Mathematisches Forschungsinstitut Oberwolfach

Report No. 1/2005

Gitter und Anwendungen

Organised by
Christiane Bachoc (Bordeaux)
Eva Bayer-Fluckiger (Lausanne)
Gabriele Nebe (Aachen)

January 2nd – January 8th, 2005

Abstract. The meeting focussed on lattices and their applications in mathematics and information technology. The research interests of the participants varied from engineering sciences, algebraic and analytic number theory, coding theory, algebraic geometry to name only a few.

Mathematics Subject Classification (2000): 11xx.

Introduction by the Organisers

Respecting the different backgrounds of the participants, most of the talks were aimed to a broad audience, among those nine survey talks invited by the organizers. This concept was very successful and opened many discussions and interdisciplinary interactions. It was also very fruitful for the many young participants. Also most of the non speakers took the opportunity to present their recent work via posters.

The theory of lattices has many applications and interactions with various other mathematical and technical disciplines such as information technology, topology, algebraic geometry, representation theory, combinatorics, number theory and modular forms to name only the most prominent ones. One of the most classical problems is the construction of dense lattice sphere packings. The densest lattice sphere packings are only known in dimensions up to 8 and, due to a recent work by H. Cohn and A. Kumar, also in dimension 24. A. Kumar gave a very illuminating talk on the strategy of their proof of this great result which uses certain linear programming techniques based on the fact that the minimal vectors of the Leech lattice form a very good design. Design techniques have also been used by B. Venkov to define the notion of strongly perfect lattices, which realize certain

local maxima of the density function and which are now classified up to dimension 12.

The theory of modular forms is one well established tool in the investigation of lattices as shown in the nice introduction by Krieg. Bannai applies this theory to bound the strength of designs provided by layers of unimodular lattices. On the other hand, lattices provide one important tool for the construction of modular forms. The last talk by Böcherer showed that in many situations all modular forms are linear combinations of theta-series.

Of increasing interest but computationally very difficult is the investigation of thin lattice sphere coverings. Vallentin and Schürmann developed new algorithms to find local optimal coverings and discovered lattice coverings better than the ones previously known.

Nguyen presented new reduction algorithms for lattices in small dimensions motivated by practical applications to cryptosystems. For certain applications in information technology not only the density of the lattice but also other properties that minimize the fading error play a role. It turns out that lattices constructed from algebraic number fields yield good codes for Rayleigh fading channels. These ideal lattices are also used to investigate the ring of integers in algebraic number fields as shown in the talk by Schoof and also in the applications of ideal lattices introduced by Bayer-Fluckiger. Strongly related to this is the application to Arakelov theory as illustrated in the talks by Bost and Künnemann.

Also Voronoi's classical theory of perfect forms (see Martinet's talk for an introduction) has new fruitful applications in number theory more precisely in the calculation of the homology of $GL_n(\mathbf{Z})$ as presented by Elbaz-Vincent.

Last but not least one should mention the talk by J.-P. Serre on BL-bases and unitary groups in characteristic 2.

Workshop: Gitter und Anwendungen

Table of Contents

Boris Venkov
Perfect lattices and spherical designs 9

Aloys Krieg
Lattices and Modular Forms 10

Eiichi Bannai (joint with Masao Koike, Masashi Shinohara, Makoto Tagami)
Spherical designs, extremal lattices and the Fourier coefficients modulo p of the extremal modular forms 12

Roland Bacher
On the Minkowski-Hlawka bound for lattice-packings 15

Rainer Schulze-Pillot (joint with Hidenori Katsurada)
A matching principle for theta series and theta integrals 17

Emanuele Viterbo (joint with E. Bayer-Fluckiger, J-C. Belfiore, F. Oggier, G. Rekaya)
Algebraic lattices and channel coding for digital transmission 20

René Schoof
Arakelov class groups and ideal lattices 23

Jacques Martinet (joint with Anne-Marie Bergé)
Voronoi graphs, cells, and spherical designs 24

Kanat Abdukhalikov (joint with Rudolf Scharlau)
Unimodular hermitian lattices 27

Michael Baake (joint with Daniel Lenz, Robert V. Moody)
Model sets as generalizations of lattices 30

Jean-Benoît Bost
Lattices and hermitian vector bundles in Arakelov geometry 33

Abhinav Kumar (joint with Henry Cohn)
Optimality and Uniqueness of the Leech lattice among lattices 34

Jean-Claude Belfiore
Application of a new lattice reduction algorithm 37

Jean-Pierre Serre
BL-bases and unitary groups in characteristic 2 37

Philippe Elbaz-Vincent (joint with Herbert Gangl, Christophe Soulé)
Perfect Lattices, Homology of Modular groups and Algebraic K-Theory . . . 41

Phong Q. Nguyên (joint with Damien Stehlé)
On Reduction Theory and its Algorithmic Aspects 44

Pham Huu Tiep (joint with Robert M. Guralnick)
Weil representations, Clifford groups, and conjectures of Larsen and Katz 45

Frank Vallentin (joint with Achill Schürmann)
Sphere Coverings in Dimensions 1, . . . , 24 48

Renaud Coulangeon
Hermite constants. 52

Tomoyoshi Ibukiyama
K. Saito's conjecture on positivity of eta products and "extremal pair" of lattices 54

Klaus Künnemann (joint with Jean-Benoît Bost)
Hermitian vector bundles and extension groups on arithmetic varieties . . . 56

Myung-Hwan Kim (joint with Wai-Kiu Chan, Byeong Moon Kim, Byeong-Kweon Oh)
A local-global principle for extensibility of representations of quadratic forms and applications 57

Takao Watanabe
Minkowski's second theorem over a simple algebra 59

Siegfried Böcherer
On the basis problem for squarefree levels 61

Abstracts

Perfect lattices and spherical designs

Boris Venkov

This talk was an introduction to the theory of perfect lattices and especially those related to spherical 5-designs, the strongly perfect lattices. The notion of a perfect lattice arose about 100 years ago in papers by Korkin, Zolotarev and especially Voronoi ([6]). It arises naturally when one studies dense lattice sphere packings in an euclidean space $\mathbf{R}^n$. If the centers of the spheres in a packing form a lattice Λ then the density of the sphere packing is proportional to the Hermite function of the lattice

$$\gamma(\Lambda) := \frac{\min\{(\lambda,\lambda) \mid 0 \neq \lambda \in \Lambda\}}{(\det(\Lambda))^{1/n}}\,.$$

So the densest lattice sphere packings correspond to maxima of the Hermite function. The densest lattices are extremely difficult to study (they are known for $n \leq 8$ and $n = 24$ (see Kumar's talk in this conference)). Much easier to study are the local maxima of γ, which are called extreme lattices. They are characterized as those lattices that are perfect and eutactic. Perfect means that the space of quadratic functions on $\mathbf{R}^n$ is generated by the squares of the linear forms associated with the minimal vectors of Λ. In particular the number of minimal vectors (kissing number) of a perfect lattice is $\geq n(n+1)$. The condition to be eutactic is more technical. Voronoi (1907, [6]) has found a very nice description of extreme forms as faces of a very natural infinite convex polyhedron in the space of positive semidefinite quadratic forms on $\mathbf{R}^n$. This description leads to an algorithm (Voronoi's algorithm) which permits in principle to find all extreme forms in a given dimension. This was worked out for $n \leq 7$. Unfortunately the number of extreme lattices grows rapidly with the dimension and Voronoi's algorithm does not seem to be practicable for $n \geq 8$. So the question arises to find more restricted classes of perfect lattices which include interesting classical lattices (such as the Leech lattice, the E_8-lattice and others) and which is more affordable for classification. One such possibility is given by the notion of strongly perfect lattices. These are lattices whose minimal vectors form a spherical 5-design. They are perfect and eutactic and hence local maxima of γ but they are not so numerous. For example the lattice E_8 is the only strongly perfect lattice in dimension 8. A complete classification of strongly perfect lattices is known up to dimension 11 ([5], [3]), the 12-dimensional case will hopefully be finished soon ([4]). Still for $n = 32$ all even unimodular lattices without roots are strongly perfect, so by Oliver King ([1]) there are $> 10^6$ strongly perfect lattices in dimension 32.

References

[1] O. King: A mass formula for unimodular lattices with no roots. Mathematics of Computation 72 (2003), no. 242, 839–863.

[2] J. Martinet: *Les Réseaux parfaits des espaces Euclidiens.* Masson (1996)

[3] G. Nebe, B. Venkov, The strongly perfect lattices of dimension 10. J. Théor. Nombres Bordeaux 12 (2000), no. 2, 503–518.
[4] G. Nebe, B. Venkov, The strongly perfect lattices of dimension 12 and 13. work in progress
[5] *B. Venkov:* Réseaux et designs sphériques. In Réseaux euclidiens, designs sphériques et formes modulaires. L'Ens. Math. Monographie **37** (2001) 10–86.
[6] G. Voronoi: Nouvelles applications des paramètres continues à la théorie des formes quadratiques: 1. Sur quelques proprietés des formes quadratiques parfaites. J. Reine Angew. Math. **133** (1908) 97–178.

Lattices and Modular Forms

Aloys Krieg

We review the interaction between the theory of lattices and the theory of modular forms in several variables. Let $\Lambda = \Lambda_{2k}$ always be an even unimodular lattice in $(\mathbb{R}^{2k}, \langle\ ,\ \rangle)$ $k \in \mathbb{N}$. The Siegel half-space of degree n is denoted by

$$\mathcal{H}_n = \big\{ Z = X + iY \in M_n(\mathbb{C});\ Z = Z^{tr},\, Y > 0 \big\}.$$

The vector space $\mathcal{M}_k^{(n)}$ of *Siegel modular forms* of degree n and weight k consists of all holomorphic functions $f : \mathcal{H}_n \to \mathbb{C}$ (also at ∞ if $n = 1$) satisfying

$$f\big((AZ + B)(CZ + D)^{-1}\big) = \det(CZ + D)^k f(Z)$$

for all $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{Z})$, i.e. $M \in M_{2n}(\mathbb{Z})$, $M^{tr} J M = J$, $J = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}$.
Each $f \in \mathcal{M}_k^{(n)}$ possesses a Fourier expansion of the form

$$f(Z) = \sum_{T \geq 0 \text{ even}} \alpha_f(T)\, e^{\pi\, i\, trace(TZ)},$$

where even means $T = T^{tr} = (t_{\nu\mu}) \in M_n(\mathbb{Z})$, $t_{\nu\nu} \in 2\mathbb{Z}$. The subspace $\mathcal{S}_k^{(n)}$ of all cusp forms in $\mathcal{M}_k^{(n)}$ consists of the kernel of the Siegel ϕ-operator

$$\phi : \mathcal{M}_k^{(n)} \to \mathcal{M}_k^{(n-1)}, \quad f \mapsto f \mid \phi(Z_1) := \lim_{y \to \infty} f \begin{pmatrix} Z_1 & 0 \\ 0 & iy \end{pmatrix}.$$

This can be characterized by the condition on the Fourier expansion

$$\alpha_f(T) = 0 \quad \text{if} \quad \det T = 0.$$

Examples are given by the *Siegel-Eisenstein series*

$$E_k^{(n)}(Z) = \sum_{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) : \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \backslash \mathrm{Sp}_n(\mathbb{Z})} \det(CZ + D)^{-k} \in \mathcal{M}_k^{(n)}, \quad E_k^{(n)} \mid \phi = E_k^{(n-1)},$$

for even $k > n + 1$. Moreover consider the *theta series* of degree n

$$\Theta_\Lambda^{(n)}(Z) = \sum_{(\lambda_1, \ldots, \lambda_n) \in \Lambda^n} e^{\pi i\, tr((\langle \lambda_\nu, \lambda_\mu \rangle) \cdot Z)} \in \mathcal{M}_k^{(n)}, \quad \Theta_\Lambda^{(n)} \mid \phi = \Theta_\Lambda^{(n-1)}.$$

Let $\mathcal{M}_k^{(n)}(\Theta)$ denote the subspace of $\mathcal{M}_k^{(n)}$ spanned by all $\Theta_\Lambda^{(n)}$, $\Lambda \subset \mathbb{R}^{2k}$ even, unimodular. The most important result is contained in

Theorem 1. (Böcherer, Freitag, Igusa, Resnikoff, Weissauer, Witt).

a) $\bigoplus_{k\in 4\mathbb{Z}} \mathcal{M}_k^{(n)}$ *is the normalization of*

$$\bigoplus\nolimits_{k\in 4\mathbb{N}} \mathcal{M}_k^{(n)}(\Theta).$$

b) *If* $0 < 2k < n$ *one has*

$$\mathcal{M}_k^{(n)} = \begin{cases} \mathcal{M}_k^{(n)}(\Theta), & \text{if } 4 \mid k, \\ \{0\}, & \text{otherwise.} \end{cases}$$

The theta series $\Theta_\Lambda^{(n)}$ *of the different isometry classes of all even unimodular lattices in* $\mathbb{R}^{2k}$ *are linearly independent if* $2k \le n$.

c) *If* $2k > 4n$, $4 \mid k$, *one has*

$$\mathcal{M}_k^{(n)} = \mathcal{M}_k^{(n)}(\Theta).$$

d) *Let* $f \in \mathcal{S}_k^{(n)}$, $n \le 2k \le 4n$, $4 \mid k$, *be a simultaneous Hecke eigenform. Then*

$$f \in \mathcal{M}_k^{(n)}(\Theta) \quad \text{if and only if} \quad \mathbb{L}_f(k-n) \neq 0,$$

where $\mathbb{L}_f(s)$ *denotes the completed standard L-function associated with* f.

e) *If* $n = 1$ *or* $n = 2$ *one has*

$$\mathcal{M}_k^{(n)} = \mathcal{M}_k^{(n)}(\Theta) \quad \text{for all} \quad 4 \mid k,$$
$$\Theta_{\Lambda_8}^{(n)} = E_4^{(n)}, \quad \Theta_{\Lambda_{16}}^{(n)} = {E_4^{(n)}}^2 = E_8^{(n)}.$$

In b) we deal with singular modular forms, i.e. the Fourier coefficients of non-degenerate matrices are 0. We observe that the theta series contains the full information about the lattice in this case because the lattice can be recovered from the Fourier expansion of the modular form. In d) we observe that $k - n$ is outside the range of absolute convergence of the L-series, which possesses an analytic continuation. In e) the results follow because the graded ring of modular forms can explicitly be described in terms of generators and relations.

Kohnen and Salvati Manni constructed a Siegel modular form of weight k, $4 \mid k$, which is not a linear combination of theta series, by means of an Ikeda lift. They applied d).

Theorem 2. (Witt, Weissauer) *Let* $\Lambda_1, \ldots, \Lambda_h$ *be representatives of the isometry classes of the even unimodular lattices in* $\mathbb{R}^{2k}$. *Then one has*

$$\sum_{\nu=1}^{h} \beta_\nu \Theta_{\Lambda_\nu}^{(n)} = \delta_{k,n} \cdot E_k^{(n)}, \quad \delta_{k,n} = \begin{cases} 1 & \text{if} \quad k > n+1 \\ \frac{1}{2} & \text{if} \quad k \le n+1 \end{cases},$$

where

$$\beta_\nu = \frac{1/\sharp \mathrm{Aut}\Lambda_\nu}{(1/\sharp \mathrm{Aut}\Lambda_1) + \ldots + (1/\sharp \mathrm{Aut}\Lambda_h)}, \quad \nu = 1, \ldots, h.$$

Here $\mathrm{Aut}\Lambda_\nu$ denotes the (finite) automorphism group of the lattice Λ_ν. Note that the Eisenstein series on the right hand side has to be constructed by analytic continuation if $k \leq n+1$.

Finally we consider the cusp forms obtained from the theta series of all even unimodular lattices of fixed dimension.
If $2k = 16$, there are two different isometry classes of even unimodular lattices given by $\Lambda_8 \bigoplus \Lambda_8$ and Λ_{16}. Kneser and Igusa showed that

$$0 \neq \Theta^{(4)}_{\Lambda_8 \bigoplus \Lambda_8} - \Theta^{(4)}_{\Lambda_{16}} \in \mathcal{S}^{(4)}_k.$$

If $2k = 24$ the filtration of the cusp forms spanned by the 24 isometry classes of even unimodular lattices was calculated by Nebe and Venkov.

References

[1] Böcherer, S.: Siegel modular forms and theta series. Theta Functions. Proc. 35th Res. Inst. Bowdoin. Proc. Symp. Pure Math. **49** (1989), 3-17.

[2] Freitag, E.: Siegelsche Modulfunktionen. Springer-Verlag, Berlin-Heidelberg-New York 1983.

[3] Kohnen, W., Salvati Manni, R.: Linear relations between theta series. Osaka J. Math. **41** (2004), 353-356.

[4] Nebe, G., Venkov, B.: On Siegel modular forms of weight 12. J. reine angew. Math. **531** (2001), 49-60.

[5] Weissauer, R.: Stabile Modulformen und Eisensteinreihen. Lect. Notes Math. **1219**, Springer-Verlag, Berlin-Heidelberg-New York 1986.

Spherical designs, extremal lattices and the Fourier coefficients modulo p of the extremal modular forms

Eiichi Bannai

(joint work with Masao Koike, Masashi Shinohara, Makoto Tagami)

Theorem of Venkov (cf.[5],[6]), which is an analogue of Assmus-Mattson theorem for codes, says that each nontrivial shell of an extremal even unimodular lattice in the Euclidean space $\mathbb{R}^n$ is (at least) a spherical 11-design (resp. 7-design, 3-design) in $\mathbb{R}^n$, if n is a multiple of 24 (resp. congruent to 8 modulo 24, congruent to 16 modulo 24). It is an interesting problem, posed by Venkov, de la Harpe and Pache (cf.[2]), when does it become a t-design, for a bigger value of t than mentioned above. This innocent looking problem is not easy to solve, as it is seen for example from the fact that the statement that no shell of the E_8-lattice can become an 8-design is equivalent to the famous Lehmer's conjecture (cf.[4]) in number theory that the Ramanujan function $\tau(m)$ can never become 0 for any positive integer m.

In the first part of this talk, we consider more specific problem when do all the shells of an even unimodular lattice become t-designs for a bigger value of t than mentioned above. We will show that, when $n \equiv 0 \pmod{24}$ this does not happen

in many cases. Namely, we prove the following experimental result:

Theorem 1. Let Λ be an extremal even unimodular lattice in $\mathbb{R}^n$ with $n = 24\mu$. If $\mu \leq 150$ and μ is **not** in B, where $B = \{5, 10, 15, 17, 20, 25, 28, 30, 39, 40, 45, 50, 52, 55, 61, 65, 70, 72, 75, 80, 83, 90, 94, 95, 100, 103, 115, 116, 120, 125, 127, 128, 130, 135, 138, 140, 145, 147, 149, 150\}$, then at least one shell Λ_{2m} of Λ is not a 12-design.

In proving Theorem 1, we use the following:
Fundamental Equation (Venkov [5],[6]). A subset $X(= -X)$ in $S^{n-1}(r)$ is a t-design (where $S^{n-1}(r)$ is the sphere of radius r with the center at the origin) if and only if for all $\alpha \in \mathbb{R}^n$

$$\frac{1}{|X|}\sum_{x\in X}(\alpha, x)^{2k} = \frac{1\cdot 3\cdot 5\cdot \cdots \cdot (2k-1)}{n(n+2)\cdots(n+2k-2)}(\alpha,\alpha)^k(x,x)^k$$

for all $k = 1, 2, \ldots, [\frac{t}{2}]$.

By taking $k = 6$ and taking α and x from Λ_{2m}, for each $\mu \leqslant 150$ ($\mu \neq 6$) not in the set B, we can find an odd prime p and m which satisfy the following conditions:
(i) $p|n(n+2)\cdots(n+2k-2)$
(ii) $p \not| 1\cdot 3\cdot 5\cdot \cdots \cdot (2k-1)$
(iii) $p \not| |\Lambda_{2m}|$
(iv) $p \not| m$.
The existence of such integer m clearly implies that Λ_{2m} is not a 12-design, by comparing the order of the p-power of both sides of the Fundamental Equation.

The extremal modular form (of weight $k = 12\mu + k_0$ with $k_0 \in \{0, 4, 6, 8, 10, 14\}$) is the modular form

$$f(\tau) = \sum_{m\geq 0} a_m q^m \quad (q = e^{2\pi i\tau}),$$

with $a_1 = a_2 = \cdots = a_\mu = 0$. (Note that the theta series of an extremal even unimodular lattice in $\mathbb{R}^n$ is the extremal modular form of weight $k = n/2$. Also, note that the extremal modular form exists for each k with k even and ≥ 4, independent of the existence of extremal even unimodular lattices.)

Motivated by Theorem 1, we are interested in studying the modulo p property of the Fourier coefficients of the extremal modular forms. Namely, we are interested in dividing for each pair of k and prime p, which of the following three (exclusive) cases holds:
Case (1) $p|a_i$, for all $i \geq 1$,
Case (2) $p \not| a_i$, for all $i \geq 1$ with $p \not| i$, and there exists at least one $j \geq 1$ with $p \not| a_j$,
Case (3) there exists at least one $j \geq 1$ with $p \not| j$ such that $p \not| a_j$.

We first prove that Case(1) holds, if and only if $(p-1)|k$. (These primes p in Case(1) are called Bernoulli type primes for k.)

We also obtain several conditions which guarantee that Case (2) holds. For example, we prove the following theorem, by using the method of Serre [3].

Theorem 2. Let k_1 to be the number in $\{4, 6, 8, \cdots, p-1, p+1\}$ such that $k \equiv k_1 (\mathrm{mod}\ p-1)$. Let $(p-1) \not| k$. Let l_1 satisfy : $pl_1 \leq \mu + 1 < p(l_1+1)$, and let k_2 to be the smallest integer with $k_2 \equiv k_1 (\mathrm{mod}\ p-1)$ and $\dim M_{k_2} \geq l_1 + 1$. Then r_2 is determined by $k = k_2 + (p-1)r_2$. If $r_2 \geq k_2$ holds for p, then the extremal modular form f of weight k is expressed as $f \equiv g(p\tau) (\mathrm{mod}\ p)$, where $g(\tau)$ is the extremal modular form of weight k_2. Moreover, we have $p \mid a_{l_1+1}$.

Theorem 2 is used to prove the following result, which was motivated by Theorem 1. (Note that the the property in Theorem 3 is true for the theta series of extremal even unimodular lattices (by using the theorem of Venkov), but we anticipated that this property may hold for extremal modular forms.

