n |\mathbf{x}_i|^{\beta_i}$$

for the multiplicative  $\boldsymbol{\beta}$ -norm on  $\mathbf{E}$ .

Let  $C \subset \mathbf{E}$  be a coordinate subspace, compatible with the structure introduced, i.e.,

$$C = \{\underline{\mathbf{x}} \in \mathbf{E}; \mathbf{x}_i = \mathbf{0} \text{ (for all } i \in I)\}$$

where  $I \subset \{1, \dots, n\}$ . We fix such a pair  $(\mathcal{S}, C)$ , and for  $\Gamma \subset \mathbf{E}$  and  $\rho > 0$  we define the quantities

$$\nu(\Gamma, \rho) := \inf\{\text{Nm}_{\beta}(\mathbf{x})^{1/t}; \mathbf{x} \in \Gamma \setminus C, |\mathbf{x}| \leq \rho\},$$

$$\text{Nm}_{\beta}(\Gamma) := \lim_{\rho \rightarrow \infty} \nu(\Gamma, \rho).$$

As usual we always interpret  $\inf \emptyset = \infty$  and  $\infty > x$  for all  $x \in \mathbb{R}$ . Special instances of the above quantities were introduced by Skriganov in [1].

By a lattice we always mean a lattice of full rank. Let  $\Lambda$  be a lattice in  $\mathbf{E}$ . We say  $\Lambda$  is a *weakly admissible* for  $(\mathcal{S}, C)$  if  $\nu(\Lambda, \rho) > 0$  for all  $\rho > 0$ . We say  $\Lambda$  is *admissible* for  $(\mathcal{S}, C)$  if  $\text{Nm}_{\beta}(\Lambda) > 0$ .

Note that weak admissibility for a lattice in  $\mathbf{E}$  depends only on the choice of  $C$  whereas admissibility depends on  $C$  and  $\beta$ . Also notice that a lattice  $\Lambda$  in  $\mathbb{R}^N$  is weakly admissible (or admissible) in the sense of Skriganov [1] if and only if  $\Lambda$  is weakly admissible (or admissible) for  $(\mathcal{S}, C)$  with  $C = \{\mathbf{0}\}$  and  $m_i = \beta_i = 1$  (for all  $1 \leq i \leq N$ ). For such lattices and aligned boxes Skriganov proved error terms for the lattice point counting problem. His error terms are surprisingly sharp with respect to the volume of the box but they involve the  $N$ -th power of the last successive minimum which makes them inappropriate for sieving, despite their slow growth in terms of the volume of the box. Moreover, Skriganov's notion of weak admissibility is too restrictive for many applications. Let us give some nontrivial examples that illustrate that our notion of weak admissibility captures new interesting cases.

Let  $\Theta \in \text{Mat}_{r \times s}(\mathbb{R})$  be a matrix with  $r$  rows and  $s$  columns and consider

$$\Lambda = \begin{bmatrix} E_r & \Theta \\ \mathbf{0} & E_s \end{bmatrix} \mathbb{Z}^{r+s} = \{(\mathbf{p} + \Theta \mathbf{q}, \mathbf{q}); (\mathbf{p}, \mathbf{q}) \in \mathbb{Z}^r \times \mathbb{Z}^s\}.$$

We take  $n = 2$ ,  $m_1 = r$ ,  $m_2 = s$  and  $C = \{(\mathbf{x}_1, \mathbf{x}_2); \mathbf{x}_2 = \mathbf{0}\}$ . Then the lattice  $\Lambda$  is weakly admissible for  $(\mathcal{S}, C)$  (for every choice of  $\beta$ ) if  $\mathbf{p} + \Theta \mathbf{q} \neq \mathbf{0}$  for every  $\mathbf{q} \neq \mathbf{0}$ . If  $\beta = (1, \beta)$  then  $\Lambda$  is admissible for  $(\mathcal{S}, C)$  if we have

$$(1) \quad |\mathbf{p} + \Theta \mathbf{q}| |\mathbf{q}|^{\beta} \geq c_{\Lambda}$$

for every  $(\mathbf{p}, \mathbf{q})$  with  $\mathbf{q} \neq \mathbf{0}$  and some fixed  $c_{\Lambda} > 0$ . The above lattice  $\Lambda$  naturally arises when considering Diophantine approximations for the matrix  $\Theta$ . Recall that the matrix  $\Theta$  is called badly approximable if (1) holds true with  $\beta = s/r$  (by Minkowski's convex body theorem  $s/r$  is the minimal possible exponent). W. M. Schmidt has shown that the Hausdorff dimension of the set of badly approximable matrices is full, i.e.,  $rs$ .

We fix a pair  $(\mathcal{S}, C)$ , and we let  $\Gamma \subset \mathbf{E}$ . We introduce the quantities

$$\lambda(\Gamma) := \inf\{|\mathbf{x}|; \mathbf{x} \in \Gamma \setminus \mathbf{0}\},$$

and

$$\mu(\Gamma, \rho) := \inf\{\lambda(\Gamma \cap C), \nu(\Gamma, \rho)\}.$$

Now we introduce the sets in which we count the lattice points. For notational reasons it is convenient to permute the coordinate tuples  $\mathbf{x}_i$  so that  $I = \{l, l + 1, \dots, n\}$  for some  $l \in \{1, \dots, n + 1\}$ , and hence

$$C = C_l = \{\mathbf{x} \in \mathbf{E}; \mathbf{x}_i = \mathbf{0} \text{ (for all } l \leq i \leq n)\}.$$

For  $\mathbf{Q} = (Q_1, \dots, Q_n) \in (0, \infty)^n$  we consider the  $\beta$ -weighted geometric mean

$$\bar{Q} = \left( \prod_{i=1}^n Q_i^{\beta_i} \right)^{1/t},$$

and we assume throughout this note that

$$Q_i \leq \bar{Q} \leq Q_j \text{ (for all } 1 \leq i < l \leq j \leq n).$$

We set

$$Q_{max} := \max_{1 \leq i \leq n} Q_i,$$

$$Q_{min} := \min_{1 \leq i \leq n} Q_i.$$

For all  $1 \leq i \leq n$  let  $\pi_i : \mathbf{E} \rightarrow \mathbb{R}^{m_i}$  be the projection defined by  $\pi_i(\mathbf{x}) = \mathbf{x}_i$ . We assume throughout that  $Z_{\mathbf{Q}} \subset \mathbf{E}$  is convex and such that for all  $1 \leq i \leq n$

$$\pi_i(Z_{\mathbf{Q}}) \subset B_{\mathbf{y}_i}(Q_i) \text{ for some } \mathbf{y}_i \in \mathbb{R}^{m_i}.$$

Here  $B_{\mathbf{y}_i}(Q_i)$  denotes the Euclidean ball in  $\mathbb{R}^{m_i}$  about  $\mathbf{y}_i$  of radius  $Q_i$ , and we write  $\underline{\mathbf{y}} = (\mathbf{y}_1, \dots, \mathbf{y}_n)$ .

Let  $\Lambda$  be a lattice in  $\mathbf{E}$  and  $\Lambda = AZ^N$  for a matrix  $A \in GL_N(\mathbb{R})$ . Note that  $\Lambda = BZ^N$  if and only if there exists  $T \in GL_N(\mathbb{Z})$  with  $B = AT$ . Moreover, with  $\gcd(\underline{\mathbf{z}}) := \gcd(z_1, \dots, z_N)$  we have  $\gcd(\underline{\mathbf{z}}) = \gcd(T\underline{\mathbf{z}})$ . Hence, we can define primitive lattice points as follows. For  $\mathbf{x} = A\underline{\mathbf{z}} \in \Lambda$  with  $\underline{\mathbf{z}} \in \mathbb{Z}^N \setminus \underline{\mathbf{0}}$  we define

$$\gcd(\mathbf{x}) := \gcd(\underline{\mathbf{z}}).$$

We say  $\mathbf{x} \in \Lambda \setminus \underline{\mathbf{0}}$  is primitive if  $\gcd(\mathbf{x}) = 1$ , and we put

$$\Lambda^* := \{\mathbf{x} \in \Lambda \setminus \underline{\mathbf{0}}; \gcd(\mathbf{x}) = 1\}.$$

We can now state our counting result.

**Theorem 1.** *Suppose  $\Lambda$  is a weakly admissible lattice for  $(\mathcal{S}, C)$ . Then there exists a constant  $c = c(N, \underline{\mathbf{y}})$  depending only on  $N$  and  $|\underline{\mathbf{y}}|$  such that for all  $\bar{Q}$  large enough we have*

$$\left| |Z_{\mathbf{Q}} \cap \Lambda^*| - \frac{\text{Vol}Z_{\mathbf{Q}}}{\zeta(N) \det \Lambda} \right| \leq c \left( \left( \frac{\bar{Q}}{\mu} \right)^{N-1} + 3^{\frac{\log(\eta\bar{Q}/\mu)}{\log \log(\eta\bar{Q}/\mu)}} \left( \frac{\bar{Q}}{\mu} \right) \right)$$

where  $\zeta(\cdot)$  denotes the Riemann zeta function,  $\mu = \mu(\Lambda, Q_{max})$ , and  $\eta = 1 + |\underline{\mathbf{y}}|/Q_{min}$ .

## REFERENCES

- [1] M. M. Skriyanov, *Ergodic theory on  $SL(n)$ , diophantine approximations and anomalies in the lattice point problem*, Invent. math. **132** (1998), 1–72.
- [2] S. G. Dani and M. Laurent and A. Nogueira *Multi-dimensional metric approximation by primitive points*, Math. Z. **279** (2015), no. 3-4, 1081–1101.
- [3] M. Laurent and A. Nogueira *Inhomogeneous approximation with coprime integers and lattice orbits*, Acta Arith. **154** (2012), no. 4, 413–427.
- [4] J. H. H. Chalk and P. Erdős, *On the distribution of primitive lattice points in the plane*, Canad. Math. Bull. **2** (1959), 91–96.

