Existence and Non-Existence of Extremal Lattices

Rudolf Scharlau

Technische Universität Dortmund

TU Wien, Institut für Diskrete Mathematik und Geometrie
7. Juni 2011

Foundations – Lattices

Definition 1.1

A (full) **lattice** on a quadratic vector space (V, b) over $\mathbb{Q}$ is a subset of the shape

$$\begin{aligned} L &= \{x_1 v_1 + x_2 v_2 + \cdots + x_n v_n \mid x_1, \ldots, x_n \in \mathbb{Z}\} \\ &= \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \ldots \oplus \mathbb{Z}v_n \end{aligned}$$

for some basis $v_1, v_2, \ldots, v_n$ of V.

The associated integral quadratic form is

$$Q(x_1, \ldots, x_n) = \tfrac{1}{2} \sum_{i,j} b(v_i, v_j)\, x_i x_j .$$

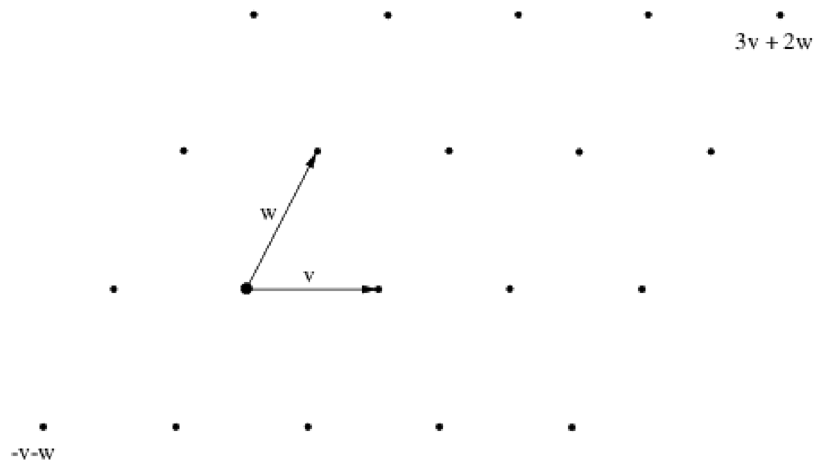

Fig. 1: A lattice in dimension 2

The most basic invariant of a lattice (after its dimension or rank) is its determinant:

Definition 1.2

The **Gram matrix** of a lattice L w.r.t. a basis $v_1, \ldots, v_n$ is the symmetric $n \times n$-matrix $(b(v_i, v_j))$.

The **determinant** $\det L$ of L is the determinant of any Gram matrix of L.

The determinant of L ist the square of the volume of a fundamental domain of L acting V.

Foundations | Lattices
Extremal lattices | Genera of lattices
Explicit classification of large genera | Some important examples of lattices

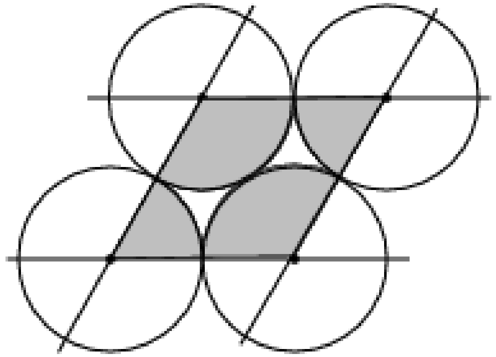

Fig. 2: Density of the hexagonal lattice

Rudolf Scharlau | Extremal Lattices

Foundations | Lattices
Extremal lattices | Genera of lattices
Explicit classification of large genera | Some important examples of lattices

Definition 1.3

A quadratic lattice is called an **integral lattice** if $b(L, L) \subseteq \mathbb{Z}$.
Equivalently, $L \subseteq L^{\#}$, where

$$L^{\#} := \{x \in V \mid \forall y \in L : b(x, y) \in \mathbb{Z}\}$$

is the **dual lattice** of L.

L is called **even** if $b(x, x) \in 2\mathbb{Z}$ for all $x \in L$.

"Even" implies "integral".

Rudolf Scharlau | Extremal Lattices

Foundations | Lattices
Extremal lattices | Genera of lattices
Explicit classification of large genera | Some important examples of lattices

Definition 1.4

Let L be an integral lattice. The **discriminant group** of L is the factor group $L^{\#}/L$. Its order is $|L^{\#}/L| = |\det L|$.