Theorem 3. Let $k = 12\mu$, and let $f_k = 1 + 0 \cdot q + 0 \cdot q^2 + \cdots + 0 \cdot q^{\mu} + a_{\mu+1} q^{\mu+1} + \cdots$ be the extremal modular form of weight k. Let p be a prime number greater than or equal to 13. Suppose that p divides $2k(2k+2)(2k+4)(2k+6)(2k+8)(2k+12)$. Then Case (2) holds for p, and we get $p|a_{\mu+1}$.

We believe that when p is in Case (2) might be characterized by the following:

Conjecture 4. Let f be the extremal modular form of weight $k = 12\mu$. Suppose that p is in Case (2). (i) Then f is expressed as

$$f(\tau) \equiv g(p\tau) (\mathrm{mod}\ p).$$

for a modular form $g(\tau)$ of smaller weight.
(ii) Moreover, there exist the extremal modular form $g(\tau)$ of a smaller weight, and a natural number r such that

$$f(\tau) \equiv g(p^r\tau) (\mathrm{mod}\ p).$$

(It would be very interesting either to prove or disprove this conjecture. We proved this in many cases, including all the cases of $\mu \leq 150$.)

Remark. We obtained a similar result as Theorem 1 for extremal Type II codes, by using the method of Bachoc [1], which gives an alternative proof of the Assmus-Mattson theorem by using the invariants theory of finite groups. Also, we note that in this code case, we can prove that each nontrivial shell of the code has the constant strength t. However, this property cannnot easily be generalized for extremal lattices so far.

References

[1] C. Bachoc, On harmonic weight enumerators of binary codes. Designs and codes—a memorial tribute to Ed Assmus. Des. Codes Cryptogr. **18** (1999), no. 1-3, 11–28.

[2] C. Pache, Shells of self-dual lattices viewed as spherical designs (preprint, 2004).

[3] J. P. Serre, Congruences et formes modulaires [d'apres H. P. F. Swinnerton-Dyer]. (French) Seminaire Bourbaki, 24e annee (1971/1972), Exp. No. 416, pp. 319–338. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[4] J. P. Serre, Sur la lacunarite des puissances de η. (French) Glasgow Math. J. **27** (1985), 203–221.

[5] B. B. Venkov, Even unimodular extremal lattices. (Russian) Algebraic geometry and its applications. Trudy Mat. Inst. Steklov. **165** (1984), 43–48.

[6] B. Venkov, Reseaux et designs spheriques. (French) Reseaux euclidiens, designs spheriques et formes modulaires, 10–86, Monogr. Enseign. Math., **37**, Enseignement Math., Geneva, 2001.

On the Minkowski-Hlawka bound for lattice-packings

Roland Bacher

Let $\mu \geq 2$ be a positive integer. A $\mu-$*sequence* is a sequence $s_0 = 1, s_1, s_2, \dots$ of strictly positive integers such that the $n-$dimensional lattice

$$\Lambda_n = \{(z_0, z_1, \dots, z_n) \in \mathbf{Z}^{n+1} \mid \sum_{k=0}^{n} s_k z_k = 0\} = (s_0, \dots, s_n)^{\perp} \cap \mathbf{Z}^{n+1}$$

has minimum $\geq \mu$ for all $n \geq 1$. Since $\det(\Lambda_n) = \sum_{k=0}^{n} s_k^2$ we get a lower bound for the center-density

$$\delta(\Lambda_n) = \sqrt{\frac{(\min \Lambda_n)^n}{4^n \det \Lambda_n}} \geq \sqrt{\frac{\mu^n}{4^n \sum_{k=0}^{n} s_k^2}}$$

(or for the density $\Delta(\Lambda_n) = \delta(\Lambda_n)\pi^{n/2}/(n/2)!$) of the $n-$dimensional lattice Λ_n associated to a $\mu-$sequence.

Theorem 1. *Given an integer $\mu \geq 2$ as above there exists a $\mu-$sequence $s_0 = 1, s_1, \dots$ satisfying for all $n \geq 1$*

$$s_n \leq 1 + \sqrt{\mu - 2}\sqrt{\mu - 1 + n/4}^n \frac{\sqrt{\pi}^n}{(n/2)!} \leq \sqrt{\mu}\sqrt{\mu + n/4}^n \frac{\sqrt{\pi}^n}{(n/2)!} \ .$$

The proof of Theorem 1 is very elementary and consists essentially of an analysis of the "greedy algorithm" which constructs the first $\mu-$sequence with respect to the lexicographic order on sequences. An easy analysis shows that the lexicographically first sequence satisfies the first inequalities of Theorem 1. The greedy algorithm, although very simple, is however quite useless for applications because of astronomical memory requirements (which can be lowered at the price of an astronomical amount of computations).

$\mu-$sequences satisfying the inequalities of Theorem 1 yield rather dense lattices as shown by the next result.

Corollary 2. *For any $\mu \geq 2$, there exists a $\mu-$sequence $(s_0, s_1, \ldots, s_n) \in \mathbf{Z}^{n+1}$ such that the density of the associated lattice $\Lambda_n = (s_0, \ldots, s_n)^{\perp} \cap \mathbf{Z}^{n+1}$ satisfies*

$$\Delta(\Lambda_n) \geq \frac{(1 + n/(4\mu))^{-n/2}}{2^n \sqrt{(n+1)\mu}} \ .$$

Remark 3. *Taking $\mu \sim n^2/4$ we get the existence of lattices in dimension n (for large n) with density Δ roughly at least equal to*

$$\frac{1}{2^{n-1}\ n\ \sqrt{(n+1)\ e}} \ .$$

This is already close to the Minkowski-Hlawka bound (which shows the existence of lattices with density at least $\zeta(n)\ 2^{1-n}$, cf. formula (14) in [3]*, Chapter 1. The best known lower bound concerning densities of lattice packings (together with a very nice proof) seems to be due to Ball and asserts the existence of $n-$dimensional lattices with density at least $2(n-1)2^{-n}\zeta(n)$, see* [2].

A more careful analysis of $\mu-$sequences yields the following result.

Theorem 4. *For every $\epsilon > 0$, there exist $n-$dimensional lattices with density*

$$\Delta \geq \frac{1-\epsilon}{2^n\ \sum_{k=1}^{\infty} e^{-k^2\pi}} \sim (1-\epsilon)\ 23.1388\ 2^{-n}$$

for all n large enough.

Denote by $\mathcal{L}_n$ the set of all $n-$dimensional sublattices in $\mathbf{Z}^{n+1}$ which are of the form Λ_n as above for a suitable $\mu-$sequence $(1, s_1, s_2, \ldots, s_{n+1})$. The following result implies that the upper bound for densities of lattices in $\mathcal{L}_n$ is equal to the maximum for densities of all $n-$dimensional lattices.

Proposition 5. *The set $\mathcal{L}_n$ is dense in the set of similarity classes of $n-$dimensional Euclidean lattices.*

The preprint [1] contains proofs of all results presented above.

References

[1] R. Bacher, *On Minkowski's bound for lattice-packings*, preprint 650 of the Institut Fourier or arXiv: math.NT/0409008.

[2] K. Ball, *A lower bound for the optimal density of lattice packings*, Internat. Math. Res. Notices 1992, no. 10, 217–221.

[3] J.H. Conway, N.J.A.Sloane, *Sphere packings, Lattices and Groups* (Third Edition), Springer (1999).

[4] M. Krivelevich, S. Litsyn, A. Vardy, *A Lower Bound on the Density of Sphere Packings via Graph Theory*, preprint arXiv:math.CO/0402132.

[5] J. Martinet, *Perfect Lattices in Euclidean Spaces*, "Grundlehren" no. 327, Springer (2003).

A matching principle for theta series and theta integrals

Rainer Schulze-Pillot
(joint work with Hidenori Katsurada)

S. Kudla [2] recently pronounced a matching principle for theta integrals that gives a systematic framework for identities between theta series for definite and for indefinite integral quadratic forms.

Such identities lead to relations between

(1) representation numbers of definite integral quadratic forms
(2) representation measures of indefinite quadratic forms
(3) geometric information, in particular degrees of special cycles on modular varieties, e. g. Heegner points on modular curves, Hirzebruch-Zagier curves on Hilbert modular surfaces, Humbert surfaces on Siegel modular threefolds.

Here the connection between b) and c) is independent of this talk; it is established in work of Kudla and Millson [3] and of Oda [5], and in other research following that work.

We discuss here first the following classical example obtained in joint work [1] by H. Katsurada and the author:

Let L be a lattice of full rank on the $m = 2k$-dimensional vector space V over $\mathbb{Q}$, $q : V \longrightarrow \mathbb{Q}$ a regular quadratic form with $q(L) \subseteq \mathbb{Z}$, $N = N(L)$ the level of q; we assume $m = 2k$ to be even. For $\mathbf{x} = (x_1, \ldots, x_n) \in L^n$ we write $q(\mathbf{x}) = (\frac{1}{2}B(x_i, x_j)) \in M_n^{\mathrm{sym}}(\frac{1}{2}\mathbb{Z})$.
If q is positive definite, the theta series

$$\vartheta^{(n)}(L, Z) = \sum_{\mathbf{x}=(x_1,\ldots,x_n)\in L^n} \exp(2\pi i \operatorname{tr}(q(\mathbf{x})Z)$$

of degree n of (L, q) is in the space $M_k^{(n)}(\Gamma_0^{(n)}(N), \chi)$ of Siegel modular forms of weight $k = \frac{m}{2}$ and character χ, where χ is the character of $\Gamma_0^{(n)}(N)$ induced by the Dirichlet character $\tilde{\chi}(d) = \left(\frac{(-1)^k \det L}{d}\right)$ modulo N and $\det L$ is the determinant of the Gram matrix of L with respect to some basis.

By $\vartheta^{(n)}(\mathrm{gen}L, Z)$ we denote Siegel's weighted average of the $\vartheta^{(n)}(K, Z)$ where K runs through a set of representatives of the classes in the genus of L.

By Siegel's theorem the Fourier coefficient $r(\mathrm{gen}\ L, A)$ of $\vartheta^{(n)}(\mathrm{gen}L, Z)$ at the positive definite half integral symmetric matrix A can be expressed as a product of local densities,

$$r(\mathrm{gen}\ L, A) = c \cdot (\det A)^{\frac{m-n-1}{2}} (\det L)^{\frac{n}{2}} \prod_{\ell \text{ prime}} \alpha_\ell(L, A) \tag{1}$$

with some constant c.

We recall that for an integral lattice of positive determinant and even rank Siegel [6] for degree one and Maaß [4] for arbitrary degree defined a holomorphic theta series in the indefinite case whose Fourier coefficients are proportional to the

product of the local densities of that lattice, subject to the restriction that the signature (m_+, m_-) satisfies the condition $\min(\frac{m_+ + m_- - 3}{2}, m_+, m_-) \geqslant n$. Denote this theta series (if it is defined) for $\tilde{L}$, normalized such that its Fourier coefficient at A is equal to

$$c \cdot (\det A)^{\frac{m-n-1}{2}} (\det \tilde{L})^{\frac{n}{2}} \prod_{\ell \text{ prime}} \alpha_\ell(A, \tilde{L}),$$

by $\vartheta^{\mathrm{hol}}(\tilde{L}, z)$. If the signature condition is not satisfied, we use the same notation for the series with these Fourier coefficients (without knowing a priori whether this series defines a modular form).

Theorem 1. *Let p be a prime not dividing the discriminant of L.*

a) *For $1 \leqslant j \leqslant \frac{m-2}{4}$ there is a unique isometry class of rational quadratic spaces $\tilde{V} = (\tilde{V}, \tilde{q})$ of dimension m and the same discriminant as V such that*

$$\tilde{V}_\ell \cong \begin{cases} {}^pV_\ell & \text{if } p \neq \ell \\ V_p & \text{if } p = \ell \end{cases} \tag{2}$$

for finite primes ℓ and $\tilde{V}_\infty = \tilde{V} \otimes_{\mathbb{Q}} \mathbb{R}$ is either positive definite or of signature $(m - 2 - 4j, 2 + 4j)$.
$\tilde{V}$ carries a lattice $\tilde{L}$ such that

$$\tilde{L}_\ell \cong \begin{cases} {}^pL_\ell & \text{if } p \neq \ell \\ L_p & \text{if } p = \ell. \end{cases} \tag{3}$$

$\tilde{V}_\infty$ is indefinite if and only if $\chi(p) = -1$.

b) *Let the notations be as in a).*
Then $\vartheta^{(n)}(\mathrm{gen}\ L, z) \mid T(p) = \lambda_p(L)\vartheta^{(n)}(\tilde{L}, z)$ with

$$\lambda_p(L) = \prod_{j=1}^{n} (1 + \chi(p)p^{k-j}).$$

In particular, the series $\vartheta^{(n)}(\mathrm{gen}\ \tilde{L}, z)$ defines a modular form of the same level as L for all $n < k$.

c) *If the level N of L is prime, the theta series $\vartheta^{(n)}(\tilde{L}, z)$ of the indefinite lattice $\tilde{L}$ can be explicitly expressed as a linear combination of the theta series of the genera $\mathrm{gen}(L_i)$ of the (positive definite) lattices on V of the same level as L.*

We let now (V', L') denote one of $(V, L), (\tilde{V}, \tilde{L})$. In the representation theoretic framework both types of theta series occurring above are expressed as theta integrals over the adelic orthogonal group with the help of the oscillator or Weil representation ω of $\mathrm{Sp}_n(\mathbb{A}) \times O_{(V',q')}(\mathbb{A})$ acting on the Schwartz-Bruhat space $S((V'(\mathbb{A}))^n)$:

With the theta kernel $\theta(g, h; \varphi) = \sum_{x \in V'(\mathbb{Q})} \omega(g)\varphi(h^{-1}x)$, where $g \in \mathrm{Sp}_n(\mathbb{A})$,

$h \in O_{(V',q')}(\mathbb{A})$, $\varphi \in S((V(\mathbb{A}))^n)$, the Siegel-Weil theorem gives that the theta integral

$$I(g;\varphi) = \int_{O_{(V,q')}(\mathbb{Q}\backslash O_{(V,q')}(\mathbb{A}))} \theta(g,h,\varphi)dh$$

is the value at $s_0 = \frac{m-n+1}{2}$ of an Eisenstein series on the adelic symplectic group. For a suitable test function φ (depending on the lattice at hand) the theta integral $I(g;\varphi)$ is proportional to the function on the group $\mathrm{Sp}_n(\mathbb{A})$ that corresponds to the holomorphic theta series of the (genus of the) lattice L respectively of $\tilde{L}$ discussed above.

Moreover, the Siegel-Weil theorem also gives a natural intertwining operator $\lambda : S(V'(\mathbb{A})) \longrightarrow I(s_0,\chi)$ (where $I(s_0,\chi)$ is a principal series representation of $\mathrm{Sp}_n(\mathbb{A})$ depending only on χ) which factors into a product $\lambda = \prod_v \lambda_v$ over all places v of $\mathbb{Q}$.

Theorem 2. *(Matching principle, Kudla) Let V_1, V_2 be quadratic spaces over $\mathbb{Q}$ of the same dimension m and discriminant d. Then two test functions $\varphi_1 \in S(V_1(\mathbb{A}))$ and $\varphi_2 \in S(V_2(\mathbb{A}))$ match if $\lambda_1(\varphi_1) = \lambda_2(\varphi_2)$.*

If two test functions $\varphi_1 \in S(V_1(\mathbb{A}))$ and $\varphi_2 \in S(V_2(\mathbb{A}))$ match as above, one has an identity of theta integrals $I(g;\varphi_1) = I(g;\varphi_2)$. Such an identity expresses nontrivial relations between the arithmetic properties of the quadratic spaces V_1, V_2.

The existence of matching test functions for a pair of quadratic spaces can often be proved by representation theoretic arguments. In such cases it is of interest to exhibit matching test functions explicitly.

We can now state the contribution of our computations to the matching principle discussed above:

Theorem 3. *Let L be of prime level N and of non-square discriminant d, let p be a prime with $\chi(p) = -1$. Let $n = 1$ and let $\varphi \in S(V(\mathbb{A})), \tilde{\varphi} \in S(\tilde{V}(\mathbb{A}))$ be the test functions giving the classical theta series for the genus of positive definite lattices $\mathrm{gen}(L)$ and the indefinite lattice $\tilde{L}$ from Theorem 1 respectively.*

Let $\vartheta(\mathrm{gen}(L))|_{T(p)} = \sum c_i \vartheta(\mathrm{gen}(L_i))$ be the explicit linear combination of theta series of all the positive definite genera of lattices of level N and discriminant in $d \cdot (\mathbb{Q}^\times)^2$ given by Theorem 1, let ψ_i be the test function attached to the positive definite lattice L_i as above.

Then the test functions $\psi := \sum_i c_i \psi_i \in S(V(\mathbb{A}))$ and $\tilde{\varphi} \in S(\tilde{V}(\mathbb{A}))$ match and we have $I(g,\psi) = I(g,\tilde{\varphi})$.

The result given above can be generalized to square free level and to higher degree n of the theta series or integrals.

References

[1] H. Katsurada, R. Schulze-Pillot: *Hecke operators and genus theta series of nebentype*, Preprint 2004

[2] S. S. Kudla, *Integrals of Borcherds forms*, Comp. Math. **137** (2003), 293-349

[3] S. S. Kudla, J. J. Millson, *The theta correspondence and harmonic forms I*, Math. Ann. **274** (1986), 353–378.

[4] H. Maass, *Modulformen zu indefiniten quadratischen Formen* Math. Scand. **17** (1965), 41–55.
[5] T. Oda, *A note on a geometric version of the Siegel formula for quadratic forms of signature* $(2, 2k)$, Sci. Rep. Niigata Univ. Ser. A **20** (1984), 13–24.
[6] C. L. Siegel, *Indefinite quadratische Formen und Modulfunktionen*, Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948, pp. 395–406. Interscience Publisher, Inc., New York, 1948.

Algebraic lattices and channel coding for digital transmission

Emanuele Viterbo
(joint work with E. Bayer-Fluckiger, J-C. Belfiore, F. Oggier, G. Rekaya)

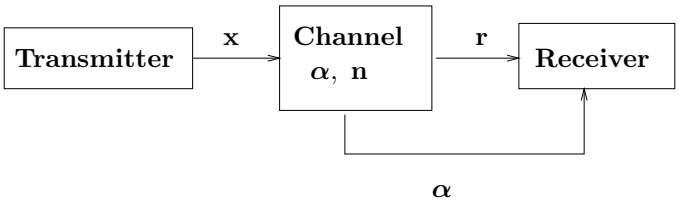
This survey talk presents some applications of algebraic lattices to the problem of code design for digital transmission over fading channels.

1. Algebraic lattices for Rayleigh fading channels

We consider the following communication problem (see the figure below). A transmitter sends a codeword $\mathbf{x}$ through a wireless channel. Since the channel attenuates the signal (this is modeled by the fading $\boldsymbol{\alpha}$) and adds noise ($\mathbf{n}$), we model the modified codeword at the receiver by

$$\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n},$$

where $*$ represents the component-wise vector product. We have that $r_i = \alpha_i x_i + n_i$ for $i = 1, 2, \ldots n$, where the α_i are independent real Rayleigh random variables and n_i are real Gaussian random variables with mean zero and variance σ^2.



The problem that we address is the design of a *codebook* or a *signal constellation* S for this channel, that is, a finite set of points in $\mathbb{R}^n$. In order to derive code design criteria, we estimate the error probability of this transmission system. Assuming the receiver estimates the channel (i.e. $\boldsymbol{\alpha}$), one can estimate the probability that the codeword $\mathbf{y}$ is received while the codeword $\mathbf{x}$ was sent, which is

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{\mathbf{1}}{\mathbf{2}} \prod_{\mathbf{x_i} \neq \mathbf{y_i}} \frac{\mathbf{8}\sigma^{\mathbf{2}}}{(\mathbf{x_i} - \mathbf{y_i})^{\mathbf{2}}} = \frac{\mathbf{1}}{\mathbf{2}} \frac{(\mathbf{8}\sigma^{\mathbf{2}})^{\mathbf{l}}}{\mathbf{d_p^{(l)}}(\mathbf{x}, \mathbf{y})^{\mathbf{2}}}$$

where $d_p^{(l)}(\mathbf{x}, \mathbf{y})$ is the *l-product distance* of $\mathbf{x}$ from $\mathbf{y}$, when these two codewords differ in l components, i.e., $d_p^{(l)}(\mathbf{x}, \mathbf{y}) = \prod_{\mathbf{x_i} \neq \mathbf{y_i}} |\mathbf{x_i} - \mathbf{y_i}|$. The minimum number of

distinct components between any two codewords $L = \min(l)$ is called the *modulation diversity* or *diversity order* of S.

To obtain a good codebook (with a low error probability), we have to:

(1) Maximize the diversity $L = \min(l)$.
(2) For a given L, maximize the minimum product distance

$$d_{p,min} = \min_{\mathbf{x} \neq \mathbf{y}} d_p^{(L)}(\mathbf{x}, \mathbf{y})$$

under the constraint of bounded average energy $\mathcal{E}_S = \frac{1}{|S|} \sum_{x \in S} \|\mathbf{x}\|^{\mathbf{2}}$.

In the design of the signal constellations, two fundamental operations should also be kept in mind: *bit labelling* and *constellation shaping*.

Bit labelling consists in mapping bits to signal points and vice-versa, and is best performed by an efficient algorithm. On the other hand, it is well known that lattice constellations bounded by a sphere have the best shaping gain. Unfortunately, labelling algorithmically a spherically shaped constellation is not easy. Cubic shaped constellations offer a good trade-off: they are only slightly worse in terms of shaping gain but are usually very easy to label.

Moreover, the complexity of the general decoding problem suggests to use constellations with lattice structure for which a more efficient decoder is available.

We conclude that good signal constellations are provided by rotated $\mathbb{Z}^n$–lattices, which have full diversity and maximal minimum product distance.

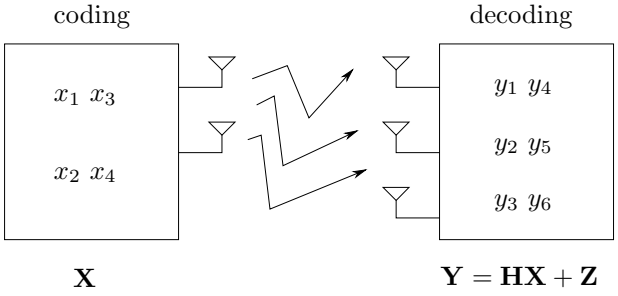
These $\mathbb{Z}^n$-lattices can be constructed via the embedding of a number field. Furthermore, both their diversity and minimum product distance can be related to the properties of the underlying number field. Constructions of such lattice codes and their performance analysis can be found in [1] while a complete survey is given in [2].