**Discriminants and the monoid of quadratic rings**

JOHN VOIGHT

We consider the natural monoid structure on the set of quadratic rings over an arbitrary base scheme and characterize this monoid in terms of discriminants [1], as follows.

Let  $R$  be a commutative ring. An  $R$ -algebra is a ring  $B$  equipped with an embedding  $R \hookrightarrow B$  of rings (mapping  $1 \in R$  to  $1 \in B$ ) whose image lies in the center of  $B$ ; we identify  $R$  with its image via this embedding. A *quadratic  $R$ -algebra* is an  $R$ -algebra  $S$  that is locally free of rank 2 as an  $R$ -module.

Let  $S$  be a quadratic  $R$ -algebra. Then  $S$  is commutative and has a unique standard involution, an  $R$ -linear map  $\sigma : S \rightarrow S$  such that  $x\sigma(x) \in R$  for all  $x \in S$ . We say  $S$  is *separable* if  $S$  is projective as an  $S \otimes_R S$ -module via  $x \otimes y \mapsto xy$ ; equivalently,  $S$  is étale over  $R$ .

Let  $\text{Quad}(R)$  be the set of isomorphism classes of quadratic  $R$ -algebras. Further, let  $\text{Quad}(R)_{\text{free}}$  be the subset of quadratic  $R$ -algebras such that  $S$  is free as an  $R$ -algebra and let  $\text{Quad}(R)_{\text{sep}}$  be the subset of quadratic separable  $R$ -algebras. If  $S \in \text{Quad}(R)_{\text{free}}$ , then  $S \simeq R[x]/(x^2 - tx + n)$  with  $t, n \in R$ , and further  $S \in \text{Quad}(R)_{\text{sep}}$  if and only if  $(x - \sigma(x))^2 = t^2 - 4n \in R^\times$ .

If  $S, T \in \text{Quad}(R)_{\text{sep}}$  with  $\sigma, \tau$  the respective standard involutions, then the ring  $S * T := (S \otimes_R T)^{\sigma \otimes \tau}$ , the fixed subring under  $\sigma \otimes \tau$ , has  $S * T \in \text{Quad}(R)_{\text{sep}}$ , so  $*$  defines a binary operation on  $\text{Quad}(R)_{\text{sep}}$  that gives  $\text{Quad}(R)_{\text{sep}}$  the structure of an abelian group of exponent 2.

**Theorem 1.** *There is a unique system of binary operations*

$$*_R : \text{Quad}(R) \times \text{Quad}(R) \rightarrow \text{Quad}(R),$$

*one for each commutative ring  $R$ , such that:*

- (i)  *$\text{Quad}(R)$  is a commutative monoid under  $*_R$ , with identity element the isomorphism class of  $R \times R$ ;*
- (ii) *The association  $R \mapsto (\text{Quad}(R), *_R)$  from commutative rings to commutative monoids is functorial in  $R$ : for each ring homomorphism  $\phi : R \rightarrow R'$ ,*

the diagram

$$\begin{array}{ccc} \text{Quad}(R) \times \text{Quad}(R) & \xrightarrow{*_R} & \text{Quad}(R) \\ \downarrow & & \downarrow \phi^* \\ \text{Quad}(R') \times \text{Quad}(R') & \xrightarrow{*_{R'}} & \text{Quad}(R') \end{array}$$

is commutative; and

(iii) If  $S, T \in \text{Quad}(R)_{\text{sep}}$  with standard involutions  $\sigma, \tau$ , then  $S *_R T$  is the fixed subring of  $S \otimes_R T$  under  $\sigma \otimes \tau$ .

A *discriminant* over  $R$  is a quadratic form  $d : L \rightarrow R$  with  $L$  an invertible (locally free rank 1)  $R$ -module such that  $d$  is a *square modulo 4*: there exists an  $R$ -linear map  $t : L \rightarrow R$  such that

$$d(x) \equiv t(x)^2 \pmod{4R}$$

for all  $x \in L$ . Let  $\text{Disc}(R)$  be the set of discriminants up to similarity; then  $\text{Disc}(R)$  is a commutative monoid under  $\otimes$ .

The map

$$\begin{aligned} \text{disc}(S) : \bigwedge^2 S &\rightarrow R \\ x \wedge y &\mapsto (x\sigma(y) - \sigma(x)y)^2 \end{aligned}$$

is a discriminant.

**Theorem 2.** *The diagram of commutative monoids*

$$\begin{array}{ccccc} \text{Quad}(R)_{\text{free}} & \longrightarrow & \text{Quad}(R) & \xrightarrow{\wedge^2} & \text{Pic}(R) \\ \downarrow \text{disc} & & \downarrow \text{disc} & & \parallel \\ \text{Disc}(R)_{\text{free}} & \longrightarrow & \text{Disc}(R) & \longrightarrow & \text{Pic}(R) \end{array}$$

is functorial and commutative with exact rows and surjective columns.

We define the *Artin-Schreier group*  $\text{AS}(R)$  to be the additive quotient

$$\text{AS}(R) = \frac{R[4]}{\wp(R)[4]} \quad \text{where} \quad \wp(R)[4] = \{n = r + r^2 \in R : r \in R\} \cap R[4]$$

and  $R[4] = \{a \in R : 4a = 0\}$ . We have a map  $i : \text{AS}(R) \hookrightarrow \text{Quad}(R)$  sending the class of  $n \in \text{AS}(R)$  to the isomorphism class of the algebra  $S = R[x]/(x^2 - x + n)$ . The group  $\text{AS}(R)$  is an elementary abelian 2-group.

**Theorem 3.** *The fibers of the map  $\text{disc} : \text{Quad}(R) \rightarrow \text{Disc}(R)$  have a unique action of the group  $\text{AS}(R)$  compatible with the inclusion  $\text{AS}(R) \hookrightarrow \text{Quad}(R)$ .*

REFERENCES

[1] John Voight, *Discriminants and the monoid of quadratic rings*, [arxiv.org/abs/1504.05228](https://arxiv.org/abs/1504.05228), 13 January 2016.

## Counting ideal lattices in $\mathbb{Z}^d$

STEFAN KÜHNLEIN

(joint work with Lenny Fukshansky, Rebecca Schwerdt)

Given a monic polynomial  $f \in \mathbb{Z}[X]$  of degree  $d$ , we denote by  $\pi_f$  the map from  $\mathbb{Z}[X]/(f) \rightarrow \mathbb{Z}^d$  sending  $[c_0 + c_1X + \cdots + c_{d-1}X^{d-1}]$  to  $(c_0, \dots, c_{d-1})$ .

A subgroup  $U$  in  $\mathbb{Z}^d$  of rank  $d$  is called an *ideal lattice* if for some monic  $f$  as above it is the image of an ideal under  $\pi_f$ .

Those ideals play a role, e.g., in Gentry's fully homomorphic encryption scheme. It might therefore be of interest to compare their frequency with that of arbitrary subgroups of full rank in  $\mathbb{Z}^d$ . Let  $a_n(d)$  be the number of all ideal lattices in  $\mathbb{Z}^d$  of index  $n$ .

It turns out that for fixed  $d$  this sequence is multiplicative, i.e. for coprime  $m, n$  we have  $a_{mn}(d) = a_m(d) \cdot a_n(d)$ .

Setting  $\zeta_d(s) := \sum_{n=1}^{\infty} \frac{a_n(d)}{n^s}$  we deduce from this multiplicativity the existence of an Euler-product decomposition. We found that  $\zeta_0(s) = 1$ ,  $\zeta_1(s) = \zeta(s)$ , the Riemann-zetafunction,  $\zeta_2(s) = \zeta(2s)\zeta(s-1)$  and  $\zeta_3(s) = \zeta(3s)\zeta(s-1)\zeta(2s-2)$ .

This shows that for  $d \leq 1$  every sublattice is an ideal lattice (which is not surprising), for  $s = 2$  the ideal lattices have positive density in the set of all lattices, and that for  $d = 3$  the number of all ideal lattices of index  $\leq N$  is  $\sim cN^2$ , while the number of all sublattices of index less than  $N$  is  $\sim c'N^3$ . These results follow from the Tauberian theorem applied to  $\zeta_d(s)$ .

For  $d \geq 1$  we guess in general

$$\zeta_d(s) = \zeta(ds) \cdot \prod_{j=1}^{d-1} \zeta(j(s-1))$$

but did not proof this yet. This always converges for  $\Re(s) > 2$ .

## On the density of cyclotomic lattices constructed from codes

PHILIPPE MOUSTROU

The *sphere packing* problem for lattices consists in finding the biggest proportion of space that can be filled by a collection of disjoint spheres having the same radius, with centers at the lattice points. This problem is solved for dimension  $n$  up to 8 and for  $n = 24$ . Here we are interested in asymptotic lower bounds for the best lattice packing when the dimension grows. Usually, these bounds come from theoretical results, and do not provide an algorithm to construct a dense lattice. A problem of interest is thus to find some *constructive* proofs of these theorems.

Let  $\Delta_n$  denote the supremum of the sphere packing density that can be achieved by a lattice in dimension  $n$ . Let us recall that Minkowski-Hlawka proved by an averaging argument that asymptotically  $\Delta_n \geq \frac{1}{2^{n-1}}$ . Later Rogers improved this bound by a linear factor. As Rush did for Minkowski-Hlawka's bound, Gaborit and



Zémor in [1] gave an "effective" proof of Roger's result: for infinitely many dimensions  $n$ , they exhibited a *finite* (although with exponential size) family of lattices, constructed from linear codes via *Construction A*, containing lattices achieving this density. Moreover in their construction the lattices afford the action of a cyclic group of order half the dimension.