2. Algebraic lattices for coherent MIMO channels

We consider the following communication problem (see the figure below). We have a transmitter with M_t transmit antennas and a receiver with M_r receive antennas. If $\mathbf{y}(k) \in \mathbb{C}^{M_r}$ is the received (column) vector at time k, we can write

$$\mathbf{y}(k) = \mathbf{H}(k)\, \mathbf{x}(k) + \mathbf{z}(k) \ ,$$

where the matrix $\mathbf{H}(k) \in \mathbb{C}^{M_r \times M_t}$ represents the channel, the column vector $\mathbf{x}(\mathbf{k}) \in \mathbb{C}^{\mathbf{M_t}}$ is the channel input and $\mathbf{z}(k) \in \mathbb{C}^{M_r}$ is zero mean i.i.d. Gaussian noise.



The channel is assumed to be block time-invariant, that is, $\mathbf{H}(k)$ is independent of k over a transmission block of m symbols, say $\mathbf{H}(k) = \mathbf{H}$. Looking at a single block of length m, during which the channel is assumed to be time-invariant, we can write

$$\mathbf{Y_{M_r \times m}} = \mathbf{H_{M_r \times M_t}} \mathbf{X_{M_t \times m}} + \mathbf{Z_{M_r \times m}} \ .$$

Information symbols are taken from a complex signal constellation (or alphabet) $\mathcal{A} \subset \mathbb{Z}[i]$ (the Gaussian integers) or $\mathbb{Z}[j]$ (the Eisenstein integers), and are encoded into the codewords $\mathbf{X}$.

The problem that we address is the design of a *codebook* or *space-time block code* $\mathcal{C}$ for this channel, in the case where $M_t = M_r = m$, that is, we have the same number of transmit and receive antennas. If we furthermore assume that the receiver has perfect knowledge of all the channel coefficients (*coherent case*), it has been shown that minimizing the probability of error requires to maximize

$$\min_{\mathbf{X} \neq \mathbf{\tilde{X}} \in \mathcal{C}} |\det(\mathbf{X} - \mathbf{\tilde{X}})|^{\mathbf{2}}.$$

Cyclic division algebras naturally provide a linear family of invertible matrices, thus codebooks whose minimum determinant is ensured to be different from zero. We further exploit the algebraic structure of the algebra to get

(1) a shaping constraint: vectorized codewords have to be points of a $\mathbb{Z}[i]^n$ (resp. $\mathbb{Z}[j]^n$) lattice with diversity, which is obtained algebraically, as in the previous section.
(2) a non-zero lower bound on the minimum determinant even when increasing the size of $\mathcal{A}$.

The above conditions appear to be a key point in improving the performance of these codes and define the so called *perfect space-time block codes*. In [7] the 2×2 Golden code is presented and in [8] all other perfect space-time codes are given, which appear only for 3×3, 4×4 and 6×6 MIMO systems.

References

[1] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, *New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel*, IEEE Transactions on Information Theory, vol. 50, no. 4, pp. 702–714, April 2004.

[2] F. Oggier, E. Viterbo, *Algebraic number theory and code design for the Rayleigh fading channel*, Foundations and Trends in communication and information theory, vol. 1.
[3] M. O. Damen, A. Tewfik, and J.-C. Belfiore, *A construction of a space-time code based on the theory of numbers*, IEEE Trans. Inform. Theory, vol. 48, no. 3, pp. 753–760, March 2002.
[4] H. El Gamal and M. O. Damen, *Universal space-time coding*, IEEE Trans. Inform. Theory, vol. 49, no. 5, pp. 1097–1119, May 2003.
[5] J.-C. Belfiore and G. Rekaya, *Quaternionic lattices for space-time coding*, in Proceedings of the Information Theory Workshop, Paris, March 31–April 4, 2003.
[6] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, *Full-diversity, high-rate space-time block codes from division algebras*, IEEE Trans. Inform. Theory, vol. 49, pp. 2596–2616, October 2003.
[7] J.-C. Belfiore, G. Rekaya, E. Viterbo, *The Golden code: A 2x2 full-rate space-time code with non vanishing determinants*, to appear in IEEE Trans. on Information Theory, 2005.
[8] F. Oggier,J.-C. Belfiore, G. Rekaya, E. Viterbo, *Perfect space-time codes*, submitted to IEEE Trans. on Information Theory, Aug. 2004.

Arakelov class groups and ideal lattices

René Schoof

In his 1972 Boulder paper [10], Daniel Shanks observed that the quadratic forms in the principal cycle of reduced binary quadratic forms of positive discriminant exhibit a group-like behavior. This was a surprising phenomenon, because the principal cycle itself constitutes the trivial class of the class group. Shanks called this group-like structure 'inside' the neutral element of the class group the *infrastructure*. He exploited it by designing an efficient algorithm to compute regulators of real quadratic number fields. Eight years later, Hendrik Lenstra made Shanks's observations more precise. He introduced a certain topological group and provided a satisfactory framework for Shanks's algorithm [4], [9]. Both Shanks and Lenstra indicated that the infrastructure ideas could be generalized to arbitrary number fields. In 1988, Buchmann [2], [3] described an algorithm for computing the class group and regulator of an arbitrary number field that, under reasonable assumptions, has a subexponential running time. It has been implemented in the LiDIA, MAGMA and PARI software packages [6], [7], [8].

In this talk we present a natural setting for the infrastructure phenomenon and for Buchmann's algorithm. It is provided by Arakelov theory [11], [12], [13]. We show that Buchmann's algorithm for computing the class number and regulator of a number field F has a natural description in terms of the *Arakelov class group* Pic_F^0 of F and the set Red_F of *reduced Arakelov divisors*. We show that Lenstra's topological group is essentially equal to the Arakelov class group of a real quadratic field. We also introduce the *oriented Arakelov class group* $\widetilde{\mathrm{Pic}}_F^0$. This is a natural generalization of Pic_F^0, useful for analyzing Buchmann's algorithm and for computing the units of the ring of integers O_F themselves rather than just the regulator. Since Arakelov divisors of number fields can be viewed as ideal lattices [1], lattice reduction algorithms [5] play an important role.

References

[1] Bayer, E.: Lattices and number fields, *Contemp. Math.* **241** (1999), 69–84.
[2] Buchmann, J.: *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, pp. 27–41 in C. Goldstein (ed): "Séminaire de Théorie des Nombres, Paris 1988–1989", Birkhäuser, Boston, 1990.
[3] Buchmann, J. and Düllmann, S.: A probabilistic class group and regulator algorithm
[4] Lenstra, H.W.: On the computation of regulators and class numbers of quadratic fields. In *Proc. Journées Arithmétiques Exeter 1980*, London Math. Soc. Lect. Notes **56** (1982), p. 123–150.
[5] Lenstra, A.K., Lenstra, H.W. and Lovász, L.: Factoring polynomials with rational coefficients, *Math. Annalen* **261** (1982), 515–534.
[6] LiDIA, A C++ Library For Computational Number Theory, Homepage: `www.informatik.tu-darmstadt.de/TI/LiDIA`
[7] The Magma Computational Algebra System for Algebra, Number Theory and Geometry, Homepage: `magma.maths.usyd.edu.au/magma`
[8] Pari-GP, Homepage: `www.parigp-home.de`
[9] Schoof, R.: *Quadratic fields and factorization*, pp. 235–286 in: H.W. Lenstra jr. and R. Tijdeman (eds.): "Computational Methods in Number Theory", MC-Tracts **154-155**, Amsterdam 1982.
[10] Shanks, D.: The infrastructure of a real quadratic field and its applications, *Proceedings of the 1972 Number Theory Conference*, Boulder (1972) 217–224.
[11] Szpiro, L.: Présentation de la théorie d'Arakelov, p. 279–293 in "Current Trends in Arithmetical Algebraic Geometry", *Contemporary Mathematics* **67**, AMS, Providence RI 1985.
[12] Szpiro, L.: Degrés, intersections, hauteurs, p. 11–28 in "Séminaire sur les pinceaux arithmétiques: La conjecture de Mordell", *Astérisque* **127** (1985).
[13] Van der Geer, G. and Schoof, R.: Effectivity of Arakelov divisors and the Theta divisor of a number field, *Selecta Mathematica*, New Ser. 6 (2000), 377–398. Preprint 9802121 at: `http://xxx.lanl.gov/list/math.AG/9802`.

Voronoi graphs, cells, and spherical designs

Jacques Martinet
(joint work with Anne-Marie Bergé)

Abstract. We discuss here various questions related to Voronoi's theory: the cellular decomposition of the space of positive definite quadratic forms over $\mathbb{R}^n$, the Voronoi graph, "mass formulae with signs", and spherical 2- (= 3-) designs. The text below is essentially a survey, except its last part, in which we present some recent constructions of strongly eutactic lattices. It is closely related to Elbaz-Vincent's talk [E].

1. The cell complex.

We fix an integer $n \geqslant 2$. We represent elements $x \in \mathbb{R}^n$ by column-matrices X. Let $\mathcal{Q}_n$ be the set of positive definite quadratic forms over $\mathbb{R}^n$. We identify $Q \in \mathcal{Q}_n$ with $A \in \mathrm{Sym}_n(\mathbb{R})$ such that $Q(x) = {}^tXAX$, and denote by $S(Q)$ or simply by S its set of *minimal vectors*; we moreover set $s = \frac{1}{2}|S|$. The *perfection rank* $\mathrm{perf}\, Q$ *of* Q is the rank of the set of matrices $X\,{}^tX \subset \mathrm{Sym}_n(\mathbb{R})$ for $x \in S$; we

say that Q is *perfect* if $\operatorname{perf} Q = \frac{n(n+1)}{2}$, the dimension of $\mathrm{Sym}_n(\mathbb{R})$. A *perfection* (resp. *eutaxy*) *relation on* S is a relation of the form

$$\sum_{x\in S} \lambda_x\, X^t X = 0 \quad (\text{resp. } \sum_{x\in S} \lambda_x\, X^t X = A^{-1})\,.$$

We say that Q is *weakly eutactic* if it possesses a eutaxy relation, and *semi-eutactic* (resp. *eutactic*) if there exists such a relation with non-negative (resp. strictly positive) coefficients.

[Note that perfection is a property of the set S whereas eutaxy, which involves convexity, does depend on Q.]

We now fix the minimum of the forms we consider and restrict ourselves to *well rounded* forms (those with $\operatorname{rk} S = n$). With S we associate the set $\mathcal{C}_S = \{Q \in \mathcal{Q}_n \mid S(Q) = S\}$. If non-empty, this is an open convex polyhedron in $\mathrm{Sym}_n(\mathbb{R})$ of dimension $\frac{n(n+1)}{2} - \operatorname{perf} S$ (the *perfection co-rank of* S). The collection of these sets is a cellular decomposition of $\mathcal{Q}_n$. Cells of dimension 0 and 1 are the vertices and the edges of the Voronoi graph.

In the talk, we briefly described an algorithm relying on the consideration of the set of perfection relations which, given the set S of minimal vectors of a cell $\mathcal{C}$, lists all cells $\mathcal{C}'$ with $\operatorname{perf}\mathcal{C}' = \operatorname{perf}\mathcal{C} - 1$. It uses the fact that the *Bacher matrix* $\mathrm{Bc} = S\,{}^tS = \sum_{x\in S} X^t X$ *of* S (the *barycentre matrix* in [E-G-S]) characterizes $\mathcal{C}$ up to equivalence. Note that a fast algorithm starting from perfect forms occurs in [E-G-S].

We also outlined an alternative method, relying on Watson's index theory (see [M1]) which could be used to classify cells with not too large $s - n$ in dimensions 7 and 8. (According to [E-G-S], interesting information on the cohomology of $\mathrm{SL}_n(\mathbb{Z})$ can be obtained using such a classification.)

Recall that the Hermite invariant of $Q \in \mathcal{Q}_n$ is $\gamma(Q) = \dfrac{\min Q}{\det(Q)^{1/n}}$. About ten years ago, we proved that a cell $\mathcal{C}$ contains at most one weakly eutactic form $E_{\mathcal{C}}$, and that the minimum of γ on $\overline{\mathcal{C}}$ is attained at $E_{\mathcal{C}}$ if $E_{\mathcal{C}}$ exists and in some cell $\mathcal{C}' \subset \overline{\mathcal{C}}\smallsetminus\mathcal{C}$ otherwise; see [M], Section 9.4.

Questions. Can one decide whether a given integral matrix is the Bacher matrix for some class ? How to construct this class if it exists ? Is there a fast algorithm to decide from its Bacher matrix whether a given class contains a (weakly) eutactic form ?

2. Mass formulae with signs.

We refer to two formulae, due to Bavard ([Bv]) and Ash ([Ash]), which both take the form of a summation on cells modulo equivalence

$$\sum_{\mathcal{C}/\sim} \frac{(-1)^{i(\mathcal{C})}}{|\mathrm{Aut}^+(\mathcal{C})|} = \chi(\mathrm{SL}_n(\mathbb{Z}))\,,$$

but differ by the domain of summation: all (well rounded) cells in Bavard's, only those which contain a eutactic lattice in Ash's; the exponent $i(\mathcal{C})$ is the perfection co-rank; $\mathrm{Aut}^+(\mathcal{C})$ is the stabilizer in $\mathrm{SL}_n(\mathbb{Z})$ of $\mathcal{C}$; $\chi(\mathrm{SL}_n(\mathbb{Z}))$, the *Euler Characteristic of* $SL_n(\mathbb{Z})$, is zero for all $n \geqslant 3$, $\zeta(-1) = -\frac{1}{12}$ for $n = 2$.

Bavard's formula is related to the action of $\mathrm{SL}_n(\mathbb{Z})$ on a symmetric space, whereas Ash's relies on topological Morse theory and an interpretation of eutactic forms as non-degenerate critical points. Of course, the sum must be zero on cells which either contain no weakly eutactic form, or contain a weakly eutactic, non-eutactic form. In dimensions $n \leqslant 5$, these two types of cells can be regrouped in pairs having the same automorphism group and whose co-ranks differ by 1, hence obviously cancel. This is not general. However, some experiments suggest that a kind of "local" cancellation could be generally true, which would allow one to deduce one formula from the other, despite their different original proofs.

3. Strongly eutactic lattices.

In this section, we use for convenience the language of lattices; $S(\Lambda)$ denotes the set of minimal vectors of a lattice Λ. We refer to Venkov's paper in [M-V] for the definition of a spherical t-design. We say that a lattice Λ is *strongly eutactic* if $S(\Lambda)$ is a spherical 2-design. This is equivalent to the existence of a eutaxy relation with *equal* (hence strictly positive) coefficients. We shall also consider *strongly semi-eutactic* lattices, which have equal *non-zero* coefficients; then the set of minimal vectors whose corresponding eutaxy coefficients are non-zero is a spherical 2-design.

In a recent work, we have tried to classify strongly eutactic lattices Λ having a basis of minimal vectors for which $s-n$ is small. The result is well-known for $s = n$ (the eutactic configurations of lines are the sets of n pairwise orthogonal lines) and easy for $s = n + 1$ (one only finds $\mathbb{A}_n^*$). For $s = n + 2$, we have proved that these lattices are either reducible, and then similar to a direct sum $\mathbb{A}_m^* \perp \mathbb{A}_m^*$, $n = 2m$, or belong to an infinite two-parameters family, of dimensions $n = k(4\ell^2 - 1) - 2$, with n large enough with respect to k.

[For some slightly too small values of n, we obtain only strongly semi-eutactic lattices.
Example: $\ell = 1$, $k = 2$, hence $n = 4$; here, $s = 7$ but the 2-design we obtain has $s = 6$.]

For $s = n+3$, results become complicated. This nevertheless suffices to classify all strongly eutactic lattices with $s \leqslant n + 3$ for, say, $n \leqslant 100$.

We have also constructed infinite families whose configuration of minimal vectors is derived from that of the root lattice $\mathbb{A}_n$ (e.g., with $s = \frac{n^2-1}{2}$, $n \geqslant 3$ odd, or with $s = \frac{(n+1)(n-2)}{2}$, $n \equiv 2 \mod 3$, $n \geqslant 5$).

The table below is an update of Table 3.1 of [M-V]. Using the Bacher matrix, the classification of strongly eutactic and semi-eutactic cells easily follows from that of all cells, due to Batut ([Bt]) in dimensions $n \leqslant 5$ and to Elbaz-Vincent and Gangl (see [E]) in dimension 6. (Previously, 20 strongly eutactic, 6-dimensional lattices were known, 19 listed in [M-V] and 1 in [Be-M].) For numerical data on 2- and 4-designs related to lattices, see http://math.u-bordeaux.fr/~martinet/ .

Low-dimensional strongly eutactic lattices

dimension	1	2	3	4	5	6
well-rounded cells	1	2	5	18	136	5634
eutactic	1	2	5	16	118	??
strongly eutactic	1	2	3	6	9	21
semi-eutactic	0	0	0	1	5	??
strongly semi-eutactic	0	0	0	1	1	6

References

[Ash] A. Ash, *On eutactic forms*, Can. J. Math. **29** (1977), 1040–1054.

[Bt] C. Batut, *Classification of quintic eutactic forms*, Math. Comp. **70** (2000), 395–417.

[Bv] C. Bavard, *Classes minimales des réseaux et rétractions géométriques équivariantes dans les espaces symétriques*, J. London Mat. Soc. **64** (2001), 275–286.

[Be-M] A.-M. Bergé, J. Martinet, *Symmetric Groups and Lattices*, Monatshefte Math. **140** (2003), 179–195.

[EM] J. Martinet (ed.), *Réseaux euclidiens, designs sphériques et formes modulaires*, L'Ens. Math., Monographie **37**, Genève (2001).

[E] Philippe Elbaz-Vincent, this conference.

[E-G-S] Philippe Elbaz-Vincent, Herbert Gangl, Christophe Soulé, in preparation; see also [E].

[M] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren **327**, Springer-Verlag, Heidelberg (2003).

[M1] J. Martinet, *Sur l'indice d'un sous-réseau*, [EM], 163–211.

[M-V] J. Martinet, B. Venkov, *Les réseaux fortement eutactiques*, [EM], 112–134.

[V] B. Venkov, *Réseaux et designs sphériques*, [EM], 10–86.

Unimodular hermitian lattices

Kanat Abdukhalikov

(joint work with Rudolf Scharlau)

In 1978 W. Feit [7] described all unimodular hermitian lattices of dimensions up to 12 over the ring of integers in $\mathbb{Q}(\sqrt{-3})$. They all have roots, that is, vectors of norm 1 or 2. Dimension 13 is the first case where a unimodular root-free lattice appears [1, 3, 15]. All unimodular lattices in dimension 13 are classified in [2]. It turns out that the lattice without roots is unique. It has minimum norm 3 and its automorphism group is isomorphic to the group $\mathbb{Z}_6 \times \mathrm{PSp}_6(3)$ of order $2^{10} \cdot 3^{10} \cdot 5 \cdot 7 \cdot 13$. The remaining lattices all have root systems of rank 12.

In this talk we are going to report on recent work extending the above results to dimensions 14 and 15. Such a classification is of interest in the broader context of investigating modular lattices over the rational integers in the sense of Quebbemann [11]. In particular, the question of existence and uniqueness of extremal modular lattices has turned out to be very interesting from several perspectives

(sphere packings, modular forms, finite groups) and has been studied by many authors in the past 10 years.

Before stating the result more precisely, we give some definitions and notation. Let ω denote a primitive cube root of 1. Then $\mathbb{Z}[\omega]$, the ring of Eisenstein integers, is the ring of integers in the field $\mathbb{Q}(\sqrt{-3})$. Let V be a vector space over $\mathbb{Q}(\sqrt{-3})$ with a positive definite hermitian product $(-,-)$. A *lattice* L on V is a finitely generated, in fact free, $\mathbb{Z}[\omega]$-module in V containing a basis $v_1, \ldots, v_n$ of V. We further assume that $(x, y) \in \mathbb{Z}[\omega]$ for all x, $y \in L$. The matrix with entries (v_i, v_j) is called the *Gram matrix* of L (with respect to the given basis), its determinant is called the *discriminant* $d(L)$ of L. The lattice L is *unimodular* if $d(L) = 1$. The *norm* of a vector $x \in L$ is $N(x) = (x, x)$. The minimum norm, or just *minimum*, of a lattice L is $\min\{N(x, x) \mid x \in L,\ x \neq 0\}$. The group $G(L)$ of all automorphisms of L which preserve the form is finite. Any lattice can be uniquely decomposed into (orthogonally) *indecomposable* lattices.

Theorem

a) There are precisely 58 *indecomposable unimodular lattices over* $\mathbb{Z}[\omega]$ *of dimension* 14. *One of them has no roots; the remaining lattices have root systems of ranks* 6, 8, 10, 11, 12, 13, *and* 14. *The root-free lattice has minimum norm* 3 *and automorphism group* $\mathbb{Z}_6 \times \mathrm{G}_2(3).2$ *of order* $2^8 \cdot 3^7 \cdot 7 \cdot 13$.

b) There are precisely 259 *indecomposable unimodular lattices over* $\mathbb{Z}[\omega]$ *of dimension* 15. *For any integer number* r *from* 0 *to* 15 *there is an indecomposable unimodular lattice of dimension* 15 *with root system of rank* r. *There are precisely two root-free lattices, with minimum norm* 3. *One of them is isometric to the exterior square* $U_6 \wedge U_6$ *of the unimodular lattice* U_6 *of rank* 6 *and has automorphism group* $\mathbb{Z}_2 \times 3.\mathrm{U}_4(3).2$ *of order* $2^9 \cdot 3^7 \cdot 5 \cdot 7$. *The second root-free lattice has automorphism group* $\mathbb{Z}_2 \times (3_+^{1+2} \times 3_+^{1+2}).\mathrm{SL}_2(3).2$ *of order* $2^5 \cdot 3^7$.

This classification illustrates the fact that hermitian lattices can be fully classified in certain cases where the classification of the corresponding modular $\mathbb{Z}$-lattices (here: 3-modular of dimensions 28 and 30) appears totally hopeless since at the same time the dimension and the class number are too large.

Our result is heavily based on the computer program `hn` by A. Schiemann [15] which determines neighbours (in the sense of Kneser) of a given lattice and computes the order of the automorphism group $G(L)$. In addition to the neighbour method we have used various other techniques for the construction of lattices, such as representations of finite groups, hand computations, codes over $\mathbb{F}_4$ and more generally root systems and gluing. For certain calculations, the Magma Computational Algebra System [4] has been used. The completeness of our list has been checked by the well known mass formula (see [7]), using the known group orders.

Some lattices are constructed with the help of self-dual codes of length 14 over $\mathbb{F}_4$. These codes have been classified in [5, 9]. Let φ denote the canonical mapping $\mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/2\mathbb{Z}[\omega] \cong \mathbb{F}_4$. Then for any self-dual code C of length 14 over $\mathbb{F}_4$ the

lattice

$$L = \frac{1}{\sqrt{2}}\langle (a_1, \ldots, a_{14}) \in I_{14} \mid (\varphi(a_1), \ldots, \varphi(a_{14})) \in C \rangle$$

is a unimodular lattice of dimension 14. In particular, one lattice is constructed with the help of the quadratic residue code [8] of length 14 over $\mathbb{F}_4$. Recall [1] that the unimodular root-free lattice of dimension 13 can also be constructed from the quadratic residue code of length 14.

Let us consider some further examples. There is a unimodular 15-dimensional lattice Λ with root system A_2 which is obtained by gluing a 2-dimensional lattice with root system A_2 and a 13-dimensional lattice Λ' with discriminant 3. Its automorphism group is isomorphic to $6.(\mathrm{S}_3 \times \mathrm{PSL}_2(27).3)$. Therefore $\mathrm{Aut}(\Lambda') \cong 6.(\mathrm{PSL}_2(27).3)$ and Λ' is associated with the irreducible complex character of the group $\mathrm{PSL}_2(27)$ of degree 13. It is the Weil character and it can indeed be realized over $\mathbb{Z}[\omega]$ (see [12]).

Similarly, there is a 15-dimensional unimodular lattice with root system A_1 with automorphism group $6.(\mathrm{S}_2 \times \mathrm{PSL}_2(13))$. It is obtained from a 14-dimensional lattice of discriminant 2 with automorphism group $6.\mathrm{PSL}_2(13)$. The corresponding vector space gives rise to an irreducible complex character of the group $\mathrm{PSL}_2(13)$ of degree 14.

As mentioned above, the unimodular 14-dimensional lattice of minimum norm 3 produces an extremal euclidean 3-modular 28-dimensional lattice (see [6, 13, 14] for more information on extremal and modular lattices). This 3-modular lattice also appears in [10] since its automorphism group is a rational irreducible maximal finite subgroup of $\mathrm{GL}_{28}(\mathbb{Q})$. The situation is completely analogous for one of the two 15-dimensional lattices of minimum norm 3. Independently of matrix groups, the two root-free lattices of dimension 15 were found previously by Schiemann [15], performing computations in the course of the works [13, 14] on euclidean extremal lattices.

There is one interesting observation in dimension 14 which did not occur in other dimensions.

Proposition *Every hermitian indecomposable unimodular lattice of dimension* 14 *has exactly* 17472 *vectors of norm* 3.

This is proved using an explicit basis of the appropriate space of modular forms which has dimension 3 in this case (see [11]).

To summarize all results known so far, the following table shows the number of indecomposable unimodular hermitian lattices of dimensions up to 15.

Dimension	1	6	8	9	10	11	12	13	14	15
Number of indecomposable lattices	1	1	1	1	2	2	11	14	58	259

The next two tables show the number of unimodular lattices in dimensions 14 and 15, respectively, with root system of given rank.

root rank	0	6	8	10	11	12	13	14	
number of lat.	1	1	2	4	4	12	12	22	58

root rk	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
number	2	1	2	2	2	4	4	8	11	11	27	31	55	54	34	11	259

References

[1] K. S. Abdukhalikov, *Invariant hermitian lattices in the Steinberg module and their isometry groups*, Commun. Algebra **25** (1997), no. 8, 2607–2626.

[2] K. S. Abdukhalikov, *Unimodular hermitian lattices in dimension 13*, J. Algebra **272** (2004), no. 1, 186–190.

[3] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Comb. Th. Ser. A **78** (1997), 92–119.

[4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp., **24**, 3/4 (1997), 235–265.

[5] J. H. Conway and N. J. A. Sloane, *Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16*, IEEE Trans. Inform. Theory **25** (1979), 312–322.

[6] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Springer-Verlag New York, Inc., 1999.

[7] W. Feit, *Some lattices over* $\mathbf{Q}(\sqrt{-3})$, J. Algebra **52** (1978) 248–263.

[8] J. H. van Lint, F. J. MacWilliams, *Generalized quadratic residue codes*, IEEE Trans. Inform. Theory **24** (1978), no. 6, 730–737.

[9] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, H. N. Ward, *Self-dual codes over $GF(4)$*, J. Combinatorial Theory, Ser. A **25** (1978) 288–318.

[10] G. Nebe, *Finite subgroups of $GL_n(\mathbb{Q})$ for $25 \leq n \leq 31$*, Commun. Algebra **24** (1996), no. 7, 2341–2397.

[11] H.-G. Quebbemann, *Modular lattices in euclidean spaces*, J. of Number Theory **54** (1995), 190–202.

[12] U. Riese, *On integral representations for* $\mathrm{SL}(2, q)$, J. Algebra **242** (2001) 729–739.

[13] R. Scharlau, R. Schulze-Pilot, *Extremal lattices*, in: B. H. Matzat, G.-M. Greuel, G. Hiss (Eds.), *Algorithmic Algebra and Number Theory*, Springer (1998), 139–170.

[14] R. Scharlau, A. Schiemann, R. Schulze-Pilot, *Theta series of modular, extremal, and hermitian lattices*, Proceedings of the Conference on Integral and Quadratic Forms and Lattices, Seoul 1998, Contemporary Math. **249** (1999), 221–233.

[15] A. Schiemann, *Classification of hermitian forms with the neighbour method*, J. Symbolic Comput. **26** (1998), no. 4, 487–508.

Model sets as generalizations of lattices

Michael Baake

(joint work with Daniel Lenz, Robert V. Moody)

Lattices in $\mathbb{R}^d$ have been studied for a long time, compare [10] and references therein, and can be considered as a well-understood paradigm of an ordered system, even though many open problems continue to challenge a large and active community. Key properties of a lattice $\varGamma \subset \mathbb{R}^d$ include its *Delone property* ($\varGamma$ is both uniformly discrete and relatively dense), *periodicity* ($\varGamma - \varGamma = \varGamma$), *coherence* (meaning that the dual object $\varGamma^* := \{x \in \mathbb{R}^d \mid e^{2\pi i x y} = 1 \text{ for all } y \in \varGamma\}$ is again a lattice), but also the *pure point diffractivity* of the lattice Dirac comb [11, 9] $\delta_\varGamma = \sum_{x \in \varGamma} \delta_x$ (which follows from Poisson's summation formula) and the *torus nature* of the appropriate orbit closure of $\{t + \varGamma \mid t \in \mathbb{R}^d\}$ (when viewed as a dynamical system under the continuous action of $\mathbb{R}^d$).

One particularly interesting class of generalizations consists of the so-called *Meyer sets* [19, 20]. In $\mathbb{R}^d$, they are the sets $\varLambda$ with the property that $\varLambda$ is relatively dense and $\varLambda - \varLambda$ is uniformly discrete. In particular, they are all Delone sets, while the converse is not true [16, 17]. Instead of periodicity, one now has $\varLambda - \varLambda \subset \varLambda + F$ with F a *finite* set, and coherence appears via relative denseness of the ε-duals $\varLambda^{\varepsilon} := \{x \in \mathbb{R}^d \mid |e^{2\pi i x y} - 1| < \varepsilon \text{ for all } y \in \varLambda\}$ for all $\varepsilon > 0$, see [20] for details. In general, pure point diffractivity is lost though [4], as is a "nice" structure of the dynamical system attached to $\varLambda$.

Among Meyer sets, model sets [22] probably form the best studied subclass. They are important examples of aperiodic order, and have proved useful as models of real world *quasicrystals*, which are solids with long-range aperiodic order and sharp diffraction images, the latter typically with non-crystallographic symmetries, see [2, 8, 21, 23, 27] for recent developments.

To construct a genuine model set, one starts with a lattice in a high-dimensional space and considers a partial "image" in a space of smaller dimension. This image will not be periodic any more, but still preserve many regularity features due to the periodicity of the underlying high-dimensional lattice structure. The approach can be extended to locally compact Abelian groups in a natural way. For a survey and further references, we refer the reader to [20, 22, 25].

Let us give a brief recapitulation of the abstract setting of a cut and project scheme and the definition of a model set, together with some of their important properties. We start from two locally compact Abelian groups, G and H, where G is also assumed to be σ-compact, see [26] for the reasons why this is needed. As usual, neutral elements will be denoted by 0 (resp. by $0_G, 0_H$). A *cut and project scheme* [25] emerges out of the following collection of groups and mappings:

$$
\begin{array}{ccccc}
G & \xleftarrow{\ \pi\ } & G \times H & \xrightarrow{\ \pi_{\mathrm{int}}\ } & H \\
\cup & & \cup & & \cup \text{ dense} \\
L & \xleftarrow{\ 1\text{-}1\ } & \tilde{L} & \longrightarrow & L^{\star} \\
\| & & & & \| \\
L & & \xrightarrow{\qquad\star\qquad} & & L^{\star}
\end{array}
\tag{1}
$$

Here, $\tilde{L}$ is a *lattice* in $G \times H$, i.e., a cocompact discrete subgroup. The canonical projection π is one-to-one between $\tilde{L}$ and L (in other words, $\tilde{L} \cap \{0_G\} \times H = \{0\}$), and the image $L^{\star} = \pi_{\mathrm{int}}(\tilde{L})$ is dense in H, the so-called internal space. In view of these properties of π and π_{int}, one defines the $\star$-map as $(.)^{\star} : L \longrightarrow H$ via $x^{\star} := \big(\pi_{\mathrm{int}} \circ (\pi|_{\tilde{L}})^{-1}\big)(x)$, where $(\pi|_{\tilde{L}})^{-1}(x) = \pi^{-1}(x) \cap \tilde{L}$, for all $x \in L$.

A *model set* [26, 22] is now any translate of a set of the form

$$
\curlywedge(W) \ := \ \{x \in L \mid x^{\star} \in W\} \tag{2}
$$

where the *window* W is a relatively compact subset of H with non-empty interior. Without loss of generality, we may assume that the stabilizer of the window, $H_W := \{c \in H \mid c + W = W\}$, is the trivial subgroup of H, i.e., $H_W = \{0\}$. If this were not the case (which could happen in compact groups H for instance), one could factor by H_W and reduce the cut and project scheme accordingly [26, 7].

Furthermore, we may assume that $\langle W-W\rangle$, the subgroup of H that is algebraically generated by the subset $W-W$, is the entire group, i.e., $\langle W-W\rangle = H$, again by reducing the cut and project scheme to this situation, compare [25, 26] for details.

There are variations on the precise requirement to W which depend on the fine properties of the model sets one is interested in, compare [22, 26, 6, 7]. In particular, a model set is called *regular* if ∂W has Haar measure 0 in H, and *generic* if, in addition, $\partial W \cap L^\star = \varnothing$. Regular, generic model sets are also *repetitive* [18, 22], i.e., each finite patch repeats itself with bounded gaps, and, in addition, does so with a well-defined frequency [25, 26].

A key feature of regular model sets, in the generality mentioned here, is their *pure point diffractivity*. This means that, given the Dirac comb $\delta_\varLambda$ of a regular model set, its autocorrelation measure $\gamma_\varLambda$ has a Fourier transform, denoted $\hat{\gamma}_\varLambda$, which is a positive, pure point measure, see [14, 15, 26, 9] and references therein for proofs of increasing generality. In this sense, model sets are really "almost lattices", and they also define very interesting dynamical systems [26, 5]. These are no longer torus-like, but have a local product structure of $G \times \mathcal{C}$, where $\mathcal{C}$ is a Cantor set, compare [1] and references therein. This, in turn, has rather interesting topological consequences on questions such as averaged shelling, patch frequencies and many other combinatorial properties, see [3].

As I have tried to indicate above, there are many properties of lattices that possess a very natural generalization to a larger class of point sets, such as Meyer sets or model sets. Quite often, this leads to new insight also to the "classical" problems, or to unexpected connections to other disciplines, both pure and applied. Some of the most fascinating aspects at present originate from the theory of dynamical systems [24, 7] with their relation to topological invariants [1], and from harmonic analysis and the theory of almost periodicity [12, 13].

References

[1] J. E. Anderson and I. F. Putnam, *Topological invariants for substitution tilings and their associated C^*-algebras*, Ergodic Th. & Dynam. Syst. **18** (1998), 509–537.

[2] M. Baake, *A guide to mathematical quasicrystals*, in: J.-B. Suck, M. Schreiber and P. Häussler (eds.), *Quasicrystals – An Introduction to Structure, Physical Properties, and Applications*, 17–48; `math-ph/9901014`.

[3] M. Baake and U. Grimm, *Combinatorial problems of (quasi-)crystallography* in: [27], 160–171; `math-ph/0212015`.

[4] M. Baake and M. Höffe, *Diffraction of random tilings: Some rigorous results*, J. Stat. Phys. **99** (2000), 219–261; `math-ph/9904005`.

[5] M. Baake and D. Lenz, *Dynamical systems on translation bounded measures: Pure point dynamical and diffraction spectra*, Ergodic Th. & Dynam. Syst. **24** (2004), 1867–1893; `math.DS/0302061`.

[6] M. Baake and D. Lenz, *Deformation of Delone dynamical systems and pure point diffraction*, J. Fourier Anal. Appl. (2005), in press; `math.DS/0404155`.

[7] M. Baake, D. Lenz and R. V. Moody, *A characterization of model sets by dynamical systems*, in preparation.

[8] M. Baake and R. V. Moody (eds.), *Directions in Mathematical Quasicrystals*, CRM Monograph Series, vol. 13, AMS, Rhode Island (2000).

[9] M. Baake and R. V. Moody, *Weighted Dirac combs with pure point diffraction*, J. Reine Angew. Math. (Crelle) **573** (2004), 61–94; `math.MG/0203030`.
[10] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer, New York (1999).
[11] J. M. Cowley, *Diffraction Physics*, 3rd ed., North-Holland, Amsterdam (1995).
[12] J. Gil de Lamadrid and L. N. Argabright, *Almost Periodic Measures*, Memoirs of the AMS, vol. 85, no. 428, AMS, Providence, RI (1990).
[13] J.-B. Gouéré, *Quasicrystals and almost periodicity*, Commun. Math. Phys. (2004), in press; `math-ph/0212012`.
[14] A. Hof, *On diffraction by aperiodic structures*, Commun. Math. Phys. **169** (1995), 25–43.
[15] A. Hof, *Diffraction by aperiodic structures*, in: [21], 239–268.
[16] J. C. Lagarias, *Meyer's concept of quasicrystal and quasiregular sets*, Commun. Math. Phys. **179** (1996), 365–376.
[17] J. C. Lagarias, *Geometric models for quasicrystals I. Delone sets of finite type*, Discr. Comput. Geom. **21** (1999), 345–372.
[18] J. C. Lagarias and P. A. B. Pleasants, *Repetitive Delone sets and quasicrystals*, Ergodic Th. & Dynam. Systems **23** (2003), 831–867; `math.DS/9909033`.
[19] Y. Meyer, *Algebraic Numbers and Harmonic Analysis*, North-Holland, Amsterdam (1972).
[20] R. V. Moody, *Meyer sets and their duals*, in: [21], 403–441.
[21] R. V. Moody (ed.), *The Mathematics of Long-Range Aperiodic Order*, NATO ASI Series C 489, Kluwer, Dordrecht (1997).
[22] R. V. Moody, *Model sets: A survey*, in: F. Axel, F. Dénoyer and J. P. Gazeau (eds.), *From Quasicrystals to More Complex Systems*, EDP Sciences, Les Ulis, and Springer, Berlin (2000), 145–166; `math.MG/0002020`.
[23] J. Patera (ed.), *Quasicrystals and Discrete Geometry*, Fields Institute Monographs, vol. 10, AMS, Providence, RI (1998).
[24] C. Radin, *Miles of Tiles*, AMS, Providence, RI (1999).
[25] M. Schlottmann, *Cut-and-project sets in locally compact Abelian groups*, in: [23], 247–264.
[26] M. Schlottmann, *Generalized model sets and dynamical systems*, in: [8], 143–159.
[27] H.-R. Trebin (ed.), *Quasicrystals – Structure and Physical Properties*, Wiley-VCH, Weinheim (2003).

Lattices and hermitian vector bundles in Arakelov geometry

Jean-Benoît Bost

from the handwritten abstract in the Vortragsbuch

In this survey talk, I gave an introduction to Arakelov geometry, emphasizing the role of constructions involving hermitian vector bundles over a scheme $\mathcal{H}$ of finite type over $Spec\,\mathbb{Z}$ - when $\mathcal{H} = Spec\,\mathbb{Z}$, they coincide with classical euclidean lattices. I also described the formalism of slopes associated to such hermitian vector bundles over $\mathcal{H} = Spec\,\mathcal{O}_k$, k a number field. When $k = \mathbb{Q}$, these slopes coincide with the successive minima of lattices; in general they satisfy nice invariance properties. Finally, I emphasized how inequalities relating the slopes of two hermitian vector bundles $\bar{\mathrm{E}}$ and $\bar{\mathrm{F}}$ over $Spec\,\mathcal{O}_k$, and the heights of some linear map $\varphi : \mathrm{E}_k \mapsto \mathrm{F}_k$ provide a geometric approach to Diophantnie approximation results, when applied to hermitian vector bundles $\bar{\mathrm{E}}$ (resp. $\bar{\mathrm{F}}$) of sections of some line bundle $\mathcal{L}$ over a projective scheme $\mathcal{H}/\mathbb{Z}$ (resp. a closed selescheme Σ) and to the restriction map φ sending a section of $\mathcal{L}$ over $\mathcal{H}$ to its restriction to Σ.

Optimality and Uniqueness of the Leech lattice among lattices

Abhinav Kumar
(joint work with Henry Cohn)

1. Introduction

The problem of finding the densest lattice in Euclidean space $\mathbb{R}^n$ is a famous problem in geometry and number theory. The determination of the largest possible density of a lattice in $\mathbb{R}^n$ also yields the Hermite constant γ_n, which is defined as the largest real number represented as the minimum nonzero value of some quadratic form of determinant 1 in n variables. In geometry, the problem of finding a densest lattice is a special case of the sphere packing problem, which asks for the densest packing of $\mathbb{R}^n$ by spheres of the same size. However, in low dimensions, many of the interesting sphere packings come from lattices, and it is believed that exceptionally dense lattices such as E_8 and the Leech lattice should solve not just the lattice packing problem, but also the sphere packing problem.

The densest lattices in $\mathbb{R}^n$ were known for $n \leq 8$; they are the root lattices $A_1, A_2, A_3, D_4, D_5, E_6, E_7$ and E_8. For $n = 3$ the result is due to Gauss, for $4 \leqslant n \leqslant 5$ to Korkine and Zolotareff, and for $6 \leqslant n \leqslant 8$ to Blichfeldt. In each dimension, the optimal lattice is also known to be unique, up to scaling and isometries. For $n \leq 5$ the optimality and uniqueness were proved simultaneously, while for $n = 6$ it was proved by Barnes and for $6 \leq n \leq 8$ by Vetčinkin.

We determine the densest lattice in dimension 24 [CK1], [CK2].

Theorem 1 (Cohn, Kumar)**.** *The Leech lattice is the unique densest lattice in $\mathbb{R}^{24}$, up to scaling and isometries of $\mathbb{R}^{24}$. No sphere packing in $\mathbb{R}^{24}$ can have density greater than $1 + 1.65 \cdot 10^{-30}$ times that of the Leech lattice.*

Using a similar line of proof, we prove an analogous result for E_8, giving another proof that E_8 is the densest lattice in 8 dimensions.

Theorem 2 (Blichfeldt, Vetčinkin)**.** *The E_8 root lattice is the unique densest lattice in $\mathbb{R}^8$, up to scaling and isometries of $\mathbb{R}^8$.*

Theorem 3. *No sphere packing in $\mathbb{R}^8$ can have density greater than $1 + 10^{-14}$ times that of the E_8 lattice.*

The error bounds in theorems 1 and 3 can be narrowed with more computation, as we shall indicate below. The next section outlines a proof of these theorems.

2. Outline of Proof

We start by applying the following of Cohn and Elkies [CE], [Co].

Theorem 4. *Suppose $f : \mathbb{R}^n \to \mathbb{R}$ is an admissible function, is not identically zero, and satisfies the following three conditions:*

(1) $f(0) = \widehat{f}(0) > 0$

(2) $f(x) \leq 0$ *for* $|x| \geq r$, *and*
(3) $\widehat{f}(t) \geq 0$ *for all* t.

Then the center density of sphere packings in $\mathbb{R}^n$ *is bounded above by* $(r/2)^n$.

We can find a function f which satisfies these properties for an r which satisfies $2 \leq r \leq 2(1 + 6.851 \cdot 10^{-32})$. Thus, an application of Theorem 4 proves the second statement in Theorem 1.

Now we wish to prove that the Leech lattice Λ_{24} is the densest lattice in $\mathbb{R}^{24}$. Assume that there exists a lattice Λ which is at least as dense as the Leech lattice. We may assume that Λ is unimodular. Then the argument outlined below will show that Λ is the same as Λ_{24} up to an orthogonal transformation.

Recall the following facts about the Leech lattice. The norms of the nonzero vectors are all the even positive integers greater than 2. The 196560 minimal vectors, of length 2, when renormalized to lie on the unit sphere, form a spherical code $\mathcal{C}_{24}$ of minimal angle $\pi/3$. In fact, they provide the unique solution to the kissing number problem in dimension 24, as was shown by Odlyzko, Sloane, Levenshtein and Bannai. This is proved by using the technique of linear programming bounds (for instance see [CS]). The spherical code $\mathcal{C}_{24}$ is a spherical 11-design. This also implies that if pairs of minimal vectors are grouped into separate classes depending on the inner product between them, we obtain the structure of an association scheme on $\mathcal{C}_{24}$. The main strategy of the proof is to prove similar assertions for the lattice Λ in order to show that it is "close to" Λ_{24} in a sense that we shall make precise.