Recently, Venkatesh [2] showed that for infinitely many dimensions  $n$ ,  $\Delta_n \geq \frac{n \log \log n}{2^{n+1}}$ , which is the first result improving the linear growth of the numerator. He obtained this result by considering lattices in cyclotomic fields invariant under the action of the group of roots of unity.

Here we use an adaptation of *Construction A* for cyclotomic fields in order to exhibit finite families of lattices that reach Venkatesh's density for the same sequence of dimensions. We also provide lattices with density larger than  $\frac{cn}{2^n}$  for a set of dimensions which is somewhat larger than that of Gaborit and Zémor. With some slight modifications in our construction, we obtain lattices that are moreover *symplectic*, a property of interest in the study of principally polarized abelian varieties, thus complementing the result of Autissier [3].

#### REFERENCES

- [1] Philippe Gaborit and Gilles Zémor, *On the construction of dense lattices with a given automorphisms group*, Ann. Inst. Fourier (Grenoble) **57** (2007), 1051–1062.
- [2] Akshay Venkatesh, *A note on sphere packings in high dimension*, International Mathematics Research Notices. IMRN **7** (2013), 1628–1642.
- [3] Pascal Autissier, *Variétés abéliennes et théorème de Minkowski-Hlawka*, Manuscripta Mathematica (2015).

## Vanishing criterion of automorphic forms on tube domains

TOMOYOSHI IBUKIYAMA

If sufficiently many Fourier coefficients of a Siegel modular form  $f$  vanish, then  $f$  itself vanishes. Effective version of this claim has been known by Siegel [4] and by Poor and Yuen [3]. Hilbert modular cases and Hermitian modular cases are also treated for example by Okazaki, Burgos Gil and Pacetti, and M. Klein. I gave a talk on a theoretical criterion for the vanishing of automorphic forms on general tube domains. Most of the proofs are obtained by generalizing the arguments of Poor and Yuen in [3].

### 1. FUNDAMENTAL ASSUMPTION

Let  $D$  be a tube domain. By definition, we may write  $D = V(\mathbb{R}) + \sqrt{-1}\Omega$ , where  $V(\mathbb{R})$  is a formally real Jordan algebra and  $\Omega$  is the symmetric cone  $\Omega = \{x^2; x \in V(\mathbb{R})^\times\}$  associated to  $V(\mathbb{R})$ . As well known, there are five kinds of simple formally real Jordan algebras, and  $\Omega$  are typical symmetric cones. They are

- I) real symmetric matrices,
- II) hermitian matrices,
- III) quaternion hermitian matrices,

IV)  $\mathbb{R}^n$  with an algebraic structure defined by a quadratic form of signature  $(n-1, 1)$ ,

V)  $3 \times 3$  symmetric matrices over the (real division) Cayley algebra.

We assume that there exists a semisimple algebraic group  $G$  over  $\mathbb{Q}$  such that  $G^0(\mathbb{R})/\text{center} = \text{Aut}(D)$ , where  $G^0(\mathbb{R})$  is the topological connected component of  $G(\mathbb{R})$  and  $\text{Aut}(D)$  is the group of biholomorphic automorphisms. We assume that  $G$  has a maximal parabolic  $\mathbb{Q}$ -subgroup  $P$  corresponding to the 0-dimensional boundary component of the Baily-Borel-Satake compactification. We also assume that  $\dim G > 3$  to exclude the exceptional case. The unipotent radical  $U$  of  $P$  is abelian. We put  $V = \text{Lie}(U)$ . We can regard  $V(\mathbb{R})$  as a formally real Jordan algebra. We sometimes identify  $U$  and  $V$ . We can define a natural automorphy factor  $J_k(g, Z)$  of weight  $k$  for positive integers  $k$ ,  $g \in G(\mathbb{Q})$  and  $Z \in D$ , the precise definition being omitted here. Let  $\Gamma$  be an arithmetic subgroup of  $G^0(\mathbb{Q}) = G(\mathbb{Q}) \cap G^0(\mathbb{R})$ . For any  $g \in G^0(\mathbb{Q})$ , we write

$$(f|_k[g])(Z) = J_k(g, Z)^{-1} f(gZ).$$

We may identify  $g^{-1}\Gamma g \cap U(\mathbb{R})$  as a lattice  $L'_g$  of  $V(\mathbb{R})$ . The algebra (a vector space)  $V(\mathbb{R})$  has a natural Euclidean inner product  $(*, *)$ . We define the dual lattice  $L_g$  of  $L'_g$  by

$$L_g = \{v \in V(\mathbb{Q}); (x, v) \in \mathbb{Z}\}.$$

In particular, if  $g = 1$ , we write  $L_1 = L$ . If  $f$  is a holomorphic function on  $D$  such that  $f|_k[\gamma] = f$  for all  $\gamma \in \Gamma$ , then we say that  $f$  is an automorphic form of weight  $k$ . If  $f$  is an automorphic form, then for any  $g \in G(\mathbb{Q})$ , we have a Fourier expansion

$$(f|_k g)(Z) = \sum_{T \in L_g} a_g(T) e^{2\pi i(T, Z)}.$$

By Koecher principle, we have  $a_g(T) = 0$  unless  $T \in \overline{\Omega}$ , where  $\overline{\Omega}$  is the closure of  $\Omega$  in  $V(\mathbb{R})$ . When  $f$  is a cusp form, by definition, we have  $a_g(T) = 0$  unless  $T \in \Omega$ .

## 2. KERNEL PROPERTY

A subset  $\mathcal{K} \subset \overline{\Omega}$  is called kernel if it satisfies the following conditions (1), (2), (3) (See [1], [3]).

- (1)  $\mathcal{K}$  is closed and convex, and  $\mathcal{K} = \mathbb{R}_{\geq 1}\mathcal{K}$ ,
- (2)  $0 \notin \mathcal{K}$ .
- (3)  $\mathbb{R}_{>0} \supset \Omega$ .

For a kernel  $\mathcal{K}$ , we put

$$\mathcal{K}^\sqcup = \{x \in V(\mathbb{R}); (x, y) \geq 1 \text{ for all } y \in \mathcal{K}\}.$$

Then it is known that  $(\mathcal{K}^\sqcup)^\sqcup = \mathcal{K}$  (See [1]).

For a cusp form  $f$ , we define

$$\text{supp}(f) = \{T \in L \cap \Omega; a(T) \neq 0\}.$$

We denote by  $\nu(f)$  the closed convex hull of  $\mathbb{R}_{\geq 1}\text{supp}(f)$ . We have

**Theorem 1.** *The set  $\nu(f)$  is a kernel.*

The proof is similar to the proof of the Koecher principle.

Now we put  $\phi_f(Z) = \det(Y)^{k/2}|f(Z)|$ . Here  $\det$  is the Haupt norm of the Jordan algebra  $V(\mathbb{R})$  and  $Y$  is the imaginary part of  $Z$ . It is well known that  $\phi_f(Z)$  attains the maximum on  $D$ . Also we have  $\phi_f(\gamma Z) = \phi_f(Z)$  for any  $\gamma \in \Gamma$ . Denote by  $Z_0 = X_0 + iY_0$  any point of  $D$  which attains the maximum of  $\phi_f(Z)$ . We may assume that  $Z_0$  is in a fundamental domain of  $\Gamma$ . By using Theorem 1 and a similar argument as in [3], we can show

**Theorem 2.** *We have*

$$\frac{k}{4\pi}Y_0^{-1} \in \nu(f).$$

### 3. FUNDAMENTAL DOMAIN AND CRITERION

Let  $K$  be a maximal compact subgroup of  $G^0(\mathbb{R})$  defined by the stabilizer of  $\sqrt{-1}e$ , where  $e$  is the unit of the Jordan algebra  $V(\mathbb{R})$ . As explained in [2], by Borel and Harish-Chandra, there exists a so-called Siegel set  $\mathfrak{S} \subset G^0(\mathbb{R})$  with  $\mathfrak{S}K = \mathfrak{S}$ , such that there exists a finite set  $C = \{g_i\} \subset G(\mathbb{Q}) \cap G^0(\mathbb{R})$  which satisfies

$$G^0(\mathbb{R}) = \bigcup_i \Gamma g_i \mathfrak{S} \quad (*).$$

Now we fix any function  $\phi$  on a set  $\Omega_1$  with  $\Omega \subset \Omega_1 \subset \bar{\Omega}$  which satisfies the following four conditions.

- i)  $\phi(s) \geq 0$  for  $s \in \Omega_1$  and  $\phi(s) > 0$  for  $s \in \Omega$ .
- ii)  $\phi(\lambda s) = \lambda \phi(s)$  for  $\lambda \in \mathbb{R}$  with  $\lambda > 0$ .
- iii)  $\phi(s_1 + s_2) \geq \phi(s_1) + \phi(s_2)$  for  $s_1, s_2 \in \Omega_1$ .
- iv)  $\phi(L)$  is discrete in  $\mathbb{R}$ .

Such  $\phi$  is called a type two function. There are various different choices of  $\phi$ .

**Theorem 3.** *Let  $f$  be a cusp form of weight  $k$  of  $\Gamma$  and  $\phi$  be a type two function. Then we have the following results.*

(1) *If*

$$\min_{g_i} \phi(\text{supp}(f|_k[g_i])) > \frac{k}{4\pi} \sup_{z \in D} \inf_{g \in \cup \Gamma g_i} \phi(\text{Im}(g^{-1}Z)^{-1})$$

*then  $f = 0$ .*

(2) *Put  $\phi_{\Gamma, \mathfrak{S}} = \sup_{Z \in \mathfrak{S}/K} \phi(\text{Im}(Z)^{-1})$ . If*

$$\min_{g_i} \phi(\text{supp}(f|_k[g_i])) > \frac{k}{4\pi} \phi_{\Gamma, \mathfrak{S}},$$

*then  $f = 0$ .*

In order to make this criterion work effectively, we have to solve the following problems.