First, note that the argument used to prove Theorem 4, namely Poisson summation, shows also that the first few vector lengths of Λ must be close to that of Λ_{24}. Let us use the term "nearly minimal vector" to mean a vector whose length is close to 2 (to be more precise, we may say it differs from 2 by at most 10^{-25}). Then, using a linear programming bound and analysis similar to Theorem 4, as well as the linear programming bound for spherical codes, we may show that there are exactly 196560 nearly minimal vectors. From the constraints on the successive vector lengths of Λ, we may show that the inner products between nearly minimal vectors are close to that of the minimal vectors of Λ_{24}, namely $0, \pm 1, \pm 2, \pm 4$. Normalizing the vectors to have unit length, we obtain a spherical code $\mathcal{C}$ of minimal angle ϕ, with $1/2 \leq \cos\phi \leq 1/2 + 6.733 \cdot 10^{-27}$. Linear programming bounds then show that $\mathcal{C}$ must be a nearly spherical 10-design. More precisely,

Lemma 5. *If* $g : S^{23} \to \mathbb{R}$ *is a polynomial of total degree at most* 10, *then*

$$\left| \sum_{z \in \mathcal{C}} g(z) - \frac{196560}{\mathrm{vol}(S^{23})} \int_{S^{23}} g(z)\, dz \right| \leqslant 2.50193 \cdot 10^{-5} |g|_2,$$

where $|g|_2$ *denotes the norm on* $L^2(S^{23})$.

Applying this lemma to suitable functions g, we deduce that $\mathcal{C}$ is also an association scheme, when we pair vectors according to their approximate inner product, and also that this scheme has the same multiplicities and intersection numbers

as $\mathcal{C}_{24}$. We show, using the uniqueness of the optimal kissing configuration in 24 dimensions, that there is only one 6-class association scheme with the same multiplicities and intersection numbers as $\mathcal{C}_{24}$. Therefore we obtain a bijection between $\mathcal{C}$ and $\mathcal{C}_{24}$, approximately preserving inner products between vectors. Next, we choose a basis of minimal vectors of Λ_{24} and look at the corresponding nearly minimal vectors of Λ. We show that they form a basis of Λ, and furthermore, that the two Gram matrices involved have corresponding entries differing by at most $5.04975 \cdot 10^{-25}$.

To finish the argument, we derive explicit bounds for the allowed perturbation in the Gram matrix of Λ_{24} in Voronoi's theorem [Vo] below and notice that Λ lies within those bounds.

Theorem 6 (Voronoi)**.** *A lattice is locally optimal for density if and only if it is perfect and eutactic.*

This proves Theorem 1. The proof of Theorem 2 is analogous.

3. Remarks

An important open problem is to determine whether a function f exists which satisfies the criteria of Theorem 4 for $n = 24$ (resp. $n = 8$) and $r = 2$ (resp. $r = \sqrt{2}$) exactly. Such functions would show that the Leech lattice and the E_8 lattice give densest sphere packings in their dimensions. In our proof, we determine by an intensive computer calculation a function f for which r is very close to 2. It seems reasonable to conjecture that with unlimited time and memory, the same method will be able to produce f for which r is arbitrarily close to 2. For a generalization of the density problem to potential energies of periodic packings and a generalization of this conjecture, we direct the reader to [CK3]. We would also like to mention recent work of Cohn and Miller regarding similar conjectures.

References

[Co] H. Cohn, *New upper bounds on sphere packings II*, Geom. Topol. **6** (2002), 329–353, `arXiv:math.MG/0110010`.

[CE] H. Cohn and N. Elkies, *New upper bounds on sphere packings I*, Annals of Mathematics **157** (2003), 689–714, `arXiv:math.MG/0110009`.

[CK1] H. Cohn and A. Kumar, *Optimality and uniqueness of the Leech lattice among lattices*, preprint, 2003, `arXiv:math.MG/0403263`.

[CK2] H. Cohn and A. Kumar, *The densest lattice in twenty-four dimensions*, Electron. Res. Announc. Amer. Math. Soc. 10 (2004), 58–67, `arXiv:math.MG/0408174`

[CK3] H. Cohn and A. Kumar, *Universally optimal distribution of points on spheres*, preprint, 2004.

[CS] J. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third edition, Springer-Verlag, 1999.

[OS] A. M. Odlyzko and N. J. A. Sloane, *New bounds on the number of unit spheres that can touch a unit sphere in n dimensions*, Journal of Combinatorial Theory **26** (1979), 210–214.

[Vo] G. Voronoi, *Propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. **133** (1908), 97–178.

Application of a new lattice reduction algorithm

Jean-Claude Belfiore

from the handwritten abstract in the Vortragsbuch

As presented by E. Viterbo, we need number theory tools to design coded modulation for the wireless communication problem. Constellations of symbols that are sent by the transmitter are either vectors with real components in the fast fading case (one transmit antenna) or matrices with complex components in the MiMo case (multiple antennas). In the fast fading case the transmit vector uses the canonical embedding in $\mathbb{R}^n$ of a well chosen number field whereas in the MiMo case, the transmit matrix uses the matrix representation of a well chosen cyclic algebra.

In this talk, we are interested in the decoding of these constellations. All these transmitted constellations are finite subsets of lattices. The receiver must solve the "closest point" problem. More over, the channel changes these lattices when time varies. In order to have a "not too complex" receiver, we need some lattice reduction with lattices that vary with the time (random lattices). The LLL algorithm may be used, but, in that specific case, another type of reduction algorithm is used.

BL-bases and unitary groups in characteristic 2

Jean-Pierre Serre

In what follows, K is a commutative field of characteristic 2.

1. A criterion for the existence of a BL-basis

Let L/K be a finite Galois extension, with Galois group G. A basis (e_i) of the K-vector space L is called a *self-dual normal basis* (BL-*basis*, for short) if it has the following two properties (cf. [1], [2], [3]):

a) $\mathrm{Tr}_{L/K}(e_i.e_j) = \delta_j^i$;

b) G acts transitively on the (e_i).

Note that b) means that (e_i) is a "normal basis" of L/K, while a) says that it is orthonormal with respect to the nondegenerate bilinear form $\mathrm{Tr}_{L/K}(x.y)$.

One finds in [1] and [2] several cases where BL-bases can be proved to exist (or not to exist):

Existence: when G is of odd order, or when G is abelian and does not contain any element of order 4.

Non-existence: when G has a quotient which is cyclic of order 4.

These results are special cases of:

Theorem 1 - *A BL-basis exists if and only if G is generated by squares and by elements of order 2.*

Note that this criterion does not depend on K, nor of the chosen extension L/K. It only depends on the structure of G. This is quite different from what happens in characteristic $\neq 2$, cf. e.g. [3].

Examples. A BL-basis exists if G is a dihedral group or a simple group; it does not exist if G is a quaternion group.

2. Proof of theorem 1

First, we may assume that K is *perfect*. Indeed, a BL-*basis* for L/K exists if and only if there exists one for the extension $L.K'/K'$, where K' is the perfect closure of K.

Consider now the group algebra $K[G]$, with its usual involution $g \mapsto g* = g^{-1}$. Let U_G^{sch} be its scheme-theoretic unitary group, which is an algebraic group over K. The group scheme U_G^{sch} is not reduced; call U_G the corresponding reduced scheme; it is a smooth algebraic group over K. We have a natural embedding $G \to U_G^{sch}(K) = U_G(K)$.

Let now $\overline{K}$ be an algebraic closure of K, and put $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$. The given extension L/K corresponds to a surjective homomorphism $\varphi_L : \Gamma_K \to G$. By composing φ_L with the embedding $G \to U_G(K)$, one may view φ_L as a 1-cocycle of Γ_K with values in $U_G(\overline{K})$. Let $z_L \in H^1(K, U_G)$ be the cohomology class of this cocycle.

Proposition 1 - *We have $z_L = 0$ if and only if L/K has a BL-basis.*

This is explained in [3], § 1.5 when the characteristic of K is $\neq 2$; the case of characteristic 2 is similar. (Loosely speaking, the BL-bases are the K-points of a U_G-torsor which corresponds to z_L.)

Put now:

U_G^o = connected component of U_G ;

G^o = subgroup of G generated by the elements of order 2 and by the squares g^2, where g runs through G.

Proposition 2 - (a) $G^o = G \cap U_G^o$.
(b) U_G/U_G^o *is a finite commutative group of type* $(2, \ldots, 2)$.

Both (b) and the inclusion $G^o \subset G \cap U_G^o$ are fairly easy. The inclusion $G \cap U_G^o \subset G^o$ requires more work.

Proposition 3 - $H^1(K, U_G^o) = 0$.

This is a special case of a general result on unitary groups, cf. §3, th.2.

Let us now prove half of theorem 1, namely that a BL-basis exists if $G = G^o$. Indeed, in that case, by Proposition 2, we may view $\varphi_L : \Gamma_K \to G$ as a 1-cocycle with values in $U_G^o(\overline{K})$; let $z_L^o \in H^1(K, U_G^o)$ be the class of this cocycle. The image of z_L^o in $H^1(K, U_G)$ is z_L. By Proposition 3, we have $z_L^o = 0$, hence $z_L = 0$ and Proposition 1 shows that L/K has a BL-basis.

It remains to show that, if $G \neq G^o$, there is no BL-basis. To do so, one first remarks that the assumption $G \neq G^o$ is equivalent to the existence of a surjective quadratic character e: $G \to \{\pm 1\}$ with the property that $e(s) = 1$ for every $s \in G$ with $s^2 = 1$. Choose such an e, and assume there exists an element x of L whose G-orbit is a BL-basis. Put:

$$x_0 = \sum_{e(g)=1} g.x \quad \text{and} \quad x_1 = \sum_{e(g)=-1} g.x.$$

An explicit computation, similar to the one made in [2], proof of Proposition 6.1 b), shows that $x_0.x_1 = 0$. Since L is a field, we have either $x_0 = 0$ or $x_1 = 0$, which contradicts the assumption that the $g.x$ are linearly independent.

3. Unitary groups

We continue to assume that K is perfect of characteristic 2.
Let R be a finite-dimensional K-algebra with involution, and let U_R be the corresponding reduced unitary group. Let U_R^o be the connected component of U_R.

Theorem 2 - $H^1(K, U_R^o) = 0$.

Let S be the quotient of U_R^o by its unipotent radical; the algebraic group S is a reductive group over K (it is the largest reductive quotient of U_R^o), and the natural map $H^1(K, U_R^o) \to H^1(K, S)$ is a bijection. Hence proving Theorem 2 amounts to proving that $H^1(K, S) = 0$. To do so, we need to describe the structure of S. The result is:

Theorem 3 - *Up to a purely inseparable isogeny, S is a product of classical groups of the following three types:*
(i) *Multiplicative group of a central simple algebra over a finite extension of K.*
(ii) *Unitary group of a central simple algebra with involution* (of first or second kind) *over a finite extension of K.*
(iii) *Special orthogonal group of a nondegenerate quadratic form of even rank > 2 over a finite extension of K.*

This is proved by choosing a maximal torus of U_R^o and looking at the weights of its action on R (by left multiplication), and at the root system of S. Most of the proof can be done under the assumption that K is algebraically closed: the descent from $\overline{K}$ to K is easy.

Once Theorem 3 is proved, Theorem 2 follows by standard methods in Galois cohomology, based essentially on the fact that $\mathrm{cd}_2(\Gamma_K) \leqslant 1$, and on the following auxiliary result:

Proposition 4 - *Let A be a connected linear algebraic group over K, and let K_1 be a quadratic extension of K. The natural map $H^1(K, A) \to H^1(K_1, A)$ is injective.*
(See e.g. [4], Chap. III, § 2.3, Exercise 2 (b).)

Here are a few more properties of the unitary group U_R:

Theorem 4 - (i) *The finite group U_R/U_R^o is commutative of type* $(2, \ldots, 2)$.
(ii) *The map $H^1(K, U_R) \to H^1(K, U_R/U_R^o)$ is injective.*
(iii) *Every commutative smooth subgroup of U_R of multiplicative type is contained in a maximal torus.*
(iv) *If K' is an odd degree extension of K, the map $H^1(K, U_R) \to H^1(K', U_R)$ is injective.*

Properties (i) and (iii) are easy; (ii) follows from (i) and from Theorem 2; (iv) follows from (ii). (It would be interesting to have an *a priori* proof of (iv).)

References

[1] E. Bayer-Fluckiger, *Self-dual normal bases, I*, Indag. Math. **51** (1989), 379-383.
[2] E. Bayer-Fluckiger and H.W. Lenstra, Jr, *Forms in odd degree extensions and self-dual normal bases*, Amer.J.Math. **112** (1990), 359-373.
[3] E. Bayer-Fluckiger and J.-P. Serre, *Torsions quadratiques et bases normales autoduales*, Amer.J.Math. **116** (1994), 1-64.
[4] J.-P. Serre, *Cohomologie Galoisienne*, cinquième édition, révisée et complétée, LNM **5**, Springer-Verlag, 1994; English translation, SMM Springer-Verlag, 1997.

Perfect Lattices, Homology of Modular groups and Algebraic K-Theory

Philippe Elbaz-Vincent
(joint work with Herbert Gangl, Christophe Soulé)

Brief abstract - For $N = 5$ and $N = 6$, we compute the Voronoï cell complex attached to real N-dimensional quadratic forms, and we obtain the homologies of $GL_N(\mathbb{Z})$ and $SL_N(\mathbb{Z})$ with trivial coefficients, up to small primes. We also prove that $K_5(\mathbb{Z}) = \mathbb{Z}$ and $K_6(\mathbb{Z}) = 0$. We give a complete list of cells for the Voronoï complex in rank 5 and 6 modulo the action of $GL_N(\mathbb{Z})$ and $SL_N(\mathbb{Z})$, and give also the list of strongly eutactic and semi-eutactic cells completing lists of Batut, Bergé and Martinet (see the extended abstract of Martinet's talk for more on this notion). Part of this report is work in progress.

1. Voronoï theory

Let $N \geqslant 2$ be an integer. Denote by C_N the space of definite and positive real quadratic forms of rank N. Given $h \in C_N$, there is only a finite number of minimal vectors of h, i.e., the non zero vectors $v \in \mathbb{Z}^N$ such that $h(v)$ is minimal. We will denote it by $m(h)$. A form $h \in C_N$ is said perfect if it is characterized by its minimum on $\mathbb{Z}^N - \{0\}$ and by $m(h)$. Denote by Γ either the group $GL_N(\mathbb{Z})$ or $SL_N(\mathbb{Z})$. Voronoï has shown [3] (Thm., p.110) that modulo the action of Γ and up to scalar multiplication by positive real numbers, there is only a finite number of perfect forms.

Denote by C_N^* the space of positive real quadratic forms on $\mathbb{R}^N$ such that the kernel is generated by a (strict) subspace of $\mathbb{Q}^N$. Let X_N^* be the quotient of C_N^* by positive homotheties, $\pi : C_N^* \to X_N^*$ the quotient map, $X_N = \pi(C_N)$ and $\partial X_N^* = X_N^* - X_N$. The group Γ acts on C_N^*, and on X_N^*, by the action

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

where γ^t denotes the transpose of γ.
If $v \in \mathbb{Z}^N - \{0\}$, we can consider the form $\widehat{v} \in C_N^*$, defined as $\widehat{v}(x) = (v|x)^2$. Given a finite subset B of $\mathbb{Z}^N - \{0\}$, the convex hull of B is the subset of X_N^*, image by π of the subset

$$\Big\{ \sum_j \lambda_j \widehat{v}_j\,,\ v_j \in B,\ \lambda_j \geqslant 0 \Big\}$$

of C_N^*. If h is a perfect form, we denote by $\sigma(h) \subset X_N^*$ the convex hull of the set $m(h)$ of its minimal vectors. Voronoï has shown [3] (§§8-15) that the cells $\sigma(h)$ and their intersections, when h runs through the set of perfect forms, give a cellular decomposition (in the sense of algebraic topology) of X_N^*, compatible with the action of Γ. We endow X_N^* of the corresponding CW-structure. If τ is a closed cell of X_N^* and if h is a perfect form such that $\tau \subset \sigma(h)$, we denote by $m(\tau)$ the set of vectors v of $m(h)$ such that $\widehat{v}$ is in τ. The cell τ is the convex hull of $m(\tau)$ and $m(\tau) \cap m(\tau') = m(\tau \cap \tau')$.

2. Explicits computations

Denote by Σ_n, $0 \leqslant n \leqslant d(N) = N(N+1)/2-1$, a set of representatives, modulo the action of Γ, of the cells of dimension n in the Voronoï complex and such that *no elements of their stabilizer in* Γ *change their orientation*. For $N \leqslant 6$ we have computed such sets Σ_n and we have the results below (the subscript $(-)_{\mathrm{op}}$ means that we work modulo the cells such that the orientation is changed by an element of its stabilizer).

Proposition 1. (Elbaz-Vincent/Gangl/Soulé, 2002).

The cardinality of Σ_n is given as follows (empty slots denote zeros):

n	5	6	7	8	9	10	11	12	...
$GL_5(\mathbb{Z})$	5	10	16	23	25	23	16	9	...
$GL_5(\mathbb{Z})_{\mathrm{op}}$	0	0	0	1	7	6	1	0	...
$GL_6(\mathbb{Z})$	3	10	28	71	162	329	589	874	...
$GL_6(\mathbb{Z})_{\mathrm{op}}$	0	0	0	0	3	46	163	340	...
$SL_6(\mathbb{Z})$	3	10	28	71	163	347	691	1152	...
$SL_6(\mathbb{Z})_{\mathrm{op}}$	0	3	10	18	43	169	460	815	...

...	13	14	15	16	17	18	19	20	total
...	4	3							136
...	2	3							20
...	1066	1039	775	425	181	57	18	7	5634
...	544	636	469	200	49	5	0	0	2455
...	1532	1551	1134	585	222	62	18	7	7576
...	1132	1270	970	434	114	27	14	7	5486

Answering a question of Martinet (cf. his extended abstract), we have shown that there are, up to equivalence, exactly 21 strongly eutactic forms and 6 strongly semi–eutactic forms in rank 6. We also have confirmed the computations of Bergé and Martinet in rank 5.

Euler characteristic (a.k.a. "mass formula"): From the data we can verify that if $N = 5, 6$, $\chi(SL_N(\mathbb{Z})) = \sum_{\sigma\in E}(-1)^{\dim(\sigma)}\frac{1}{|\Gamma_\sigma|} = 0$, E family of representatives of cells of the Voronoï complex of rank N and Γ_σ is the stabilizer of σ in $SL_N(\mathbb{Z})$. More precisely, for $N = 6$, we get:

$$\frac{45047}{1451520} - \frac{10633}{11520} + \frac{6425}{576} - \frac{12541}{192} + \frac{7438673}{34560} - \frac{3841271}{8640} + \frac{9238}{15} - \frac{266865}{448} + \frac{14205227}{34560}$$
$$- \frac{14081573}{69120} + \frac{830183}{11520} - \frac{205189}{11520} + \frac{61213}{20736} - \frac{1169}{3840} + \frac{17}{1008} - \frac{1}{2880} = 0\,.$$

For the dimension $N = 7$ the computations are not complete yet (only 60% of the forms).

3. Cohomology of modular groups and the K-theory of integers

Using the previous computations and the Borel/Serre duality for arithmetic groups [1], we get the following theorem.

Let m be a positive integer. We denote by $\mathcal{S}_m$ the Serre class of finite abelian

groups A such that for every prime number p dividing the order of A the inequality $p \leqslant m$ holds.

Theorem A. (Elbaz-Vincent/Gangl/Soulé, 2002)

(i) Modulo $\mathcal{S}_5$ we have

$$H^m(GL_5(\mathbb{Z}), \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if} \quad m = 0, 5, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) Modulo $\mathcal{S}_7$ we have

$$H^m(GL_6(\mathbb{Z}), \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if} \quad m = 0, 5, 8, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$H^m(SL_6(\mathbb{Z}), \mathbb{Z}) = \begin{cases} \mathbb{Z}^2 & \text{if} \quad m = 5, \\ \mathbb{Z} & \text{if} \quad m = 0, 8, 9, 10, \\ 0 & \text{otherwise.} \end{cases}$$

At the level of the K–theory of integers we have

Theorem B. (Elbaz-Vincent/Gangl/Soulé, 2002 and 2003)
We have $K_5(\mathbb{Z}) = \mathbb{Z}$ and $K_6(\mathbb{Z}) = 0$.

The Theorem B is mainly a consequence of the study of the torsion of the so-called Hurewicz map and from the computation of homology of $GL_N(\mathbb{Z})$ with coefficients in Steinberg modules. Namely, we have the following computations

Proposition 2. (Elbaz-Vincent/Gangl/Soulé, 2002 and 2003).

(i) Modulo $\mathcal{S}_2$ we have $H_3(GL_3(\mathbb{Z}), St_3) = \mathbb{Z}$ and

$$H_1(GL_5(\mathbb{Z}), St_5) = H_2(GL_5(\mathbb{Z}), St_5) = H_2(GL_4(\mathbb{Z}), St_4) = H_4(GL_2(\mathbb{Z}), St_2) = H_1(GL_6(\mathbb{Z}), St_6) = 0\,.$$

(ii) Modulo $\mathcal{S}_3$ we have $H_3(GL_4(\mathbb{Z}), St_4) = \mathbb{Z}$ and

$$H_4(GL_3(\mathbb{Z}), St_3) = H_5(GL_2(\mathbb{Z}), St_2) = 0\,.$$

Remark: For $K_7(\mathbb{Z})$ the computations are still incomplete. We expect that the perfect forms of rank 7 do not contribute to the odd torsion of $K_7(\mathbb{Z})$ (we already know that for 60% of the perfect forms). We also know that the kernel of the so-called Hurewicz map is a subgroup of $\mathbb{Z}/15$ (up to 2-torsion).

References

[1] A. Borel, and J.-P. Serre, *Corners and arithmetic groups*, Comment. Math. Helv. **48** (1973), 436–491.

[2] Ph. Elbaz-Vincent, H. Gangl and C. Soulé, *Quelques calculs de la cohomologie de $GL_N(\mathbb{Z})$ et de la K-théorie de $\mathbb{Z}$*, C.R. Acad. des Sc. Paris, Série I, **335**, (2002), 321–324.

[3] G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques I*, J. Crelle **133** (1907), 97–178.

On Reduction Theory and its Algorithmic Aspects

Phong Q. Nguyên
(joint work with Damien Stehlé)

Reduction theory, in the language of quadratic forms, goes back to the work of Lagrange, Gauss, Hermite, Korkine-Zolotarev, Minkowski, *etc.* It was introduced to upper bound Hermite's constant: the existence of the constant was first proved by means of reduction, namely Hermite's reduction. In low dimension up to dimension four, Hermite-Korkine-Zolotarev (HKZ) reduction gives tight bounds on Hermite's constant. From a mathematical point of view, the strongest notions of reduction known are those of Hermite-Korkine-Zolotarev and Minkowski.

¿From an algorithmic point of view, one is rather interested in notions of reduction which are easy to compute: given an arbitrary basis of a lattice, one would like to find a reduced basis efficiently. The celebrated LLL (or L^3) algorithm [1] was the first efficient reduction algorithm in arbitrary dimension: Its running time is $O(d^6|og^3B)$ where d is the lattice dimension and B is an upper bound on the Euclidean norm of the initial basis vectors. It outputs lattice bases which are almost Hermite-reduced, and therefore consist of relatively short lattice vectors. LLL has had incredibly many applications over the past twenty years, especially in algorithmic number theory and theoretical computer science (see for instance the survey [2]).

In this talk, we discuss two new reduction algorithms: the greedy algorithm [3] and the L^2 algorithm [4]. The greedy algorithm is a natural geometric generalization of Euclid's gcd algorithm, which can itself be viewed as a one-dimensional reduction algorithm. In fixed dimension $\leqslant 4$, the greedy algorithm outputs Minkowski-reduced bases with the same running time as Euclid's algorithm: without fast integer arithmetic, the complexity is $O(\log^2 B)$. In dimension $\geqslant 5$, greedy-reduced bases may be arbitrarily far from the first minimum of the lattice, and it is unknown if the greedy algorithm still has polynomial-time complexity, except in dimension 5. The L^2 algorithm [4] achieves approximate Hermite reduction in time polynomial in d and $\log B$ like LLL. However, it is the first polynomial-time reduction algorithm whose complexity without fast integer arithmetic is $O(\log^2 B)$ (instead of the usual $O(\log^3 B)$) for fixed dimension d. In other words, L^2 matches the complexity of Euclid's algorithm.

References

[1] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261: 513–534, 1982.

[2] P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Cryptography and Lattices – Proc. ANTS-VI*, volume of *Lecture Notes in Computer Science*, pages 146–180. Springer-Verlag, 2001.

[3] P. Q. Nguyen and D. Stehlé. Low-dimensional Lattice Basis Reduction Revisited. In *Algorithmic Number Theory – Proc. ANTS-VI*, volume 3076 of *Lecture Notes in Computer Science*, pages 338–357. Springer-Verlag, 2004.

[4] P. Q. Nguyen and D. Stehlé. Floating-Point LLL Revisited. In *Advances in Cryptology – Proc. Eurocrypt*, to appear in *Lecture Notes in Computer Science*. Springer-Verlag, 2005.

Weil representations, Clifford groups, and conjectures of Larsen and Katz

Pham Huu Tiep
(joint work with Robert M. Guralnick)

Let $V = \mathbb{C}^d$ with $d > 4$. Fix a nondegenerate quadratic form and if d is even fix a nondegenerate symplectic form on V, and let $\mathcal{G}$ be one of $GL(V)$, $O(V)$ or $Sp(V)$. If G is any subgroup of $GL(V)$, define $M_{2k}(G,V)$ to be the dimension of $\mathrm{End}_G(V^{\otimes k})$, and G is called *reductive* if G is closed and the connected component G° of G is reductive. We are interested in Larsen's conjecture:

Conjecture 0.1. *If G is a reductive subgroup of $\mathcal{G}$, then either $G \geq [\mathcal{G},\mathcal{G}]$ or $M_{2k}(G,V) > M_{2k}(\mathcal{G},V)$ for some $k \leq 4$.*

An interesting application of this conjecture comes from algebraic geometry [Ka1]. Given a projective smooth variety X of dimension $n+1 \geq 1$ over a finite field k. Of interest is the monodromy group G_d which is the Zariski closure of the monodromy group of a local system $\mathcal{F}_d$ on the space of all smooth degree d hypersurface sections (see [Ka1]). Fix a degree d hypersurface H which is tranverse to X, and let V be the subspace spanned by the vanishing cycles in $H^n((X \otimes_k \bar{k}) \cap H, \overline{\mathbb{Q}}_\ell)$ [D, (4.2.4)]. Then the cup product induces a (G_d-invariant) nondegenerate bilinear form on V. Deligne [D, 4.4] showed that $G_d = Sp(V)$ if n is odd; if $n \geq 2$ is even then $G_d = O(V)$ or G_d is finite. One would like to be able to rule out the finite group possibility (under additional hypotheses). Katz has shown in [Ka1] that G_d is a subgroup of $\mathcal{G} := Sp(V)$ or $O(V)$ with the same *fourth moment* as of $\mathcal{G}$, that is, $M_4(G_d,V) = M_4(\mathcal{G},V)$.

A more recent application is described in [Ka2], where Larsen's conjecture, as well as *drop ratio conjectures* (cf. [Ka2, Chapter 2] and Theorem 5 below) play an important role in the determination of the geometric monodromy group attached to a family of character sums over finite fields.

Another application is purely lattice-theoretic. Assume that $\mathcal{G} = O(V)$ and G is a finite subgroup of $\mathcal{G}$ such that $M_{2k}(G,V) = M_{2k}(\mathcal{G},V)$ for some $k \geq 2$. Then any (symmetrized) G-orbit on V is a spherical $2k$-design, cf. [LST]. Moreover, for any subspace $0 \neq U < V$, the G-orbit of U is a grassmannian $2k$-design as defined in [BCN]. IF G stabilizes an integral lattice Λ in V, then Λ is strongly perfect as defined by Venkov.

In fact, we will prove:

Theorem 1. *Let $V = \mathbb{C}^d$ with $d \geq 5$ and $\mathcal{G}$ be $GL(V)$, $Sp(V)$, or $O(V)$. Assume that G is a closed subgroup of $\mathcal{G}$ such that G° is reductive. Then one of the following holds:*

(i) $M_8(G,V) > M_8(\mathcal{G},V)$;

(ii) $G \geq [\mathcal{G}, \mathcal{G}]$;
(iii) $d = 6$, $\mathcal{G} = Sp(V)$, *and* $G = 2J_2$.

Notice that in the case (iii) of Theorem 1, G and $\mathcal{G}$ have the same $2k$-moments if and only if $k \leq 5$.

Theorem 2. *Let $V = \mathbb{C}^d$ with $d \geq 5$, $\mathcal{G} = GL(V)$, $Sp(V)$, or $O(V)$. Assume G is a closed subgroup of $\mathcal{G}$. Then G is irreducible on every $\mathcal{G}$-composition factor of $V^{\otimes 3}$ (this condition is equivalent to $M_6(G, V) = M_6(\mathcal{G}, V)$ if G° is reductive) if and only if one of the following holds.*

(A) $G \geq [\mathcal{G}, \mathcal{G}]$; *moreover, $G \neq SO(V)$ if $d = 6$.*

(B) *(Extraspecial case) $d = 2^a$ for some $a > 2$. If $\mathcal{G} = GL(V)$ then $G = Z(G)E \cdot Sp_{2a}(2)$ with $E = 2^{1+2a}_+$. If $\mathcal{G} = Sp(V)$, resp. $O(V)$, then $E \cdot \Omega^\epsilon_{2a}(2) \leq G \leq E \cdot O^\epsilon_{2a}(2)$, with $E = 2^{1+2a}_\epsilon$ and $\epsilon = -$, resp. $\epsilon = +$.* (This groups are called *Clifford groups* in [NRS].)

(C) *(Exceptional cases) G is finite, with the unique nonabelian composition factor being $L_3(4)$, $U_3(3)$, $U_4(3)$, J_2, Alt_9, $\Omega^+_8(2)$, $U_5(2)$, $G_2(4)$, Suz, J_3, Co_2, Co_1, $F_4(2)$, and $\dim(V)$ being 6, 6, 6, 6, 8, 8, 10, 12, 12, 18, 23, 24, and 52, respectively.*

From Theorem 2 we recapture the facts that the Barnes-Wall lattices BW_{2^n}, the root lattice E_8, the Leech lattice Λ_{24} and the short Leech lattice Λ_{23} give rise to spherical/grassmannian 6-designs, which are well-known to the experts in the area.

Theorem 3. *Let $V = \mathbb{C}^d$ with $d \geq 5$, $\mathcal{G} = GL(V)$, $Sp(V)$, or $O(V)$. Assume G is a closed subgroup of $\mathcal{G}$. Set $\bar{S} = S/Z(S)$ for $S := F^*(G)$ if G is finite. Then G is irreducible on every $\mathcal{G}$-composition factor of $V \otimes V^*$ (this condition is equivalent to $M_4(G, V) = M_4(\mathcal{G}, V)$ if G° is reductive) if and only if one of the following holds.*

(A) $G \geq [\mathcal{G}, \mathcal{G}]$.

(B) *(Lie-type case) One of the following holds.*

(i) $\bar{S} = PSp_{2n}(q)$, $n \geq 2$, $q = 3, 5$, $G = Z(G)S$, *and $V \downarrow_S$ is a Weil representation of dimension $(q^n \pm 1)/2$.*

(ii) $\bar{S} = U_n(2)$, $n \geq 4$, *and $V \downarrow_S$ is a Weil representation of dimension $(2^n + 2(-1)^n)/3$ or $(2^n - (-1)^n)/3$.*

(C) *(Extraspecial case) $d = p^a$ for some prime p, $p > 2$ if $\mathcal{G} = GL(V)$ and $p = 2$ otherwise, $F^*(G) = Z(G)E$ for some extraspecial subgroup E of order p^{1+2a} of $\mathcal{G}$ (and G satisfies one more technical condition which we omit here).*

(D) *(Exceptional cases) $(G, \dim(V))$ is either one of the 13 examples described in Theorem 2, or one of 19 more explicit exceptions (which we omit here).*

Corollary 4. *Assume G is one of the finite groups mentioned in Theorem 3 and let χ be the character of the G-module V.*

(i) *If $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\exp(2\pi i/3))$ then G gives rise to a strongly perfect lattice.*

(ii) *If $\mathcal{G} = O(V)$ then any G-orbit of any nonzero proper subspace of V is a grassmannian 4-design.*

Corollary 4 yields several new infinite series of strongly perfect lattices as well as of grassmannian 4-designs.

Katz [Ka2] defines the *projective drop* $\boldsymbol{d}_V(g)$ of any element $g \in GL(V)$ to be the smallest codimension (in V) of g-eigenspaces on V. In [Ka2], Katz has formulated three conjectures on the projective drop, Conjectures (2.7.1), (2.7.4), and (2.7.7), in increasing order of strength. We will show that the second strongest, Conjecture (2.7.4) of [Ka2], holds true. (A slightly different version of this result has also been proved by Gluck and Magaard.)

Theorem 5. *Let $V = \mathbb{C}^d$ with $d \geq 2$, $\mathcal{G} = GL(V)$, $Sp(V)$, or $O(V)$. Assume G is a finite subgroup of $\mathcal{G}$ such that $M_4(G,V) = M_4(\mathcal{G},V)$. Then*

$$\min\left\{\frac{\boldsymbol{d}_V(g)}{\dim(V)} \mid g \in G \setminus Z(\mathcal{G})\right\} \geq 1/8 \ .$$

Moreover, the equality occurs precisely when G is the Weyl group $W(E_8)$ of type E_8 on its (8-dimensional) reflection representation.

In fact we have also proved modular versions of the above results (that is, where V is a finite dimensional vector space over algebraically closed fields of positive characteristics), cf. [GT] for more details. In particular, our results give another proof for Dixon's conjecture [Di] in the case of finite simple groups of Lie type defined over $\mathbb{F}_q$ when $q \to \infty$.

References

[BCN] C. Bachoc, R. Coulangeon, and G. Nebe, Designs in Grassmannian spaces and lattices. *J. Algebraic Combin.* **16** (2002), 5 – 19.

[D] P. Deligne, La conjecture de Weil II, *Publ. Math. I.H.E.S.* **52** (1980), 137 – 252.

[Di] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199 – 205.

[GT] R. M. Guralnick and Pham Huu Tiep, Decompositions of small tensor powers and Larsen's conjecture, *Representation Theory* **9** (2005), 138 – 208.

[Ka1] N. Katz, Larsen's alternative, moments, and the monodromy of Lefschetz pencils, in: "*Contributions to Automorphic Forms, Geometry, and Number Theory*", Johns Hopkins University Press, pp. 521 – 560.

[Ka2] N. Katz, Moments, Monodromy, and Perversity: a Diophantine Perspective, *Annals of Math. Study*, Princeton Univ. Press (to appear).

[LST] W. Lempken, B. Schröder, and Pham Huu Tiep, Symmetric squares, spherical designs, and lattice minima, *J. Algebra* **240** (2001), 185 – 208.

[NRS] G. Nebe, E. M. Rains, and N. J. A. Sloane, The invariants of the Clifford groups, *Des. Codes Cryptogr.* **24** (2001), 99 – 121.

Sphere Coverings in Dimensions 1, . . . , 24

Frank Vallentin
(joint work with Achill Schürmann)

1. Introduction

Classical problems in geometry are the determination of most economical sphere packings and coverings of the Euclidean space $\mathbb{R}^d$. While the sphere packing problem and especially the lattice packing problem has attracted many mathematicians over the last three hundred years, the sphere covering problem has only a comparatively short history. Even if we restrict ourselves to the special case of lattice coverings we are just beginning to develop a theory.

We present the current state of this theory for low-dimensional lattice coverings. This includes an algorithm which in principle solves the lattice covering problem in every given dimension d. Using this approach we were able to solve the lattice covering problem up to dimension 5 (which was known before) and we were able to find new best known lattice coverings in dimensions $6, 7, 8$. Furthermore, we show that the Leech lattice gives a locally optimal solution of the lattice covering problem in dimension 24. We give the current best known lattice coverings in dimension $1, \ldots, 24$ and conclude with the most tantalizing questions. For more details and for references to the relevant literature we refer to [SV04a] and [SV04b].

2. The Lattice Covering Problem

We shall define the lattice covering problem. A *lattice* L is a full rank, discrete subgroup of $\mathbb{R}^d$. There exist matrices $A \in \mathsf{GL}_d(\mathbb{R})$ with $L = A\mathbb{Z}^d$ which we call *bases* of L. If B^d denotes the Euclidean unit ball, then the Minkowski sum $L+\alpha B^d = \{\boldsymbol{v}+\alpha\boldsymbol{x} : \boldsymbol{v} \in L,\ \boldsymbol{x} \in B^d\}$, $\alpha \in \mathbb{R}_{>0}$, is a lattice covering if $\mathbb{R}^d = L+\alpha B^d$. The covering radius $\mu(L)$ is given by $\mu(L) = \min\{\mu : L + \mu B^d \text{ is a lattice covering}\}$. For a lattice L we define its *determinant* $\det(L) = |\det(A)|$. The *covering density* of L is $\Theta(L) = \sqrt{\mu(L)^d/\det(L)} \cdot \mathrm{vol} B_d$.

Problem. (Lattice Covering Problem) For $d \geq 1$, determine $\Theta_d = \min_L \Theta(L)$ and lattices L attaining it.

3. Dimensions $1, \ldots, 5$

The lattice covering problem has only been solved up to dimension 5 where the one-dimensional case is trivial. The (unique) solutions are shown in Table 1. This table invites to a question formulated by Ryshkov in 1967, who asked for the lowest dimension in which A_d^* does not give the thinnest lattice covering.

d	lattice	density Θ_d	author(s)
1	$\mathbb{Z}$	1	
2	A_2^*	1.2091...	Kershner, 1939
3	A_3^*	1.4635...	Bambah, 1954
4	A_4^*	1.7655...	Delone, Ryshkov, 1963
5	A_5^*	2.1242...	Ryshkov, Baranovskii, 1975

TABLE 1. Optimal lattice coverings

4. Classifying all locally optimal lattice coverings

Now we describe how one finds all locally optimal lattice coverings in a given dimension. These are only finitely many and one finds them by solving convex optimization problems. This is mainly due to Voronoi's theory of Delone subdivisions [Vor08], which we briefly review.

4.1. **Voronoi's Theory of Delone Subdivisions.**

We work in the classical setting of positive definite quadratic forms (PQFs from now on) to represent lattices. Let Q be a positive semidefinite quadratic form. A polyhedron $P = \mathrm{conv}\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots\}$ with $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots \in \mathbb{Z}^d$, is called a *Delone polyhedron* of Q if there exists a $\boldsymbol{c} \in \mathbb{R}^d$ and a real number $r \in \mathbb{R}$ with $Q[\boldsymbol{v}_i - \boldsymbol{c}] = r^2$ for all $i = 1, 2, \ldots$, and $Q[\boldsymbol{v} - \boldsymbol{c}] > r^2$ for all other $\boldsymbol{v} \in \mathbb{Z}^d \setminus \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots\}$. The set $\mathrm{Del}(Q)$ of all Delone polyhedra is called the *Delone subdivision* of Q. It is a periodic face-to-face tiling of $\mathbb{R}^d$. Therefore $\mathrm{Del}(Q)$ is completely determined by all Delone polytopes having a vertex at the origin $\mathbf{0}$. We call two Delone polyhedra L, L' *equivalent* if there exists a $\boldsymbol{v} \in \mathbb{Z}^d$ such that $L = \boldsymbol{v} \pm L'$. Note moreover that the inhomogeneous minimum $\mu(Q)$ is at the same time the maximum squared circumradius of its Delone polyhedra. We say that the Delone subdivision of a positive semidefinite quadratic form Q' is a *refinement* of the Delone subdivision of Q, if every Delone polytope of Q' is contained in a Delone polytope of Q.

By the theory of Voronoi, the set of positive semidefinite quadratic forms with a fixed Delone subdivision $\mathcal{D}$ is an open (with respect to its affine hull) polyhedral cone in the cone of positive semidefinite quadratic forms $\mathcal{S}_{\geq 0}$. We refer to this set as the *secondary cone* (L-type domain) $\boldsymbol{\Delta}(\mathcal{D})$ of the subdivision. The topological closure $\overline{\boldsymbol{\Delta}(\mathcal{D})}$ of a secondary cone is a closed polyhedral cone. The relative interior of each face is the secondary cone of another Delone subdivision. If a face is contained in the boundary of a second face, then the corresponding Delone subdivision of the first is a true refinement of the second one.

The interior of faces of maximal dimension $\binom{d+1}{2}$ contain PQFs whose Delone subdivision is a triangulation, that is, it consists of simplices only. We refer to such a subdivision as a *simplicial* Delone subdivision or *Delone triangulation*. The group $\mathsf{GL}_d(\mathbb{Z})$ acts on $\mathcal{S}_{\geq 0}$. One of the key observations is that under this group action there exist only finitely many inequivalent Delone subdivisions, respectively secondary cones.

Theorem. The topological closures of secondary cones of Delone triangulations give a face-to-face tiling of $\mathcal{S}_{\geq 0}$. The group $\mathsf{GL}_d(\mathbb{Z})$ acts on the tiling, and under this group action there are only finitely many non-equivalent secondary cones.

Given a Delone triangulation $\mathcal{D}$, the Delone triangulations $\mathcal{D}'$ with $\overline{\mathbf{\Delta}(\mathcal{D}')}$ sharing a facet with $\overline{\mathbf{\Delta}(\mathcal{D})}$ are attained by *bistellar operations* (*flips*). These change a triangulation only in certain *repartitioning polytopes* associated to the facet. By this operation it becomes possible to enumerate all Delone triangulations, and hence all Delone subdivisions in a given dimension.

4.2. **Obtaining Local Optima via Convex Optimization.**
For a fixed triangulation $\mathcal{D}$, we can formulate the lattice covering problem in the framework of *Determinant Maximization Problems* which can be efficiently solved (in the sense that one can approximate optimal solution for every given precision) by interior point methods. We maximize $\det(Q)$ while $\mu(Q) \leq 1$. For all $Q \in \overline{\mathbf{\Delta}(\mathcal{D})}$ this can be achieved by solving

$$\begin{array}{ll} \textbf{minimize} & -\log\det(Q) \\ \textbf{subject to} & Q \succ 0, \\ & Q \in \overline{\mathbf{\Delta}(\mathcal{D})},\ \mu(Q) \leq 1. \end{array}$$

5. Dimensions 6, ..., 24

For each of the triangulations in dimension $d \leq 5$ we determined by an implemention (in C++) the local optima with respect to Θ. By this we confirmed the known results for dimensions $d \leq 5$. Since they are several millions (no reasonable bound is known) different triangulations in dimension 6 there is no hope that this algorithm will solve the problem in this dimension. Nevertheless, we found a lattice in dimension 6 which currently is the best known covering lattice. Thereby we answer Ryshkov's question.

Theorem. ([SV04a]) In dimension 6, there exits a lattice L_6^c with $\Theta(L_6^c) = 2.4648\ldots$.

In [SV04b] we show that the root lattice E_8 does not give a locally optimal lattice covering, by constructing a refining triangulation $\mathcal{D}$ of $\mathrm{Del}(Q_{\mathsf{E}_8})$ in which Θ's local optimum is not attained by the PQF Q_{E_8}. The PQF found in this way even beats the formerly best known value $\Theta(\mathsf{A}_8^*)$ by more than 12%.

Looking at the results in dimension $d = 6, 8$ it is interesting to observe that we found the new covering lattices by looking at triangulations refining the Delone subdivisions of the lattices E_d^* which inherits as much symmetry as possible. By looking at a corresponding refinement of E_7^*, we also found a new covering record in dimension 7. It remains to see if these results have a common explanation.

Theorem. ([SV04b]) In dimension 8, there exists a lattice L_8^c with $\Theta(L_8^c) = 3.1423\ldots$.

Motivated by the work of Cohn and Kumar on the lattice packing problem we proved

Theorem. ([SV04b]) The Leech lattice provides a locally optimal lattice covering in dimension 24.

This provides a first step for proving the conjecture that the Leech lattice gives the optimal sphere covering in dimension 24. The proof does not make use of computers.

We conclude with Table 2 which lists the currently best known lattice covering in dimensions $6, \ldots, 24$.

d	**lattice**	**density Θ_d**	**d**	**lattice**	**density Θ_d**
6	L_6^c	2.464803	16	A_{16}^*	15.310927
7	L_7^c	w.i.p.	17	A_{17}^*	18.287811
8	L_8^c	3.142297	18	A_{18}^*	21.840949
9	A_9^5	4.340185	19	A_{19}^*	26.081820
10	A_{10}^*	5.251713	20	A_{20}^*	31.143448
11	A_{11}^4	5.598338	21	A_{21}^*	37.184568
12	A_{12}^*	7.510113	22	Λ_{22}^*	≤ 27.8839
13	A_{13}^7	7.864060	23	Λ_{23}^*	≤ 15.3218
14	A_{14}^5	9.006610	24	Λ_{24}	7.903536
15	A_{15}^8	11.601626			

Table 2. Best known lattice coverings.

6. The Situation

The situation of the sphere covering problem is quite embarrassing. We think that the restriction to lattices is a crucial restriction and that there are sphere coverings in low dimensions beating the optimal lattice coverings. Another point of embarrassment is Table 2 which should — and definitely can — be drastically improved at least for $9 \leq d \leq 21$. Then, the covering densities of the lattices Λ_{22}^* and Λ_{23}^* are not known and a proof of the global optimality of the Leech lattice covering seems not to be in reach at the moment.