### Open problems

- (1) Give exact parameters of the Siegel set  $\mathfrak{S}$  for  $\Gamma$  which satisfies (\*).
- (2) For such a Siegel set  $\mathfrak{S}$ , evaluate  $\phi_{\Gamma, \mathfrak{S}}$  for a concretely chosen  $\phi$ .

Acknowledgment: This work was supported by JSPS KAKENHI Grant Number 25247001.

### REFERENCES

- [1] A. Ash, D. Mumford, M. Rapoport, Y. Tai, *Smooth compactification of locally symmetric varieties*. Second Edition, Cambridge Univ. Press (2010) x+230 pp.
- [2] A. Borel, *Introduction aux groupes arithmétiques*, Hermann (1969), 125 pp.
- [3] C. Poor and D. S. Yuen, Linear dependence among Siegel modular forms. *Math. Ann.* 318 (2000), 205–234.
- [4] C. L. Siegel. Einführung in die Theorie der Modulformen n-ten Grades. *Math. Ann.* 116, (1939). 617–657.

### Analytic properties of some indefinite theta series

MARTIN WESTERHOLT-RAUM

Theta series

$$\theta_L(\tau) = \sum_{l \in L} \exp(2\pi i q(l)\tau), \quad \tau \in \mathbb{H} = \{\tau = x + iy \in \mathbb{C} : y > 0\}$$

for definite, integral lattices  $(L, q)$  are holomorphic modular forms. In particular,  $\theta_L$  is annihilated by the anti-holomorphic differential  $\partial_{\bar{\tau}}$ . Equivalently, it lies in the kernel of the differential operators  $y^2 \partial_{\bar{\tau}}$ , which is covariant for the slash actions of  $\mathrm{SL}_2(\mathbb{R})$  on  $\mathbb{C}(\mathbb{H})$ :

$$(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(\tau) := (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

$$y^2 \partial_{\bar{\tau}}(f|_k g) = (y^2 \partial_{\bar{\tau}} f)|_{k-2} g \quad \text{for all } g \in \mathrm{SL}_2(\mathbb{R}).$$

The indefinite case is less clear. Summing the above exponential naively over the lattice yields a non-convergent series. After choosing a majorant  $q^+$  of  $q$ , one can define a theta series

$$\theta_L^{q^+}(\tau) = \sum_{l \in L} \exp(2\pi i (q(l)x + q^+(l)iy)),$$

which converges and is a modular form in a suitable sense. Its analytic properties from the perspective of (covariant) differential operators are unclear, however. One introduces an additional variable  $z = u + iv \in L \otimes \mathbb{C}$ , and instead studies

$$\theta_L^{q^+}(\tau, z) = \sum_{l \in L} \exp(2\pi i (q(l)x + q^+(l)iy + \langle u, l \rangle + \langle iv, l \rangle^+)),$$

where  $\langle l, l' \rangle = q(l+l') - q(l) - q(l')$  and  $\langle l, l' \rangle^+$  are the bilinear forms attached to  $q$  and  $q^+$ . The behavior with respect to differentials  $\partial_z$  and  $\partial_{\bar{z}}$  is straightforwardly determined. In addition, one checks that  $\theta_L^{q^+}$  is annihilated by a Casimir operator

for the real Jacobi group  $SL_2(\mathbb{R}) \times (L \otimes \mathbb{R}^2) \tilde{\times} \mathbb{R}$ , which is an order 3 differential operator if  $\text{rk}(L) = 1$  and of order 4, otherwise.

There is another notion of indefinite theta series, which is connected to mock theta series appearing in Zwegers’s thesis. The idea is to sum over an appropriate cone  $C$  in  $L \otimes \mathbb{R}$ :

$$\text{hol}\theta_L^C(\tau) \approx \sum_{L \cap C} \exp(2\pi i q(l)\tau).$$

To give a precise definition for a non-degenerate lattice that has signature  $(\text{rk}^+(L), \text{rk}^-(L))$ , we choose vectors  $c_{i,1}, c_{i,2} \in L \otimes \mathbb{R}$  for  $1 \leq i \leq \text{rk}^-(L)$  with mutually orthogonal  $\text{span}\{c_{i,1}, c_{i,2}\}$ , and  $q(c_{i,1}) < 0, q(c_{i,2}) = 0$ . We further set  $C = \{(c_{i,1}, c_{i,2}) : 1 \leq i \leq \text{rk}^-(L)\}$ . Then

$$\text{hol}\theta_L^C(\tau, z) = \sum_L \prod_i (\text{sgn}\langle c_{i,1}, l \rangle - \text{sgn}\langle c_{i,2}, l \rangle) \exp(2\pi i (q(l)\tau + \langle z, l \rangle)).$$

We show that there is a modular completion of  $\text{hol}\theta_L^C$  in terms of  $\theta_L^{q^+}$  with  $q^+$  given by the majorant attached to the maximal negative subspace  $L^- = \text{span}\{c_{i,1} : 1 \leq i \leq \text{rk}^-(L)\}$  of  $L \otimes \mathbb{R}$ . This completion is annihilated by the above Casimir operator for the real Jacobi group, by  $\text{rk}^+(L)$  many covariant differential operators of order 1, and by  $\text{rk}^-(L)$  many order 2 covariant differential operators.

This completion can be interpreted as an extension of Schrödinger-Weil representations. In particular, we obtain a well-behaved geometric realization of a reducible, indecomposable Harish-Chandra module. In the case of reductive groups, this only occurs for induced representations and the attached Eisenstein and theta series. Can one connect indefinite theta series of the above kind to principal series of the real Jacobi group?

### From Grothendieck’s Chern classes to lattices of dimension 14 and determinant 2

JEAN LANNES

(joint work with H.-W. Henn)

Let  $R$  be a unital commutative ring with  $2 \in R^\times$ ; the theory developed by Grothendieck in his paper “Classes de Chern et représentations linéaires des groupes discrets” [1] leads to the definition of an unstable algebra over the mod 2 Steenrod algebra, let us say  $\text{Ch}_n(R)$ , and of a natural morphism

$$\gamma_{n,R} : \text{Ch}_n(R) \rightarrow H^*(GL_n(R); \mathbb{F}_2) \quad .$$

**Examples 1.** • *The morphism  $\gamma_{n,\mathbb{C}}$  identifies with the morphism*

$$H^*(\text{BGL}_n^{\text{top}}(\mathbb{C}); \mathbb{F}_2) \rightarrow H^*(\text{BGL}_n^{\text{dis}}(\mathbb{C}); \mathbb{F}_2)$$

*$\text{GL}_n^{\text{top}}(\mathbb{C})$  and  $\text{GL}_n(\mathbb{C})$  denoting the group  $\text{GL}_n(\mathbb{C})$  equipped respectively with the usual and discrete topology.*

- Similarly the morphism  $\gamma_{n,\mathbb{R}}$  identifies with the morphism

$$H^*(\mathrm{BGL}_n^{\mathrm{top}}(\mathbb{R}); \mathbb{F}_2) \rightarrow H^*(\mathrm{BGL}_n^{\mathrm{dis}}(\mathbb{R}); \mathbb{F}_2) \quad .$$

- If  $R$  is a finite field (with  $\mathrm{char}(R) \neq 2$ ), then the work of Quillen [2] implies that  $\gamma_{n,R}$  is an isomorphism. In this case the algebra  $\mathrm{Ch}_n(R)$  is not too difficult to determine; for example, for  $|R| \equiv -1 \pmod{4}$ , one checks that  $\mathrm{Ch}_n(R)$  identifies with the subalgebra of  $H^*(\mathrm{BGL}_n^{\mathrm{dis}}(\mathbb{R}); \mathbb{F}_2)$  generated by the classes  $w_k^2$  and  $\mathrm{Sq}^{k-1} w_k$ ,  $1 \leq k \leq n$ .
- One checks

$$\mathrm{Ch}_n(\mathbb{Z}[\frac{1}{2}]) \cong \mathrm{Ch}_n(\mathbb{F}_3) \otimes_{\mathrm{Ch}_n(\mathbb{C})} \mathrm{Ch}_n(\mathbb{R}) \quad .$$

QUESTION: For which  $n$  is  $\gamma_{n,\mathbb{Z}[\frac{1}{2}]}$  an isomorphism?

One knows that it is the case for  $n \leq 3$  (the case  $n = 3$ , due to Henn, is already delicate [3]). The question above led us to compare the mod 2 homology of the orthogonal groups  $O(\Lambda)$  and  $O(\mathbb{F}_3 \otimes \Lambda)$ ,  $\Lambda$  denoting a finite-dimensional free module over  $\mathbb{Z}[\frac{1}{2}]$  equipped with a positive non-degenerate symmetric bilinear form. To do this comparison we use an avatar of the Bruhat-Tits building for  $O(\mathbb{Q}_2 \otimes \Lambda)$  defined in terms of integral lattices  $L$  with  $2L^\# \subset L$  (see for example [4]). A byproduct of our study is that  $\gamma_{n,\mathbb{Z}[\frac{1}{2}]}$  is not an isomorphism for  $n \geq 14$  (the preceding record, by Bill Dwyer, was  $n \geq 32$  [5]). The technical tool to obtain this result is the proposition stated hereafter.

Let  $G$  be a discrete group endowed with an action on a CW-complex  $X$  which satisfies the following assumptions:

- $\dim X < \infty$ ;
- $\tilde{H}^*(X; \mathbb{F}_2) = 0$ ;
- the action is cellular;
- the isotropy subgroups of all cells are “uniformly” finite.

One denotes by  $X_s$  the 2-singular locus of  $X$ : the subspace of those points in  $X$  which are fixed by some element of order 2.

**Proposition 1.** *Let  $G$  and  $X$  be as above. If there exists a group homomorphism  $\alpha : G \rightarrow F$ , with  $F$  finite, which induces an isomorphism on  $H^*( ; \mathbb{F}_2)$ , then one has  $H_G^*(X, X_s; \mathbb{F}_2) = 0$ .*

#### REFERENCES

- [1] Grothendieck, A, *Classes de Chern et représentations linéaires des groupes discrets, Dix exposés sur la cohomologie des schémas*, 215-305, Adv. Stud. Pure Math., **3**, 1968.
- [2] Quillen, D., *On the cohomology and K-theory of the general linear groups over a finite field*, Ann. of Math., **96** (1972), 552-586.
- [3] Henn, H.-W., *The cohomology of  $\mathrm{SL}(3, \mathbb{Z}[\frac{1}{2}])$* , K-Theory **16** (1999), 299359.
- [4] Abramenko, P. and Nebe, G., *Lattice chain models for affine buildings of classical type*, Math. Ann., **322** (2002), 537-562.
- [5] Dwyer, W. G., *Exotic cohomology for  $\mathrm{GL}_n(\mathbb{Z}[\frac{1}{2}])$* , Proc. Amer. Math. Soc., **126** (1998), 2159-2167.

## Energy minimization and formal duality of periodic point configurations

ACHILL SCHÜRMAN

(joint work with Henry Cohn, Renaud Coulangeon, Abhinav Kumar, Christian Reiher)

Point configurations that minimize energy for a given pair potential function occur in diverse contexts of mathematics and its applications. There exist numerous numerical approaches to find locally optimal or stable configurations. However, a mathematical rigorous treatment proving optimality of a point configuration is quite difficult.

**Universal Optimality.** In [1] Cohn and Kumar introduced the notion of a universally optimal point configuration, that is, a set of points in a given space, minimizing energy for all completely monotonic potential functions. It turned out that there exist several fascinating examples among spherical point sets. Considering infinite point sets in Euclidean spaces appears more difficult though. Even a proper definition of potential energy bears subtle convergence problems. However, for *periodic sets* such problems can be avoided. These sets are a union of finitely many translates of a given full-rank lattice  $L \subset \mathbb{R}^n$  (a discrete subgroup of  $\mathbb{R}^n$ ). In particular, a full-rank-lattice  $L \subset \mathbb{R}^n$  itself is a periodic set. In general we can write  $\Lambda = \bigcup_{i=1}^N (t_i + L)$  where  $t_1, \dots, t_N$  are some vectors in  $\mathbb{R}^n$ . For a potential function  $f$ , the  $f$ -energy of  $\Lambda$  is defined as

$$(1) \quad E(f, \Lambda) = \frac{1}{m} \sum_{i=1}^N \sum_{x \in \Lambda, x \neq t_i} f(|t_i - x|).$$

A periodic point set is called *universally optimal* if it minimizes  $f$ -energy for all completely monotonic potential functions  $f$ .

**Experiments in the Gaussian Core Model.** Working with local variations of periodic sets it is often convenient to work with a parameter space up to translations and orthogonal transformations, as introduced in [5]. In [3] we undertook an experimental study of energy minima among periodic sets of low dimensions ( $n \leq 9$ ) in the *Gaussian core model*, that is, for potential functions  $g_c(r) := \exp(-\pi c r^2)$ , with  $c > 0$ . Cohn and Kumar conjectured the hexagonal lattice, the  $E_8$  root lattice and the 24-dimensional Leech lattice  $\Lambda_{24}$  to be universally optimal. Our experiments support their conjecture in dimension 2 and 8. In dimension 4, to our own surprise, numerical experiments suggest that the root lattice  $D_4$  is universally optimal as well. In all other dimensions the situation is much less clear. In dimension 3, for  $c$  in a small interval around 1, there is a *phase transition*, for which periodic point-configurations seem not to minimize energy at all. For all larger  $c > 1$  the fcc-lattice (also known as  $D_3$ ) and for all smaller  $c < 1$  the bcc-lattice (also known as  $D_3^*$ ) appear to be energy minimizers.

In dimensions 5, 6 and 7 non-lattice packings seem to minimize energies, in contrast to a conjecture of Torquato and Stillinger from 2008. In dimension 5 and 7

the conjectured optimal configurations are sets  $D_n^+(\alpha) = \{(x_1, \dots, x_{n-1}, \alpha x_n) : x \in D_n^+\}$  where  $D_n^+ = D_n \cup ((\frac{1}{2}, \dots, \frac{1}{2}) + D_n)$  is the periodic set consisting of two translates of the root lattice  $D_n$ . Unexpectedly, in dimension 9 the 2-periodic set  $D_n^+$  appears to be universally optimal.

**Local Optimality.** Even in dimension 2 a proof of universal optimality appears to be quite difficult and not yet established. In higher dimensions proofs showing optimality for a given or even all potential functions seem currently out of reach. In [4] we therefore considered a kind of local universal optimality among periodic sets. We showed that lattices whose shells are spherical 4-designs and which are locally optimal among lattices can not locally be improved to another periodic set with lower energy. (For a corresponding result for the case  $c \rightarrow \infty$  see [6].) By a result due to Sarnak and Strömbergsson, this implies local universal optimality for the  $D_4$  and the  $E_8$  root lattice, as well as for the Leech lattice  $\Lambda_{24}$ . In an ongoing project we are currently hoping to generalize this kind of local optimality for  $g_c$ -energies with large  $c$  to certain periodic sets. In particular for 2-periodic sets, whose shells are all spherical 3-designs such a result seems possible. It would imply local optimality of  $D_9^+$  (at least for large  $c$ ).

**Formal Duality.** Maybe the most interesting result of our numerical experiments, is the observation that all energy minimizing periodic sets (at least for  $n \leq 9$ ) appear to satisfy a certain kind of *formal duality*. It generalizes the familiar lattice duality, which has been known for long: If a lattice  $L$  is a minimizer for  $g_c$ -energy among lattices, then its dual lattice  $L^*$  is a minimizer for  $g_{1/c}$ -energy, due to the Poisson summation formula  $\sum_{x \in L} f(x) = \delta(L) \sum_{y \in L^*} \hat{f}(y)$ . Here  $\delta(L)$  denotes the point density of  $L$  and  $\hat{f}$  the Fourier transform of  $f$ . By a result of Córdoba the Poisson summation formula holds for all Schwartz functions only if  $L$  is a lattice. For periodic sets  $\Lambda = \bigcup_{i=1}^N (t_i + L)$  we therefore consider the *average pair sum*

$$\Sigma_f(\Lambda) := \frac{1}{N} \sum_{j,k=1}^N \sum_{z \in L} f(z + t_j - t_k)$$

instead. We say two periodic sets  $\Lambda$  and  $\Gamma$  are *formally dual* to each other if  $\Sigma_f(\Lambda) = \delta(\Lambda) \Sigma_{\hat{f}}(\Gamma)$  for every Schwartz function  $f : \mathbb{R}^n \rightarrow \mathbb{R}$ . Assuming  $\Gamma = \bigcup_{j=1}^M (s_j + K)$  with a lattice  $K$ , it can be shown that  $\Lambda - \Lambda \subseteq K^*$  and  $\Gamma - \Gamma \subseteq L^*$  in case  $\Lambda$  and  $\Gamma$  are formally dual to each other. Since the notion of formal duality is invariant towards translations, we may assume  $0 \in \Lambda, \Gamma$ , which allows us to reduce the study of formal duality to the study of finite sets in finite abelian groups: It can be shown that  $T = \{t_1, \dots, t_N\} \subseteq G = K^*/L$  and  $S = \{s_1, \dots, s_M\} \subseteq \hat{G} = L^*/K$  (respectively  $\Lambda$  and  $\Gamma$ ) are formally dual to each other if and only if

$$\left| \frac{1}{N} \sum_{j=1}^N \exp(2\pi i \langle t_j, s \rangle) \right|^2 = \frac{1}{M} \# \{(k, l) : 1 \leq k, l \leq M \text{ and } s = s_k - s_l\}$$



for every  $s \in \widehat{G}$ . As the right hand side is rational and the left hand side is usually not, it shows that formal duality among periodic sets is a rather rare phenomenon. This makes it somehow even more mysterious that energy minimizers in low dimensions all appear to have this property.

In [2] we collected all that is known about formal duality so far. Next to a reduction of the general classification to the study of finite sets in dual abelian groups, we provide a complete list of currently known primitive formally dual pairs (which are not obtained as cross-products or as cosets of proper subgroups of other formally dual sets). The lattice case  $\mathbb{Z}$ , corresponding to trivial finite sets and groups  $T = G = S = \widehat{G} = \{0\}$ , is the case of classical lattice duality. There is only one known other 1-dimensional pair of primitive formally (self-)dual sets, which we baptized TITO (for two-in-two-out). It is obtained by setting  $G = \widehat{G} = \mathbb{Z}/4\mathbb{Z}$  and  $T = S = \{0, 1\}$ . A closer investigation of the conjectured energy minimizers from our numerical experiments revealed that all of them are obtained by linear images of cross products of these basic examples! However, we found one additional family of formally dual sets (in dimension 2) which we did not observe in energy minimization problems so far: For  $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$  the sets  $S = \{(\alpha n^2, \beta n) : n \in \mathbb{Z}/p\mathbb{Z}\}$  and  $T = \{(n, n^2) : n \in \mathbb{Z}/p\mathbb{Z}\}$  are formally dual in the cyclic groups  $G = \widehat{G} = (\mathbb{Z}/p\mathbb{Z})^2$ .