References

[SV04a] A. Schürmann and F. Vallentin, *Computational approaches to lattice packing and covering problems*, 36 pages, arXiv:math.MG/0403272.

[SV04b] ———, *Local covering optimality of lattices: Leech lattice versus root lattice E_8*, 13 pages, arXiv:math.MG/0405441.

[Vor08] G. F. Voronoi, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxiéme Mémoire. recherches sur les parallélloedres primitifs.*, J. Reine Angew. Math. **134** (1908), 198–287, and **136** (1909), 67–181.

Hermite constants.

Renaud Coulangeon

This is a survey on recent work about generalizations of the classical Hermite constant $\gamma_n = \sup_{A\in P_n^1} \min_{X\in\mathbb{Z}^n\setminus\{0\}} A[X]$, where P_n^1 stands for the set of n-ary real positive definite quadratic forms with determinant 1.

First we present two examples of *Hermite like constants*, namely the Hermite-Rankin constant ([7], [3]) and the Hermite-Humbert constant([4], [1]). These examples, and others, fit into the general setting of *adelic geometry of numbers* that was developed recently by Takao Watanabe and which is explained below (see [9] and [6] for details):

Let k be a number field, and $\mathfrak{V} = \mathfrak{V}_f \cup \mathfrak{V}_\infty$ the set of places of k. In what follows, G denotes a connected reductive algebraic group over k. Let

$$\rho : G \longrightarrow GL(V)$$

be a strongly k-rational absolutely irreducible representation of G on a k-vector space V and D the highest weight space of ρ, with stabilizer P (parabolic subgroup). Then $X := G/P$ is a smooth projective variety embedded in $\mathbb{P}(V)$ via ρ. One also needs a maximal compact subgroup K in $G(\mathbb{A})$, satisfying some technical assumptions (see [9]). Namely, if for $x \in GL(V(\mathbb{A}))V(k)$, we set $||x||_{\mathbb{A}} := \prod_{v\in\mathfrak{V}} ||x_v||_v$, we assume that $||.||_{\mathbb{A}}$ is K-invariant. Moreover, one can normalize $||.||_{\mathbb{A}}$ by the condition that $||x_0||_{\mathbb{A}} = 1$ for $x \in D(k) \setminus \{0\}$. Let $G(\mathbb{A})^1 := \{g \in G(\mathbb{A}) : \forall \chi \in X_k(G) \quad |\chi(g)|_{\mathbb{A}} = 1\}$. For each $g \in G(\mathbb{A})^1$, define $H_g(x) := ||\rho(g\gamma)x_0||_{\mathbb{A}}^{1/[k:\mathbb{Q}]}$, where $x = \rho(\gamma)x_0$. Then

Theorem 1 (Watanabe, 2000 [9])**.**

$$\begin{aligned} K \setminus G(\mathbb{A})^1/G(k) &\longrightarrow \mathbb{R}_+ \\ g &\mapsto \min_{x\in X(k)} H_g(x) \end{aligned}$$

is a bounded continuous function. The generalized Hermite constant associated to $(\rho, ||.||_{\mathbb{A}})$ *is*

$$\mu(\rho, ||.||_{\mathbb{A}}) := \max_{g\in G(\mathbb{A})^1} \min_{x\in X(k)} H_g(x)^2.$$

Examples. Let G be the general linear group GL_n. Varying the ground field k and the representation ρ, one obtains:

(1) $k = \mathbb{Q}$,
  (a) ρ the natural representation in $\mathbb{Q}^n$,
    then $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_n$, the Hermite constant.
  (b) ρ_d the natural *exterior* representation in $\bigwedge^d \mathbb{Q}^n$,
    then $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_{n,d}$, the Hermite-Rankin constant.

(2) $k =$ number field,
  ρ the natural representation in k^n,
  then $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_{n,k}$, the Hermite-Humbert constant.

The last part of the talk is devoted to the so-called Voronoï theory. We first recall the following classical theorem

Theorem 2 (Voronoï's theorem 1908 [8])**.** *A positive definite quadratic form A is* **extreme** *(i.e. achieves a local maximum of the function γ) if and only if it is* **perfect** *and* **eutactic**.

A similar characterization holds for extremality with respect to the Hermite-Rankin invariant [3] and the Hermite-Humbert invariant [4]. This allowed us to compute the actual value of the Hermite-Humbert constant in dimension 2 over real quadratic fields of small discriminant:

d	2	3	5
$\gamma_{2,\mathbb{Q}(\sqrt{d})}$	$4/(2\sqrt{6}-3)$	4	$4/\sqrt{5}$

Baeza, Coulangeon, Icaza, O'Ryan (2001) [1]

In a recent work with Watanabe ([5]), we defined the Hermite constant of a quaternion field, and also obtained a characterization of extreme points in terms of perfection and eutaxy. An important tool regarding this kind of problems is the theory developed by Bavard in [2]. It would, of course, be interesting to extend these results to a widest class of Hermite like invariants, and to know for instance under which assumptions on the group G and the representation ρ a Voronoï type theorem holds for Watanabe's constant $\mu(\rho, ||.||_{\mathbb{A}})$.

References

[1] R. Baeza, R. Coulangeon, M.I. Icaza et M. O'Ryan (2001), *Hermite's constant for quadratic number fields*, Experimental Mathematics **10**, no. 4, 543–551.

[2] C. Bavard *Systole et invariant d'Hermite*, J. Reine Angew. Math. **482** (1997), 93–120.

[3] R. Coulangeon, (1996) *Réseaux k-extrêmes.*, Proc. London Math. Soc. (3), **73**, no. 3, 555–574.

[4] R. Coulangeon (2001), *Voronoï theory over algebraic number fields*, Monographies de l'Enseignement Mathématique, no. 37, 147–162.

[5] R. Coulangeon et T. Watanabe, *Hermite constant and Voronoï theory over a quaternion skew field*, submitted.

[6] M. Masanori et T. Watanabe, *Adèle geometry of numbers*, Class field theory – its centenary and prospect (Tokyo, 1998), Math. Soc. Japan, Tokyo (2001), 509–536.

[7] R. A. Rankin, *On positive definite quadratic forms*, J. London Math. Soc., **28** (1953), 309–314.

[8] G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques : 1 Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine angew. Math, **133** (1908), 97–178.

[9] T. Watanabe, *On an analog of Hermite's constant.*, J. Lie Theory, **10** (2000), no. 1, 33–52.

K. Saito's conjecture on positivity of eta products and "extremal pair" of lattices

Tomoyoshi Ibukiyama

This report is a summary of the paper [1]. Let $\eta(\tau)$ be the Dedekind eta function defined by

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

where $q = e^{2\pi i \tau}$ and $\tau \in \mathbb{C}$, $Im(\tau) > 0$. In his theory of extended affine root systems and other things, K. Saito treated eta products of the form

$$\prod_i \eta(i\tau)^{e(i)}$$

where $e(i)$ are integers which might be negative, and considered the condition that the coefficients of the q-expansion of this function are all non-negative. For example, in his paper [2], he defined a notion of elliptic eta product and he proved that an eta product of this kind has only non-negative coefficients if and only if this is not a cusp form. There are exactly four such eta products. These cases are examples of his more general conjecture on the positivity of eta products defined by "regular systems of weight" ([2], [3]). Apparently irrelevant to this, he also gave a conjecture in his paper [4] that for any natural number h the eta product

$$\frac{\eta(h\tau)^{\phi(h)}}{\prod_{d|h} \eta(d\tau)^{\mu(d)}}$$

has only non-negative Fourier coefficients, where $\phi(h)$ is the Euler function and $\mu(d)$ is the Möbius function. He has proved this conjecture for $h = 2$, 3, 5, 6, 10. When h is a prime p or a product of two different primes p, q, we can see that the latter conjecture is contained in the former conjecture. Anyway we can prove the latter conjecture when h is a power of any prime p. Namely we have

Main Theorem

(1) For any prime p, all the Fourier coefficients of

$$\frac{\eta(p\tau)^p}{\eta(\tau)} = q^{(p^2-1)/12} \prod_{n=1}^{\infty} (1 - q^{pn})^p (1 - q^n)^{-1}$$

are non-negative.

(2) For any prime p and any natural number a, all the Fourier coefficients of

$$\frac{\eta(p^a\tau)^{p^a - p^{a-1}} \eta(p\tau)}{\eta(\tau)}$$

are non-negative.

The outline of the proof is given as follows. The assertion (2) is an easy corollary of the assertion (1). So we prove (1). For the sake of simplicity, we write $f_p(\tau) = \eta(p\tau)^p/\eta(\tau)$. We also assume that $p \geq 5$ since the case $p = 2$ or 3 is easier.

(i) A key point of the proof of (1) is to express this function as a difference $\theta_{L_1}(\tau) - \theta_{L_2}(\tau)$ of theta functions associated with a lattice L_1 and a sublattice $L_2 \subset L_1$ up to constant. It is clear that such difference has only non-negative coefficients. The Fourier coefficients of $f_p(\tau)$ starts in a sense from the biggest possible power of q, and in this sense, the pair L_1 and L_2 may be called "extremal pair" of lattices as an analogue of the usual extremal lattice.

(ii) We need some characterization of $f_p(\tau)$ as a modular form. We put

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}); c \equiv 0 \bmod p \right\}$$

and for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$, we put $\psi(\gamma) = \left(\frac{(-1)^{(p-1)/2}}{d}\right)$. We denote by $M_k(\Gamma_0(p), \psi)$ the space of holomorphic modular forms of $\Gamma_0(p)$ with character ψ. Then, we can show that $f_p(\tau)$ is, up to constant, the unique element in $M_{(p-1)/2}(\Gamma_0(p), \psi)$ such that it has at the cusp $i\infty$ zero of order more than or equal to $(p^2-1)/24$. This is an easily proved lemma but useful.

(iii) To find the lattices we want, the theory of cyclotomic fields is helpful. We take the cyclotomic field generated by $\zeta = e^{2\pi i/p}$. We regard $\mathbb{Q}(\zeta)$ as a $(p-1)$ dimensional vector space over $\mathbb{Q}$ with a positive definite quadratic form $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x\overline{x})/p$ and take ideals in the ring of integers $\mathbb{Z}[\zeta]$ as lattices. We put $L_1 = (1-\zeta)^{(p-3)/2}\mathbb{Z}[\zeta]$ and $L_2 = (1-\zeta)^{(p-1)/2}\mathbb{Z}[\zeta]$. The minimum length of elements of these lattices are at most $p-1$. This is fairly small compared with $(p^2-1)/12$ which we expect for $f_p(\tau)$. So lattices does not seem very promising at first look for big p.

(iv) But a really surprising point is that the number of vectors in L_1 and L_2 are the same up to the length $(p^2-1)/12-1$. This can be proved by some tricky argument. Then we can show $f_p(\tau) = (\theta_{L_1}(\tau) - \theta_{L_2}(\tau))/p(p-1)$.

Open problem: When h is divisible by at least two distinct primes, the conjecture becomes more complicated and we have no general answer, except for some affirmative examples proved by alternating sum of theta functions.

References

[1] T. Ibukiyama, Positivity of eta products – a certain case of K. Saito's conjecture, to appear in Proceedings RIMS.

[2] K. Saito, Extended affine root systems V. Elliptic eta-products and their Dirichlet series. *Proceedings on Moonshine and related topics (Montréal, QC, 1999), 185–222, CRM Proc. Lecture Notes, 30, Amer. Math. Soc., Providence, RI, 2001*

[3] K. Saito, Duality for regular systems of weights. Mikio Sato: a great Japanese mathematician of the twentieth century. *Asian J. Math.* 2 (1998), no. 4, 983–1047.

[4] K. Saito, Non-negativity of Fourier Coefficients of Eta-products (in Japanese), *Proceedings of the Second Spring Conference on Modular Forms and Related Topics, 2003 at Hamana Lake, ed. T. Ibukiyama* (2004), 95–142.

Hermitian vector bundles and extension groups on arithmetic varieties

Klaus Künnemann
(joint work with Jean-Benoît Bost)

Let K be a number field with ring of integers $\mathcal{O}_K$. For hermitian vector bundles $\overline{F}$ and $\overline{G}$ on the arithmetic curve $S = \operatorname{Spec} \mathcal{O}_K$, we introduce the group $\widehat{\operatorname{Ext}}^1(F, G)$ of admissible extensions of $\overline{F}$ by $\overline{G}$

$$\overline{\mathcal{E}} : 0 \to \overline{G} \to \overline{E} \to \overline{F} \to 0$$

(i.e. the underlying sequence of projective $\mathcal{O}_K$-modules is exact and $\overline{F}_{\mathbb{C}}$ and $\overline{G}_{\mathbb{C}}$ carry the induced hermitian metrics from $\overline{E}_{\mathbb{C}}$). For arithmetic curves, this group has a natural structure of a real torus with Riemannian metric. The *size* $\int(\overline{\mathcal{E}})$ of an admissible extension $\overline{\mathcal{E}}$ is a measure for its non-triviality and is defined as the distance to zero in the torus. Using the transference theorem from the geometry of numbers and the inequalities relating $\widehat{\operatorname{udeg}}$, $\hat{\mu}_{\max}$, and $-\log \lambda_1$ discussed in the talk of Jean-Benoît Bost at this meeting, one obtains the following fundamental inequality

$$\hat{\mu}_{\min}(\overline{G}) - \hat{\mu}_{\max}(\overline{F}) + \int(\overline{\mathcal{E}}) \leq \frac{\log |\Delta_K|}{[K:\mathbb{Q}]} + \log \left(\frac{\operatorname{rk}_K G \cdot \operatorname{rk}_K F}{2} \right),$$

which relates the size of $\overline{\mathcal{E}}$ to slope invariants of the involved hermitian vector bundles.

A prori the size of an extension $\overline{\mathcal{E}}$ may decrease under base change for a finite extension L/K of the ground field. The problem of invariance of size under base change is discussed. It asks whether the (suitably normalized) size of an extension remains invariant under base change for finite extensions L/K. In the case $K = \mathbb{Q}$, we give the following positive answers to this problem. The size $\int(\overline{\mathcal{E}})$ is invariant under base change if i) $L/\mathbb{Q}$ is abelian, or ii) $\overline{F^\vee \otimes G}$ is a root lattice, or iii) $\overline{F^\vee \otimes G}$ is a lattice of Voronoi's first kind. Using reduction theory, one gets furthermore that the size is invariant under base change up to a constant which depends only on K and the ranks of F and G.

As an example of an admissible extension, the arithmetic Hodge extension associated with an elliptic curve is introduced and discussed. Let X be an elliptic curve over K which has semiabelian reduction and admits a projective, regular, semistable model $\mathcal{X}$ over S. Let $\overline{\mathcal{H}}$ denote the rank two hermitian vector bundle given as the hypercohomology $\mathcal{H} = H^1(\mathcal{X}, \Omega^{\cdot}_{\mathcal{X}/S,\leq 1})$ of the truncated de Rham complex equipped with the hermitian metric from complex Hodge theory. The hypercohomology spectral sequence degenerates at E_2 and $\mathcal{H}$ defines a natural extension of $H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ by $H^0(\mathcal{X}, \Omega^1_{\mathcal{X}/S})$. We obtain an admissible extension which we call the *arithmetic Hodge extension*. An application of the fundamental inequality to this extension gives an upper bound for the Faltings height of X in terms of the conductor of X and the size of the Hodge extension.

A local-global principle for extensibility of representations of quadratic forms and applications

Myung-Hwan Kim
(joint work with Wai-Kiu Chan, Byeong Moon Kim, Byeong-Kweon Oh)

In 1978, Hsia, Kitaoka and Kneser [HKK] proved the following remarkable theorem:

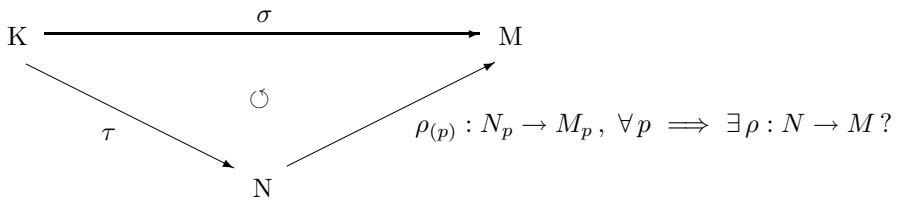
Theorem 1. (Hsia-Kitaoka-Kneser) *Let M be a positive definite $\mathbb{Z}$-lattices of rank $m \geqslant 2n+3$. Then there exists a constant $C = C(M) > 0$, depending only on M, such that M represents any positive definite $\mathbb{Z}$-lattice N of rank n, provided that $\mu_1(N) > C$ and M_p represents N_p at every prime p, where $\mu_1(N)$ is the minimum of N.*

See [BR], [CEJ], [J1], [J2], [JK], and [DS], [OS], [R], [T] for related works.

Let us consider a more general setting as follows: Let K and M be positive definite $\mathbb{Z}$-lattices of rank k and m, respectively, with $0 \leqslant k < m$, such that M represents K via σ. Let N be any positive definite $\mathbb{Z}$-lattice of rank n with $k < n < m$, representing K via τ. Assume further that for every prime p, there exists a local representation $\rho_{(p)} : N_p \to M_p$ such that $\rho_{(p)} \circ \tau_p = \sigma_p$ on K_p. We can ask: *"Under what condition does there exist a global representation $\rho : N \to M$ such that $\rho \circ \tau = \sigma$ on K ?"*

A representation $\sigma : K \to M$ is said to be *extensible* to N (at p, resp.) via τ if there exists a representation $\rho : N \to M$ ($\rho_{(p)} : N_p \to M_p$, resp.) such that Diagram $(*)$ commutes. Such ρ ($\rho_{(p)}$, resp.) is called an *extension* of σ to N (at p, resp.) via τ.

Diagram $(*)$



In this talk, we prove

Theorem 2. *If $m \geqslant k+2(n-k)+3$, then there exists a constant $C = C(K, M) > 0$, depending only on K and M, such that the local extensibility of σ to N at every prime p via τ implies the global extensibility of σ to N via τ, provided that $\mu_{k+1}(N) > C$, where $\mu_{k+1}(N)$ is the $(k+1)$-th successive minimum of N.*

In this vein, we may call Theorem 2 a local-global principle for extensibility for representations of $\mathbb{Z}$-lattices.

Observe that if we replace $\mathbb{Z}$-lattices K, M, N by quadratic spaces $\mathbb{Q}K, \mathbb{Q}M, \mathbb{Q}N$, respectively, then there exists a representation $\rho' : \mathbb{Q}N \to \mathbb{Q}M$ by Hasse-Minkowski's theorem, provided that $\sigma : \mathbb{Q}K \to \mathbb{Q}M$ is extensible to $\mathbb{Q}N$ at p via $\tau : \mathbb{Q}K \to \mathbb{Q}N$ for every p and hence there exists a representation $\rho : \mathbb{Q}N \to \mathbb{Q}M$ such that $\rho \circ \tau = \sigma$ by Witt's theorem. So, the local-global principle for extensibility of representations holds over $\mathbb{Q}$.

If we let $K = \{0\}$, then $\sigma = \tau = 0$ and hence any $\rho_{(p)} : N \to M$ is an extension of σ to N at every p via τ. Therefore, Theorem 1 follows immediately as a special case of Theorem 2.

In matrix term, Theorem 2 can be rephrased as following:

Theorem 3. *Let $M \in \mathcal{S}_m^+(\mathbb{Z})$, $H \in \mathcal{S}_{n-k}^+(\mathbb{Z})$ and $A \in \mathcal{M}_{k\times m}(\mathbb{Z})$, $B \in \mathcal{M}_{k\times(n-k)}(\mathbb{Z})$ such that $m \geqslant k + 2(n-k) + 3$. Then there exists a constant $C = C(B, M) > 0$, depending only on B and M, satisfying the following property: If $X^t MX = H$ and $AX = B$ has a solution $X \in \mathcal{M}_{m\times(n-k)}(\mathbb{Z}_p)$ for all p and $\mu_1(H) > C$, then it has a solution $X \in \mathcal{M}_{k\times(n-k)}(\mathbb{Z})$.*

As a very simple application of Theorem 3 (with $n = 2$ and $k = 1$), we prove: *If $m \geqslant 6$, then the system of equations*

$$\begin{cases} c_1x_1^2 + \cdots + c_mx_m^2 = h \\ a_1x_1 + \cdots + a_mx_m = b \end{cases}$$

has a solution in $\mathbb{Z}$ if h is sufficiently large, c_i's are pairwise coprime positive odd integers, and $(h-b)a_1 \cdots a_m$ is even.

This can be regarded as a generalization of Cauchy's Lemma which was used in the proof of his famous polygonal number theorem. Theorem 3 can also be used to show that certain Fourier coefficients of Siegel-Jacobi theta series do not vanish.

A $\mathbb{Z}$-lattice M is called (*almost*) *n-universal* if M represents all $\mathbb{Z}$-lattices of rank n (except finitely many, resp.). An (almost) n-universal $\mathbb{Z}$-lattice is called *new* if it does not contain an (almost) n-universal sublattice of smaller rank. As another application of Theorem 2, we prove that there are infinitely many new almost 2-universal $\mathbb{Z}$-lattices of rank 6. More precisely: *$\mathbb{Z}$-lattices of the form $M(a, b) \cong \langle 1, 1, 2, 5, a, b\rangle$ are new almost 2-universal if a is sufficiently large, where $a \leqslant b$ such that $5 \nmid (a, b)$, $8 \nmid (a, b)$, and $p^2 \nmid (a, b)$ for each prime p satisfying $(\frac{10}{p}) = -1$.*

This is a quite different feature for almost universality compared to the fact that there are only finitely many new n-universal $\mathbb{Z}$-lattices (see [KKO]).

References

[BR] S. Böcherer, S. Raghavan, On Fourier coefficients of Siegel modular forms, *J. Reine Angew. Math.* 384 (1988), 80–101.

[CEJ] W. K. Chan, D. Estes and M. Jöchner, Representations of codimension ≥ 3 by definite quadratic forms, *J. Number Theory* 71 (1998), 81–85.

[DS] W. Duke and R. Schulze-Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoid, *Invent. Math.* 99 (1990), 49–57.

[HKK] J. Hsia, Y. Kitaoka and M. Kneser, Representations of positive definite quadratic forms, *J. Reine Angew. Math.* 301 (1978), 132–141.

[J1] M. Jöchner, Representation of positive definite quadratic forms with congruence and primitive conditions II, *J. Number Theory* 50 (1995), 145–153.