**Conclusion.** Already these first steps of work on energy minimization of periodic pointsets revealed quite interesting, partially unexpected, new phenomena. We expect that improved numerical simulations could reveal a lot more, for instance a better understanding of phase transitions and a better understanding of periodic point configurations in dimensions beyond  $n = 9$ . Using the theory of generalized theta series it may be possible to prove local universal optimality of 2-periodic sets like  $D_9^+$ . The phenomenon of formal duality certainly deserves further studies. A full classification, at least in dimension 1 and 2, should be possible with additional efforts. Can someone provide an explanation why energy minimizing periodic sets appear to have this rather rare formal duality property? We hope that future work will help to shed more light on this still mysterious phenomenon.

#### REFERENCES

- [1] Henry Cohn and Abhinav Kumar, Universally optimal distribution of points on spheres, *J. Amer. Math. Soc.*, 20 (2007), 99–148.
- [2] Henry Cohn, Abhinav Kumar, Christian Reiher and Achill Schürmann, Formal duality and generalizations of the Poisson summation formula, *AMS Contemporary Mathematics*, 625 (2014), 123–140.
- [3] Henry Cohn, Abhinav Kumar and Achill Schürmann, Ground states and formal duality relations in the Gaussian core model, *Phys. Rev. E*, 80, 061116 (2009).
- [4] Renaud Coulangeon and Achill Schürmann, Energy minimization, periodic sets and spherical designs, *Internat. Math. Res. Notices*, vol. 2011, No. 4, 829–848.
- [5] Achill Schürmann, *Computational geometry of positive definite quadratic forms*, AMS, Providence, 2009.
- [6] Achill Schürmann, Strict Periodic Extreme Lattices, *AMS Contemporary Mathematics*, 587 (2013), 185–190.

## New upper bounds for the density of translative packings of superballs

MARIA DOSTERT

(joint work with Cristóbal Guzmán, Fernando Mário de Oliveira Filho, Frank Vallentin)

The sphere packing problem is one of the most famous geometric optimization problems. In materials science also densest packings of superballs  $B_3^p$  (unit balls for the  $l_3^p$ -norm) in three dimensions are of interest. Jiao, Stillinger, and Torquato [5] computed lower bounds for the maximal density of packings of superballs by using stochastic optimization and numerical simulation. Although they allowed for congruent packings, the computer simulation returned only lattice packings as candidates for maximizers.

We determine upper bounds for the maximal density of translative packings of superballs by using the infinite dimensional linear program of Cohn and Elkies [2]. It was originally designed for the packing of round spheres and until now, it was only used for this case. The rotational symmetry of a sphere allows the restriction of the optimization variable  $f$ , which has to be a continuous  $L^1$ -function, to be radial. For superballs, we cannot use this restriction. Therefore, the optimization problem is much harder to solve. Instead of optimizing over the entire space of  $L^1$ -functions, we optimize over polynomials  $p$  up to a fixed degree  $2d$  and we use  $\hat{f} = p(u)e^{-\pi\|u\|^2}$  for calculating the function  $f$  from  $p$ . We get the  $L^1$ -function  $f(x) = \int_{\mathbb{R}^n} p(u)e^{-\pi\|u\|^2} e^{2\pi i u \cdot x} dx$  and the following optimization problem

$$\begin{aligned} \vartheta^t(B_3^p) &= \inf f(0) \\ p &\in \mathbb{R}[u]_{\leq 2d} \\ p(0) &\geq \text{vol } B_3^p \\ p(x) &\geq 0 \quad \forall x \in \mathbb{R}^3 \setminus \{0\} \\ f(x) &\leq 0 \quad \forall x \notin (2B_3^p)^\circ \end{aligned}$$

By using the decomposition of  $p$  into spherical harmonics, we are able to determine  $f$  from  $p$  by solving a system of linear equations. The more difficult constraint is the nonnegativity condition, which is generally NP-hard to check. Therefore, it will be replaced by a *sum of squares* (SOS) condition, which gives a semidefinite relaxation. A polynomial  $p \in \mathbb{R}[u_1, \dots, u_n]_{\leq 2d} = \mathbb{R}[u]_{\leq 2d}$  of degree at most  $2d$  is said to be SOS, if and only if, there exist polynomials  $q_1, \dots, q_m \in \mathbb{R}[u]_{\leq d}$ , such that  $p(x) = \sum_{i=1}^m q_i^2(x)$ . The advantage of using a SOS condition is that this can be checked efficiently by using a solver for semidefinite programs (SDP). But for  $n = 3$  and  $d = 15$  the positive semidefinite matrix  $Q$  of the corresponding SDP has dimension 816, which is too large for current SDP solvers.

We can assume that the function  $f$  of Cohn-Elkies is invariant under the symmetry group of  $B_3^p$  and so we can restrict the program to polynomials which are invariant under this group. This symmetry group is the octahedral group  $B_3$ , which is a finite reflection group. Gaterman and Parrilo [3] developed an abstract

theorem to simplify the SOS condition for polynomials, which are invariant under a finite matrix group. We make this theorem concrete by considering finite reflection groups.

The invariant ring  $\mathbb{C}[x]^G$  of a finite reflection group  $G \subseteq \text{GL}_n(\mathbb{C})$  is generated by its basic invariants  $\theta_1, \dots, \theta_n$ .

$$\mathbb{C}[x]^G = \mathbb{C}[\theta_1, \dots, \theta_n]$$

The coinvariant algebra is

$$\mathbb{C}[x]_G = \mathbb{C}[x]/(\theta_1, \dots, \theta_n),$$

which is a  $|G|$ -dimensional graded algebra. In particular,

$$\mathbb{C}[x] = \mathbb{C}[x]^G \otimes \mathbb{C}[x]_G$$

holds. The action of  $G$  on  $\mathbb{C}[x]_G$  is equivalent to the regular representation of  $G$ . Let  $\widehat{G}$  be the set of irreducible representations of  $G$  up to equivalence and  $d_\pi$  be the dimension of  $\pi \in \widehat{G}$ . Then the coinvariant algebra  $\mathbb{C}[x]_G$  has a basis

$$\varphi_{ij}^\pi, \text{ with } \pi \in \widehat{G}, 1 \leq i, j \leq d_\pi,$$

of homogeneous polynomials, such that

$$g\varphi_{ij}^\pi = (\pi(g)_j)^T \begin{pmatrix} \varphi_{i1}^\pi \\ \vdots \\ \varphi_{id_\pi}^\pi \end{pmatrix}, i = 1, \dots, d_\pi,$$

holds, where  $\pi(g)_j$  is the  $j$ -th column of the unitary matrix  $\pi(g) \in U(d_\pi)$ .

For the group  $B_3$ , all irreducible unitary representation are orthogonal representations. Therefore, we can just consider real polynomials.

**Theorem** Let  $G \subseteq \text{GL}_n(\mathbb{R})$  be a finite group generated by reflections. The cone of  $G$ -invariant polynomials which can be written as sum of squares equals

$$\left\{ p \in \mathbb{R}[x] : p = \sum_{\pi \in \widehat{G}} \langle P^\pi, Q^\pi \rangle, P^\pi \text{ is a SOS matrix polynomial in } \theta_i \right\}.$$

Here  $\langle A, B \rangle = \text{Tr}(B^T A)$  denotes the trace inner product, the matrix  $P^\pi$  is an SOS matrix polynomial in the variables  $\theta_1, \dots, \theta_n$ , i.e. there is a matrix  $L^\pi$  with entries in  $\mathbb{R}[x]^G$  such that  $P^\pi = (L^\pi)^T L^\pi$  holds and  $Q^\pi \in (\mathbb{R}[x]^G)^{d_\pi \times d_\pi}$  is defined componentwise by

$$[Q^\pi]_{kl} = \sum_{i=1}^{d_\pi} \varphi_{ki}^\pi \varphi_{li}^\pi.$$

This theorem can also be formulated for the complex case, but then we have to consider complex conjugation. A Hermitian symmetric polynomial  $p \in \mathbb{C}[z, \bar{w}]$  is a *sum of Hermitian squares* if there are polynomials  $q_1, \dots, q_r \in \mathbb{C}[z]$  so that

$$p(z, \bar{w}) = \sum_{i=1}^r q_i(z) \overline{q_i(w)}$$

holds.

By using the theorem, the matrix  $Q$  can be decomposed into many smaller block matrices, and thus we are able to solve the program by using an SDP solver. Afterwards, we check whether the solution is feasible for the Cohn-Elkies theorem by using interval arithmetic to get rigorous bounds.

We can also use this approach to compute upper bounds for the density of translative packings of Platonic and Archimedean solids having tetrahedral symmetry. Zong [7] published in 2014 upper bounds for the maximal density of translative packings of tetrahedra (0.3840...) and of cuboctahedra (0.9601...), which we both improved to 0.3754... and 0.9364...

Body	Lower bound	Upper bound
Regular octahedron ( $B_3^1$ )	0.9473... [6]	0.9729...
$B_3^3$	0.8095... [5]	0.8236...
$B_3^4$	0.8698... [5]	0.8742...
$B_3^5$	0.9080... [5]	0.9224...
$B_3^6$	0.9318... [5]	0.9338...
Regular tetrahedron	0.3673... [4]	0.3745...
Truncated cube	0.9737... [1]	0.9845...
Truncated tetrahedron	0.6809... [1]	0.7292...
Rhombic cuboctahedron	0.8758... [1]	0.8794...
Truncated cuboctahedron	0.8493... [1]	0.8758...
Cuboctahedron	0.9183... [4]	0.9364...

## REFERENCES

- [1] U. Betke and M. Henk, *Densest lattice packings of 3-polytopes*, Comput. Geom. **16** (2000) 157–186.
- [2] H. Cohn and N.D. Elkies, *New upper bounds on sphere packings I*, Ann. of Math. **157** (2003), 689–714.
- [3] K. Gatermann and P.A. Parrilo, *Symmetry groups, semidefinite programs, and sums of squares*, J. Pure Appl. Algebra **192** (2004), 95–128.
- [4] H. Groemer, *Über die dichteste gitterförmige Lagerung kongruenter Tetraeder*, Monatsh. Math. **66** (1962) 12–15.
- [5] Y. Jiao, F.H. Stillinger, and S. Torquato, *Optimal packings of superballs*, Phys. Rev. E **79** (2009), 041309, 12 pp.
- [6] H. Minkowski, *Dichteste gitterförmige Lagerung kongruenter Körper*, Nachr. Ges. Wiss. Göttingen (1904), 311–355.
- [7] C. Zong, *On the translative packing densities of tetrahedra and cuboctahedra*, Adv. Math. **260** (2014) 130–190.

## Some integral perfect lattices of minimum 4

ROLAND BACHER

For  $d \geq 7$ , the  $d$ -dimension integral lattice of all integral vectors in  $\mathbb{Z}^{d+2}$  which are orthogonal to  $(1, 1, \dots, 1)$  and to  $(1, 2, 3, \dots, n+2)$  has minimum 4 and is perfect (see the monograph [2] for definitions). This construction can be relaxed by leaving a few “holes” in the vector  $(1, 2, \dots)$ . More precisely, the lattice given by all integral vectors with zero coefficient-sum and which are orthogonal to a fixed vector of the form  $(1, 2, \dots, i_1 - 1, \widehat{i_1}, i_1 + 1, \dots, \widehat{i_2}, \dots, \widehat{i_k}, \dots, d+k+2)$  is perfect if  $d \geq \max(7, 2(k+1)^3 - 1)$ , see [1, Theorem 2.2]. Moreover, all those lattices are essentially non-isomorphic, after taking into account that two vectors  $(1, 2, \dots)$  with holes in respective symmetric positions yield lattices which are obviously isometric. It follows that the number  $p_d$  of perfect  $d$ -dimensional lattices (up to similitude, of course) grows faster than any polynomial in  $d$ , see [1, Theorem 2.5].

In this talk we gave an improvement to at least exponential growth for  $p_d$ . This is done by twisting the above construction in the following way: Allow only at most one “hole” in every set  $Bn+1, Bn+2, \dots, Bn+B-1$  of  $B$  consecutive integers (forming the coefficients of  $(1, 2, \dots)$  for some large integer  $B$  (taking  $B = 60$  certainly works), we get again perfect lattices if the dimension is large enough. There is now an exponentially growing number of such lattices and they are again all essentially non-isomorphic. Details of a close (but technically slightly easier) variation of this construction are currently being written up.

Let me finish this short abstract by mentioning that the above lattices are closely related to the lattices considered in Lenny Fukshansky’s talk. Indeed, almost all of the lattices considered by Fukshansky are also perfect by section 5 (which considers exactly Fukshansky’s lattices) in [1].

### REFERENCES

- [1] R. Bacher, *Constructions of some perfect integral lattices with minimum 4*, Journal de Théorie des Nombres de Bordeaux **27** (2015), 655–687.
- [2] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften **327**, Springer-Verlag, Berlin, 2003.

## Rationally isomorphic Hermitian forms

EVA BAYER-FLUCKIGER

(joint work with Uriya First)

Let  $R$  be a discrete valuation ring and let  $F$  be its fraction field. Assume that 2 is a unit in  $R$ . The following theorem is well-known:

**Theorem 1.** *Let  $f, f'$  be two unimodular quadratic forms over  $R$ . If  $f$  and  $f'$  become isomorphic over  $F$ , then they are isomorphic over  $R$ .*

Over the years, this result has been generalized in many ways: to other local rings, and other types of forms (instead of quadratic). Many of these results are consequences of a conjecture of Grothendieck and Serre (see [10], [6] and [7]) :

**Conjecture 1.** *Let  $R$  be a regular local integral domain with fraction field  $F$ . Then for every smooth reductive group scheme  $G$  over  $R$ , the induced map  $H_{\text{et}}^1(R, G) \rightarrow H_{\text{et}}^1(F, G)$  is injective.*

The Grothendieck-Serre conjecture was recently proved by Fedorov and Panin, provided  $R$  contains a field  $k$  (see [5] for the case where  $k$  is infinite and [9] for the case  $k$  is finite. Many special cases of the conjecture were known before. In particular, when  $\dim R = 1$  the conjecture was shown without any further restriction on  $R$  by Nisnevich (see [8]).

Recently, Auel, Parimala and Suresh generalized the above theorem in a different way, considering quadratic forms that are not unimodular, but “close” to being unimodular. They show the following (cf. [1], Corollary 3.8) :

**Theorem 2.** *Let  $q$  and  $q'$  be two quadratic forms over  $R$  with simple degeneration of multiplicity one. If  $q$  and  $q'$  become isomorphic over  $F$ , then they are isomorphic.*

Recall from [1] that a quadratic form over  $R$  is said to have *simple degeneration of multiplicity one* if it is isomorphic to the orthogonal sum of a unimodular quadratic form and a form of rank one of the shape  $\langle \pi \rangle$ , where  $\pi$  is a uniformizer.

Note that this result cannot be seen as a consequence of the Grothendieck–Serre conjecture, since the corresponding group scheme is not reductive.

This is the starting point of our research. Our aim is to put the result of Auel, Parimala and Suresh in a different perspective, and to study how far one can generalize it. Our point of view is inspired by the treatment of non-unimodular forms in [2]. Roughly speaking, idea is that non-unimodular forms in a hermitian category can be treated as *unimodular* forms over a different “module-like” category in a way which is compatible with flat base change. In this setting, the condition of being “simply degenerate of multiplicity one” is equivalent to having a particular “base module”.

We prove the following (cf. [4]) :

**Theorem 3.** *Let  $A$  be a maximal  $R$ -order in a separable  $F$ -algebra, and let  $\sigma : A \rightarrow A$  be an  $R$ -linear involution. Let  $f$  and  $f'$  be two hermitian forms over  $(A, \sigma)$  such that  $f$  and  $f'$  have isomorphic semisimple coradicals. If  $f$  and  $f'$  are isomorphic over  $(A_F, \sigma_F)$ , then they are isomorphic.*

Note that this is a generalization of the result of Auel, Parimala and Suresh. We also obtain a cohomological result, in the spirit of the Grothendieck–Serre conjecture – note however that the group scheme considered here is not reductive.

We also prove a result on quadratic forms invariant by a finite group. Let  $\Gamma$  be a finite group, and assume that the order of  $\Gamma$  is invertible in  $R$ . Recall that a  $\Gamma$ -quadratic form is a pair  $(P, f)$ , where  $P$  is a projective  $R[\Gamma]$ -module of finite rank, and  $f : P \times P \rightarrow R$  is a quadratic form such that  $f(gx, gy) = f(x, y)$  for all  $x, y \in P$  and all  $g \in \Gamma$ . We have the following :

**Theorem 4.** *Let  $(P, f)$  and  $(P', f')$  be two  $\Gamma$ -forms over  $R$  with isomorphic semisimple coradicals. If  $(P_F, f_F) \cong (P'_F, f'_F)$  as  $\Gamma$ -forms, then  $(P, f) \cong (P', f')$  as  $\Gamma$ -forms.*

The strategy of the proof is to establish a “descent result” for unimodular hermitian forms over hereditary orders. Indeed, the endomorphism rings of the objects of the “module-like category” we use are hereditary. This is actually our main technical result. It is proved in two main steps: on one hand, prove the result in the case where  $R$  is complete, on the other hand, deduce the general case from this result by patching techniques. These two steps are contained in the papers [3] and [4].

#### REFERENCES

- [1] A. Auel, R. Parimala, V. Suresh, *Quadratic surface bundles over surfaces*, Documenta Math. (Extra vol.: Alexander S. Merkurjev’s sixtieth birthday) (2015), 31–70.
- [2] E. Bayer–Fluckiger, L. Fainsilber, *Non-unimodular hermitian forms*, Invent. Math. **123** (1996), 233–240.
- [3] E. Bayer–Fluckiger, U. First, *Patching and weak approximation in isometry groups*, (<http://arxiv.org/abs/1504.01280>).
- [4] E. Bayer–Fluckiger, U. First, *Rationally isomorphic hermitian forms and torsors of some non-reductive groups*, preprint 2016.
- [5] R. Fedorov, I. Panin, *A proof of Grothendieck–Serre conjecture on principal bundles over regular local rings containing infinite fields*, Publ. Math. IHES (2015), 1–25.
- [6] A. Grothendieck, *La torsion homologique et les sections rationnelles*, Anneaux de Chow et applications, Séminaire C. Chevalley, 2e année (1958).
- [7] A. Grothendieck : *Le groupe de Brauer II. Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics (1968).
- [8] Y. Nisnevich, *Espaces homogènes principaux rationnellement triviaux et arithmétique des schémas en groupes réductifs sur les anneaux de Dedekind*, C. R. Acad. Sci. Paris Sér. I Math., **299** (1984), 5–8.
- [9] I. Panin, *On Grothendieck–Serre conjecture concerning principal  $G$ -bundles over regular semi-local domains containing a finite field*, (<http://arxiv.org/abs/146.0241>).
- [10] J-P. Serre, *Espaces fibrés algébriques*, Anneaux de Chow et applications, Séminaire C. Chevalley, 2e année (1958).