[J2] M. Jöchner, On the representation theory of positive definite quadratic forms, Integral Quadratic Forms and Lattices (Seoul, 1998), 73–86, *Contemp. Math.* 249, Amer. Math. Soc., 1999.

[JK] M. Jöchner and Y. Kitaoka, Representation of positive definite quadratic forms with congruence and primitive conditions, *J. Number Theory* 48 (1994), 88–101.

[KKO] B. M. Kim, M.-H. Kim, B.-K. Oh, A finiteness theorem for representability of Quadratic Forms by Forms, to appear in *J. Reine Angew. Math.*

[OS] K. Ono and K. Soundararajan, Ramanujan's ternary quadratic forms, *Invent. Math.* 130 (1997), 415–454.

[R] S. Raghavan, Modular forms of degree n and representations by quadratic forms, *Ann. of Math.* 70 (1959), 446–477.

[T] W. Tartakovski, Die Gesamtheit der Zhalen, die durch eine positiv quadratische Form $F(x_1, \ldots, x_s)$ $(s \geqslant 4)$ darstellbar sind, *Izv. Akad. Nauk SSSR.* 7 (1929), 111–122; 165–196.

Minkowski's second theorem over a simple algebra

Takao Watanabe

Let k be a global field, D a central division k-algebra of degree d and $\mathfrak{A} = M_m(D)$ the simple algebra of m by m matrices with entries in D, V a right free $\mathfrak{A}$-module of rank n with a basis $e_1, \cdots, e_n$ and G the group of $\mathfrak{A}$-linear automorphisms of V. By the obvious way, V and G are identified with $M_{mn,m}(D)$ and $GL_{mn}(D)$, respectively. For a place v of k, let k_v be a completion of k at v. Since $D \otimes_k k_v$ is a central simple k_v-algebra, it is isomorphic with an algebra $M_{d/d_v}(D(v))$, where $D(v)$ is a division k_v-algebra of degree d_v. Then $\mathfrak{A} \otimes_k k_v$ and $V \otimes k_v$ are identified with $M_{m_v}(D(v))$ and $M_{m_v n, m_v}(D(v))$, respectively, where $m_v = dm/d_v$. We denote by $G(\mathbf{A})$ the adele group of G.

Let $s \geqslant t > 0$ be positive integers and let $\mathcal{I}_{s,t}$ denote the set of all subsets $I \subset \{1, 2, \ldots, s\}$ with cardinality $|I| = t$. For each infinite place v, the map $A \mapsto A^*$ from $M_{s,t}(D(v))$ to $M_{t,s}(D(v))$ is defined by $A^* = (\overline{a}_{ij})^T$ for $A = (a_{ij})$, where the superscript T means the transpose and $a_{ij} \mapsto \overline{a}_{ij}$ stands for the canonical involution of $D(v)$. The local height $F_v^{(s,t)}$ on the matrix space $M_{s,t}(D(v))$ is defined as follows:

$$F_v^{(s,t)}(A) = \begin{cases} |\mathrm{Nr}_{M_t(D(v))/k_v}(A^*A)|_{k_v}^{1/2} & (v \text{ is infinite}) \\ \sup\limits_{I \in \mathcal{I}_{s,t}} (|\mathrm{Nr}_{M_t(D(v))/k_v}({}_I A)|_{k_v}) & (v \text{ is finite}) \end{cases}$$

where ${}_I A$ denotes the t by t submatrix of $A \in M_{s,t}(D(v))$ having rows indexed by I. Then, for $g = (g_v) \in G(\mathbf{A})$, we define the global twisted height $H_g : V \longrightarrow \mathbf{R}_+$ by

$$H_g(X) = \prod_{v \in \mathfrak{V}} F_v^{(m_v n, m_v)}(g_v X)^{1/(dm)} \qquad \text{for } X \in V.$$

For $g \in G(\mathbf{A})$ and a positive real number λ, we set

$$\Omega_g(\lambda) = \{x \in Ge_1 \ : \ H_g(x) \leqslant \lambda\}.$$

Then $\Omega_g(\lambda)\mathfrak{A}^\times = \Omega_g(\lambda)$, and $\Omega_g(\lambda)/\mathfrak{A}^\times$ is a finite set. The i-th successive minima $\lambda_i(g)$ of g is defined to be

$$\lambda_i(g) = \min\{\lambda > 0 \ : \ \Omega_g(\lambda) \text{ contains } i \ \mathfrak{A}\text{-linearly independent elements}\}.$$

We introduce the notion of a *g-chain*. A sequence of n $\mathfrak{A}$-linearly independent elements $x_1, \dots, x_n \in Ge_1$ is identified with the matrix $\boldsymbol{x} = (x_1, \dots, x_n)$ in G. We call an element $\boldsymbol{x} \in G$ a g-chain if $H_g(x_1) = \lambda_1(g)$ and

$$H_g(x_i) = \min\{H_g(y) \ : \ y \in Ge_1 \text{ and } x_1, \dots, x_{i-1}, y \text{ are } \mathfrak{A}\text{-linearly independent}\}$$

holds for all $i = 2, \dots, n$. Let $\mathcal{X}_g$ denote the set of all g-chains in G. If $\boldsymbol{x} \in \mathcal{X}_g$, we set

$$\lambda_i(g, \boldsymbol{x}) = H_g(x_i) \qquad \text{for } i = 1, 2, \dots, n.$$

If $m \geqslant 2$, then $\mathfrak{A}$ has zero divisors, and we can not conclude that $x_1, \dots, x_{i-1}, y$ are $\mathfrak{A}$-linearly independent even if $y \notin x_1\mathfrak{A} + \cdots + x_{i-1}\mathfrak{A}$. Taking account of this, we define another successive minima $\mu_i(g, \boldsymbol{x})$ for $g \in G(\mathbf{A})$ and $\boldsymbol{x} \in G$ as follows:

$$\mu_i(g, \boldsymbol{x}) = \min\{H_g(y) \ : \ y \in Ge_1 \text{ and } y \notin x_1\mathfrak{A} + \cdots + x_{i-1}\mathfrak{A}\}\,.$$

We define the constant $c(g)$ by

$$c(g) = \min_{\boldsymbol{x} \in \mathcal{X}_g} \max_{1 \leqslant i \leqslant n} \left\{ \frac{\lambda_i(g, \boldsymbol{x})}{\mu_i(g, \boldsymbol{x})} \right\} \geqslant 1\,.$$

The main theorem is the following, which is an extension of Minkowski's second theorem.

Theorem 1. *The inequality*

$$\lambda_1(g) \cdots \lambda_n(g) \leqslant c(g)^n \widetilde{\gamma}_n(\mathfrak{A})^{1/(dm)} |\mathrm{Nr}_{M_{mn}(D)/k}(g)|_{\mathbf{A}}^{1/(dm)}$$

holds for any $g \in G(\mathbf{A})$, where we put

$$\widetilde{\gamma}_n(\mathfrak{A}) = \max_{g \in G(\mathbf{A})} \frac{\lambda_1(g)^{dmn}}{|\mathrm{Nr}_{M_{mn}(D)/k}(g)|_{\mathbf{A}}}\,.$$

If $m = 1$, i.e., $\mathfrak{A} = D$ is a division algebra, then $c \equiv 1$ and we have

$$\lambda_1(g) \cdots \lambda_n(g) \leqslant \widetilde{\gamma}_n(D)^{1/d} |\mathrm{Nr}_{M_n(D)/k}(g)|_{\mathbf{A}}^{1/d}\,.$$

In the case that k is an algebraic number field and $d = m = 1$, this result is due to Vaaler [3]. The constant $\widetilde{\gamma}_n(\mathfrak{A})$ is an analogue of Hermite's constant. For example, if k is an algebraic number field, then $\widetilde{\gamma}_n(M_m(k)) = \gamma_{mn,m}(k)^{n[k:\mathbf{Q}]/2}$ holds. A Minkowski–Hlawka type lower bound of $\widetilde{\gamma}_n(\mathfrak{A})$ is given in [2]. If D is a quaternion algebra, then an upper bound of $\widetilde{\gamma}_n(D)$ is given in [1]. More general theory of Hermite's constant was developed in [4].

References

[1] R. Coulangeon and T. Watanabe, *Hermite constant and Voronoi theory over a quaternion skew field*, preprint.
[2] Y. Nakamura and T. Watanabe, The normalization constant of a certain invariant measure on $GL_n(D_{\mathbf{A}})$, Manuscripta Math. **115** (2004), 259–280.
[3] J. Vaaler, *The best constant in Siegel's lemma*, Monatsh. Math. **140** (2003), 71–89.
[4] T. Watanabe, *Fundamental Hermite constants of linear algebraic groups*, J. Math. Soc. Japan **55** (2003), 1061–1080
[5] T. Watanabe, *Minkowski's second theorem over a simple algebra*, preprint

On the basis problem for squarefree levels

Siegfried Böcherer

We first recall the definition of theta series: For a given positive definite even integral matrix S of even size $m = 2k$ we put

$$\vartheta^n(S, Z) = \sum_{X \in \mathbb{Z}^{(m,n)}} exp(tr(X^t S X Z))\,,$$

where Z is an element of Siegel's upper half space $\mathbb{H}_n$.
It is well known that this defines an element of $M_k^n(N, \chi_S)$, the space of Siegel modular forms of weight k and nebentypus $\chi_S = \left(\frac{(-1)^k det(S)}{\cdot}\right)$ for the group $\Gamma_0^n(N)$. For a genus $\mathfrak{g}$ of such quadratic forms we can consider the linear space $\theta^n(\mathfrak{g})$ generated by all the $\vartheta^n(S)$ with $S \in \mathfrak{g}$. Then for a given quadratic character χ with $\chi(-1) = (-1)^k$

$$M_k^n(N, \chi) \supset \sum_{\mathfrak{g}} \theta^n(\mathfrak{g}),$$

where $\mathfrak{g}$ runs over all the genera of level (dividing) N, rank m and character χ.
We can ask two versions of the basis problem (with the notations above):
Weak version: *When does* $M_k^n(N, \chi)^{cusp} \subset \sum_{\mathfrak{g}} \theta^n(\mathfrak{g})$ *hold ?*
Genus version: *Here we fix a genus* $\mathfrak{g}$ *and ask, whether* $M_k^n(N, \chi)^{cusp} \subset \theta^n(\mathfrak{g})$ *holds.*
In my talk I present two recent contributions to these questions, both for squarefree levels. From now on N should be squarefree.
Theorem 1: (with Katsurada and Schulze-Pillot)
If $k \geq 2n+1$*, then all cusp forms of degree n, weight k and character* χ *are linear combination of appropriate theta series, i.e.*

$$M_k^n(N, \chi)^{cusp} \subset \sum_{\mathfrak{g}} \theta^n(\mathfrak{g})\,.$$

In this formulation, we avoid any problem at the bad primes, but we have to allow theta series from sufficiently many genera of levels dividing N. In the proof, a recent result of Katsurada and Schulze-Pillot about the space of Eisenstein series is crucial [4]; it allows us to use the "pullback method" for a "simple" Eisenstein series of level N; here "simple" means that we can compute (or avoid) contributions

from the bad primes. An additional feature used here is the injectivity of the $U(p)$-operator ($p \mid N$) on such spaces [2].

The second theorem is about the genus version. We will only consider the case n=1 and the case N=q (a prime). We have not much hope to extend this to the Siegel case, the restriction to prime level is only done to simplify our statements. In principle, our methods work for arbitrary squarefree level.
To illustrate the result, we recall a famous theorem of Waldspurger: For a prime $q \equiv 1$ and m divisible by 4, we denote by $\mathfrak{g}(m, q, q^\nu)$ the genus of quadratic forms of level q and discriminant q^ν with ν odd, $1 \leq \nu \leq m-1$ and we put $\theta(m, q, q^\nu) = \theta^1(\mathfrak{g}(m, q, q^\nu)$.

Theorem (Waldspurger)

$$M_k(\Gamma_0(q), k, \chi)^{cusp} \subset \theta(m, q, q) + \theta(m, q, q^{m-1}) \iff$$
the Hecke operator $U(q)$ does not have real eigenvalues.

This is a somewhat mysterious condition and one may naturally ask what happens for the remaining genera. Surprisingly (for me), the situation becomes much simpler:

Theorem 2: For $1 < \nu < m-1$ we always have

$$M_k(\Gamma_0(q), \chi)^{cusp} \subset \theta(m, q, q^\nu)$$

Remarks:

- The really delicate case is $m = 4$, where only the genera treated by Waldspurger exist.
- This result also works for theta series with harmonic polynomials.
- There is also a formulation for squarefree N (instead of $N = q$).
- There is also a version of this for $m \equiv 2$ modulo 4.
- Our method also works for Haupttypus (trivial character), but here Waldspurger already had an affirmative answer to the basis problem (even for more general levels, but always just for one particular genus). By our method, we can get a result for the genus version of the basis problem for *all* genera!

References

[1] Böcherer, S.: The genus version of the basis problem for elliptic modular forms. In preparation
[2] Böcherer, S.: On the Hecke operator U(p). Preprint 2004
[3] Böcherer, S., Katsurada, H., Schulze-Pillot, R.: On the basis problem for Siegel modular forms of squarefree level. In preparation
[4] Katsurada, H., Schulze-Pillot, R.: In preparation
[5] Waldspurger, J.-L.: L'engendrement par des series de theta de certains espaces de formes modulaires. Invent. 50, 135–168 (1978)

Reporter: Cordian Riener, Maria Teider

Participants

Prof. Dr. Kanat Abdukhalikov
abdukhalikov@math.kz
abdukhalik@member.ams.org
Institute of Mathematics
Pushkin Str. 125
480100 Almaty Kazakhstan
Kazakstan

Prof. Dr. Michael Baake
mbaake@math.uni-bielefeld.de
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld

Prof. Dr. Roland Bacher
Roland.Bacher@ujf-grenoble.fr
Laboratoire de Mathematiques
Universite de Grenoble I
Institut Fourier
B.P. 74
F-38402 Saint-Martin-d'Heres Cedex

Prof. Dr. Christine Bachoc
bachoc@math.u-bordeaux1.fr
Laboratoire d'Algorithmique
Arithmetique
Universite Bordeaux I
351 cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Eiichi Bannai
bannai@math.kyushu-u.ac.jp
Faculty of Mathematics
Graduate School
Kyushu University
Hakozaki 6-10-1, Higashi-ku
Fukuoka 812-8581
JAPAN

Prof. Dr. Eva Bayer-Fluckiger
eva.bayer@epfl.ch
Institut de Mathematiques
Ecole Polytechnique Federale
de Lausanne
MA-Ecublens
CH-1015 Lausanne

Prof. Dr. Jean-Claude Belfiore
belfiore@enst.fr
E.N.S.T.
Dept. Communications & Electronique
46, rue Barrault
F-75013 Paris

Prof. Dr. Anne-Marie Berge
berge@math.u-bordeaux1.fr
Laboratoire d'Algorithmique
Arithmetique
Universite Bordeaux I
351 cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Siegfried Böcherer
boecherer@math.uni-mannheim.de
boecherer@t-online.de
Fakultät für Mathematik und
Informatik
Universität Mannheim
68131 Mannheim

Prof. Dr. Jean-Benoit Bost
Jean-Benoit.Bost@math.u-psud.fr
Department of Mathematics
Univ. Paris-Sud
Bat. 425
F-91405 Orsay Cedex

Frank Bowert
Frank.Bowert@mathematik.uni-dortmund.de
Fachbereich Mathematik
Universität Dortmund
44221 Dortmund

Prof. Dr. Jean-Paul Cerri
Jean-Paul.CERRI@wanadoo.fr
2, route de Saint-Die
F-88600 Aydoilles

Prof. Dr. Wai Kiu Chan
wkchan@wesleyan.edu
Department of Mathematics and
Computer Science, Wesleyan Univers.
655 Science Tower
265 Church Street
Middletown CT 06459-0128
USA

Prof. Dr. Renaud Coulangeon
coulange@math.u-bordeaux.fr
Mathematiques et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Philippe Elbaz-Vincent
pev@math.univ-montp2.fr
Departement de Mathematiques
Universite Montpellier II
Place Eugene Bataillon
F-34095 Montpellier Cedex 5

Prof. Dr. Philippe Gaborit
gaborit@unilim.fr
LACO
Universite de Limoges
123, av. A. Thomas
F-87060 Limoges

Dr. Herbert Gangl
herbert@mpim-bonn.mpg.de
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Julien Houriet
Julien.houriet@epfl.ch
Departement de Mathematiques
Ecole Polytechnique Federale
de Lausanne
CH-1015 Lausanne

Prof. Dr. Tomoyoshi Ibukiyama
ibukiyam@math.wani.osaka-u.ac.jp
Department of Mathematics
Graduate School of Science
Osaka-University Machikaneyama 1-16
Toyonaka
Osaka 560-0043
JAPAN

Prof. Dr. Maria Ines Icaza
icazap@inst-mat.utalca.cl
Instituto de Matematica y Fisica
Universidad de Talca
Campus Lircay
Casilla 721
Talca
CHILE

Prof. Dr. Myung-Hwan Kim
mhkim@math.snu.ac.kr
Department of Mathematical Sciences
Seoul National University
Seoul 151-747
KOREA

Dr. Oliver D. King
ok@csua.berkeley.edu
Whitehead Institute for Biomedical
Research
Nine Cambridge Center
Cambridge MA 02142-1479
USA

Prof. Dr. Aloys Krieg
krieg@mathA.rwth-aachen.de
Lehrstuhl A für Mathematik
RWTH Aachen
52056 Aachen

Prof. Dr. Abhinav Kumar
abhinavk@mit.edu
Dept. of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
USA

Prof. Dr. Klaus Künnemann
klaus.kuennemann@...
...mathematik.uni-regensburg.de
NWF-I Mathematik
Universität Regensburg
93040 Regensburg

Prof. Dr. Jacques Martinet
martinet@math.u-bordeaux1.fr
Jacques.Martinet@math.u-bordeaux1.fr
Laboratoire d'Algorithmique
Arithmetique
Universite Bordeaux I
351 cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Jorge F. Morales
morales@math.lsu.edu
Dept. of Mathematics
Louisiana State University
Baton Rouge, LA 70803-4918
USA

Prof. Dr. Gabriele Nebe
nebe@math.rwth-aachen.de
Lehrstuhl D für Mathematik
RWTH Aachen
52056 Aachen

Dr. Phong Nguyen
pnguyen@di.ens.fr
Departement de Mathematiques et
d'Informatique
Ecole Normale Superieure
45, rue d'Ulm
F-75005 Paris Cedex

Frederique Oggier
frederique.oggier@epfl.ch
Institut de Mathematique Bernoulli
Ecole Polytechnique Federale
de Lausanne
CH-1015 Lausanne

Prof. Dr. Wilhelm Plesken
plesken@momo.math.rwth-aachen.de
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Prof. Dr. Michael E. Pohst
pohst@math.tu-berlin.de
Fakultät II -Institut f. Mathematik
Technische Universität Berlin
Sekr. MA 8-1
Straße des 17. Juni 136
10623 Berlin

Prof. Dr. Heinz-Georg Quebbemann
quebbemann@mathematik.uni-oldenburg.de
Fachbereich 6 Mathematik
Carl von Ossietzky
Universität Oldenburg
26111 Oldenburg

Cordian Riener
cordi777@gmx.de
Laboratoire d'Algorithmique
Arithmetique
Universite Bordeaux I
351 cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Rudolf Scharlau
Rudolf.Scharlau@math.uni-dortmund.de
Fachbereich Mathematik
Universität Dortmund
44221 Dortmund

Prof. Dr. Rene Schoof
schoof@science.uva.nl
schoof@mat.uniroma2.it
Dipartimento di Matematica
Universita degli Studi di Roma II
Tor Vergata
Via della Ricerca Scientifica
I-00133 Roma

Dr. Rainer Schulze-Pillot
schulzep@math.uni-sb.de
schulzep@count.math.uni-sb.de
Fachrichtung - Mathematik
Universität des Saarlandes
Postfach 151150
66041 Saarbrücken

Prof. Dr. Jean-Pierre Serre
serre@dma.ens.fr
6, Avenue de Montespan
F-75116 Paris

Prof. Dr. Tetsuji Shioda
shioda@rikkyo.ac.jp
shioda@rkmath.rikkyo.ac.jp
Dept. of Mathematics
Rikkyo University
Nishi-Ikebukuro
Tokyo 171
JAPAN

Prof. Dr. Nils-Peter Skoruppa
skoruppa@math.uni-siegen.de
Universität Siegen
Fachbereich 6 Mathematik
Walter-Flex-Str. 3
57068 Siegen

Prof. Dr. Patrick Sole
ps@essi.fr
Laboratoire d'Informatique
Signaux et Systems de
Sophia Antipolis (I3S)
250, rue Albert Einstein
F-06560 Valbonne

Bernd Souvignier
souvi@math.ru.nl
Dept. of Mathematics
Radboud Universiteit Nijmegen
Postbus 9010
NL-6500 GL Nijmegen

Dipl.-Math. Ute Staemmler
ute@math.uni-sb.de
Fachrichtung 6.1 Mathematik
Universität des Saarlandes
Geb. 27
66123 Saarbrücken

Prof. Dr. Ivan Suarez Atias
ivan.suarez@epfl.ch
Departement de Mathematiques
Ecole Polytechnique Federale
de Lausanne
CH-1015 Lausanne

Maria Teider
maria.teider@mathematik.uni-ulm.de
Abteilung Reine Mathematik
Universität Ulm
89069 Ulm

Prof. Dr. Pham Huu Tiep
tiep@math.ufl.edu
Dept. of Mathematics
University of Florida
358 Little Hall
P.O.Box 118105
Gainesville, FL 32611-8105
USA

Frank Vallentin
vallenti@ma.tum.de
Zentrum Mathematik
TU München
Boltzmannstr. 3
85748 Garching bei München

Prof. Dr. Boris B. Venkov
bbvenkov@yahoo.com
St. Petersburg branch of Steklov
Mathematical Institute
Fontaka 27
191011 St. Petersburg
Russia

Prof. Dr. Emanuele Viterbo
viterbo@polito.it
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca degli Abruzzi, 24
I-10129 Torino

Ina Voigt
Ina.Voigt@mathematik.uni-dortmund.de
Fachbereich Mathematik
Universität Dortmund
44221 Dortmund

Prof. Dr. Takao Watanabe
watanabe@math.wani.osaka-u.ac.jp
Dept. of Mathematics
Graduate School of Science
Osaka University
Machikaneyama 1-16, Toyonaka
Osaka 560-0043
JAPAN