## Participants

**Prof. Dr. Roland Bacher**

Laboratoire de Mathématiques  
Université de Grenoble I  
Institut Fourier  
B.P. 74  
38402 Saint-Martin-d'Herès Cedex  
FRANCE

**Prof. Dr. Christine Bachoc**

Institut de Mathématique de Bordeaux  
Université de Bordeaux  
351, cours de la Libération  
33405 Talence Cedex  
FRANCE

**Prof. Dr. Eva Bayer-Fluckiger**

EPFL  
SB IMB CSAG (Batiment MA)  
Station 8  
1015 Lausanne  
SWITZERLAND

**Prof. Dr. Siegfried Böcherer**

Fakultät f. Mathematik & Informatik  
Universität Mannheim  
68131 Mannheim  
GERMANY

**Dr. Martino Borello**

EPFL  
SB IMB CSAG (Batiment MA)  
Station 8  
1015 Lausanne  
SWITZERLAND

**Prof. Dr. Jean-Benoit Bost**

Département de Mathématiques  
Université de Paris-Sud  
Bat. 425  
91405 Orsay Cedex  
FRANCE

**Oliver Braun**

Lehrstuhl D für Mathematik  
RWTH Aachen  
52056 Aachen  
GERMANY

**Prof. Dr. Wai Kiu Chan**

Department of Mathematics &  
Computer Science  
Wesleyan University  
655 Science Tower  
265 Church Street  
Middletown CT 06459-0128  
UNITED STATES

**Dr. Sungmun Cho**

Department of Mathematics  
University of Toronto  
40 St George Street  
Toronto, Ont. M5S 2E4  
CANADA

**Prof. Dr. Henry Cohn**

Microsoft Research New England  
One Memorial Drive  
Cambridge, MA 02142  
UNITED STATES

**Prof. Dr. Renaud Coulangeon**

Institut de Mathématiques de Bordeaux  
Université de Bordeaux  
351, cours de la Libération  
33405 Talence Cedex  
FRANCE

**Maria Dostert**

Mathematisches Institut  
Universität zu Köln  
Weyertal 86-90  
50931 Köln  
GERMANY



**David Dursthoff**

Lehrstuhl D für Mathematik  
RWTH Aachen  
Pontdriesch 14/16  
52056 Aachen  
GERMANY

**Prof. Dr. Mathieu Dutour Sikirić**

Rudjer Boskovic Institute  
Laboratory of Satellite Oceanography  
Dept. of Environmental & Marine  
Research  
Bijenicka 54  
10000 Zagreb  
CROATIA

**Prof. Dr. Philippe Elbaz-Vincent**

Institut Fourier  
UMR 5582, CNRS/UJF  
Université de Grenoble Alpes I  
P.O. Box 74  
38402 Saint-Martin-d'Herès  
FRANCE

**Prof. Dr. Graham Ellis**

Mathematics Department  
National University of Ireland, Galway  
University Road  
Galway  
IRELAND

**Jessica Fintzen**

Department of Mathematics  
Harvard University  
Science Center  
One Oxford Street  
Cambridge MA 02138-2901  
UNITED STATES

**Prof. Dr. Lenny Fukshansky**

Department of Mathematics  
Claremont McKenna College  
500 E. Ninth Street  
Claremont, CA 91711  
UNITED STATES

**Prof. Dr. Eric Gaudron**

Laboratoire de Mathématiques  
UMR 6620 du CNRS  
Université Blaise Pascal-Clermont II  
Plateau des Cezeaux  
63177 Aubière Cedex  
FRANCE

**Dr. Matthew Greenberg**

Department of Mathematics & Statistics  
University of Calgary  
2500 University Drive N.W.  
Calgary, Alberta T2N 1N4  
CANADA

**Prof. Dr. Tomoyoshi Ibukiyama**

Department of Mathematics  
Graduate School of Science  
Osaka University  
Machikaneyama 1-1, Toyonaka  
Osaka 560-0043  
JAPAN

**Dr. Paul Jenkins**

Department of Mathematics  
Brigham Young University  
Provo, UT 84602-6539  
UNITED STATES

**Dr. Markus Kirschmer**

Lehrstuhl D für Mathematik  
RWTH Aachen  
Templergraben 64  
52062 Aachen  
GERMANY

**Tamás Korodi**

Lehrstuhl B für Mathematik  
RWTH Aachen  
Pontdriesch 10-16  
52062 Aachen  
GERMANY

**Dr. Stefan Kühnlein**

Institut für Algebra und Geometrie  
Universität Karlsruhe  
Englerstrasse 2  
76131 Karlsruhe  
GERMANY

**Prof. Dr. Jean Lannes**

Centre de Mathématiques  
École Polytechnique  
Plateau de Palaiseau  
91128 Palaiseau Cedex  
FRANCE

**Prof. Dr. Joshua M. Lansky**

Department of Mathematics and  
Statistics  
American University  
Washington, DC 20016  
UNITED STATES

**Prof. Dr. Ling Long**

Department of Mathematics  
Louisiana State University  
Baton Rouge LA 70803-4918  
UNITED STATES

**Prof. Dr. Annika Meyer**

FB Elektrotechnik &  
Informationstechnik  
Fachhochschule Südwestfalen  
Postfach 4161  
58041 Hagen  
GERMANY

**Dr. Tsuyoshi Miezaki**

Faculty of Education, Art and Science  
Yamagata University  
1-4-12 Kojirakawa-chou  
Yamagata 990-8560  
JAPAN

**Philippe Moustrou**

Institut de Mathématique de Bordeaux  
Université de Bordeaux  
351, cours de la Liberation  
33405 Talence Cedex  
FRANCE

**Prof. Dr. Gabriele Nebe**

Lehrstuhl D für Mathematik  
RWTH Aachen  
52056 Aachen  
GERMANY

**Dr. David Pollack**

Department of Mathematics  
Wesleyan University  
265 Church Street  
Middletown, CT 06459-0128  
UNITED STATES

**Prof. Dr. Gaël Rémond**

Institut Fourier  
UMR 5582, CNRS/UGA  
Université Grenoble Alpes  
100, rue des maths  
38402 Saint-Martin-d'Hères Cedex  
FRANCE

**Maren Helene Ring**

Institut für Mathematik  
Universität Rostock  
18057 Rostock  
GERMANY

**Dr. Jeremy Rouse**

Department of Mathematics  
Wake Forest University  
340 Manchester Hall  
P.O. Box 7388  
Winston-Salem, NC 27109  
UNITED STATES

**Prof. Dr. Rudolf Scharlau**  
Fakultät für Mathematik  
Technische Universität Dortmund  
44221 Dortmund  
GERMANY

**Sebastian Schönnebeck**  
Lehrstuhl D für Mathematik  
RWTH Aachen  
52056 Aachen  
GERMANY

**Prof. Dr. René Schoof**  
Dipartimento di Matematica  
Universita degli Studi di Roma II  
Tor Vergata  
Via della Ricerca Scientifica  
00133 Roma  
ITALY

**Dr. Rainer Schulze-Pillot**  
Fachrichtung Mathematik  
Universität des Saarlandes  
Postfach 151150  
66041 Saarbrücken  
GERMANY

**Prof. Dr. Achill Schürmann**  
Institut für Mathematik  
Universität Rostock  
18057 Rostock  
GERMANY

**Prof. Dr. Joachim Schwermer**  
Institut für Mathematik  
Universität Wien  
Oskar-Morgenstern-Platz 1  
1090 Wien  
AUSTRIA

**Prof. Dr. Nils-Peter Skoruppa**  
Department Mathematik  
Universität Siegen  
Emmy-Noether-Campus  
Walter-Flex-Strasse 3  
57068 Siegen  
GERMANY

**Prof. Dr. Christophe Soulé**  
I.H.E.S.  
Le Bois Marie  
35, route de Chartres  
91440 Bures-sur-Yvette  
FRANCE

**Dr. Ha Tran**  
Department of Mathematics and  
Systems Analysis, School of Science  
Aalto University  
Otakaari 1  
02150 Espoo 15  
FINLAND

**Ivica Turkalj**  
Fakultät für Mathematik  
Technische Universität Dortmund  
44221 Dortmund  
GERMANY

**Prof. Dr. Frank Vallentin**  
Mathematisches Institut  
Universität zu Köln  
50931 Köln  
GERMANY

**Dr. John Voight**  
Department of Mathematics  
Dartmouth College  
6188 Kemeny Hall  
Hanover, NH 03755-3551  
UNITED STATES

**Prof. Dr. Lynne H. Walling**

Department of Mathematics  
University of Bristol  
University Walk  
Bristol BS8 1TW  
UNITED KINGDOM

**Dr. Martin Widmer**

Department of Mathematics  
Royal Holloway College  
University of London  
Surrey TW20 0EX  
UNITED KINGDOM

**Prof. Dr. Takao Watanabe**

Department of Mathematics  
Graduate School of Science  
Osaka University  
Machikaneyama 1-1, Toyonaka  
Osaka 560-0043  
JAPAN

**Dr. Dan Yasaki**

Department of Mathematics & Statistics  
University of North Carolina at  
Greensboro  
116 Petty Building  
Greensboro, NC 27402-6170  
UNITED STATES

**Dr. Martin Westerholt-Raum**

Mathematics Department  
Chalmers Technical University  
Chalmers Tvärgata 3  
412 96 Göteborg  
SWEDEN

**Marc-Christian Zimmermann**

Fakultät für Mathematik  
Technische Universität Dortmund  
44221 Dortmund  
GERMANY