The **exponent of L** is the exponent of its discriminant group, that is, the smallest natural number m such that $mL^{\#} \subseteq L$.

The **level** of an even lattice L is the smallest natural number m such that the rescaled dual lattice ${}^{m}L^{\#} = {}^{m}(L^{\#})$ is again even.

The level is equal to the exponent or 2 times the exponent of L.

Proof: The dual lattice corresponds to the inverse of the Gram matrix (in a two-fold sense).

Rudolf Scharlau | Extremal Lattices

Theorem 1.1 (Finiteness of Class Number)

For a given determinant d, the number of isometry classes of (positive definite) integral lattices with determinant d is finite.

This is a consequence of reduction theory, which gives a lattice basis with $b(v_i, v_i) \leq C\, d^{1/n}$ for some constant C.
The constant C depends on the dimension of the lattice, and on the reduction theory chosen. Important notions of "reduced basis" have been introduced by Korkine and Zolotareff, Hermite, Minkowski, Voronoi, B.A. Venkov, and LLL (A. Lenstra, H. Lenstra and L. Lovasz).

Foundations – Genera of lattices

Let p be a prime number. Every quadratic vector space (V, b) over $\mathbb{Q}$ embeds into a quadratic vector space (V_p, b) over $\mathbb{Q}_p$, where $V_p := V \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and the natural extension $b_p : V_p \times V_p \to \mathbb{Q}_p$ is simply denoted by b again.
(V_p, b) is called the **completion** of (V, p) at the prime p.
This definition extends to $p = \infty$ with $\mathbb{Q}_\infty := \mathbb{R}$.
Similarly, a quadratic lattice L embeds into its **completion** $L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p$.
One also sets $L_\infty = V_\infty$.

The local-global principle of Minkowski and Hasse for quadratic spaces does not hold for quadratic lattices. Therefore, the following notion is introduced.

Definition 1.5

Two lattices L and M are in the same **genus** if $L_p \cong M_p$ for all $p \in \mathbb{P} \cup \{\infty\}$.
The number $h(\mathcal{G})$ of isometry classes in a genus $\mathcal{G}$ is finite. It is called the **class number** of the genus.

For this talk, dimension, parity (even/odd), level and determinant are enough to distinguish genera.

Foundations – Some important examples of lattices

- the Barnes lattice P_6: $n = 6,\ \det = 7^3,\ \min = 4$
- the Coxeter-Todd lattice K_{12}: $n = 12,\ \det = 3^6,\ \min = 4$
- the Barnes-Wall lattice BW_{16}: $n = 16,\ \det = 2^8,\ \min = 4$
- the Leech lattice Λ_{24}: $n = 24,\ \det = 1, \min = 4$
- the Quebbemann lattices Q_{32}: $n = 32,\ \det = 2^{16},\ \min = 6$
- the lattices $P_{48p}, P_{48q}, P_{48n}$ $n = 48,\ \det = 1,\ \min = 6$
- the Nebe lattice (August 2010): $n = 72,\ \det = 1,\ \min = 8$

Extremal lattices

Extremality via modular forms

If L is an even lattice of even dimension $n = 2k$ and level ℓ, we denote by

$$\Theta_L(q) = \sum_{m \geq 0} r_L(m) q^m, \quad r_L(m) := |\{x \in L \mid (x, x) = 2m\}|$$

its **theta series**, where as usual $q = e^{2\pi i z}$ and z is a variable in the upper half plane. This is a modular form of weight k for the group $\Gamma_0(\ell)$ and a certain quadratic character $\varepsilon : \Gamma_0(\ell) \to \{\pm 1\}$. Using standard notation this means that

$$\Theta_L \in \mathcal{M}_k(\ell, \varepsilon).$$

Definition 2.1

a) Let $\mathcal{M}$ be a subspace of $\mathcal{M}_k(\ell)$. We say that **extremality is definable** with respect to $\mathcal{M}$ if the projection $\mathcal{M} \to \mathbb{C}^d$ to the first $d = \dim \mathcal{M}$ coefficients of the q-expansion

$$f = \sum_{m \geq 0} a_m q^m \mapsto (a_0, a_1, \ldots, a_{d-1})$$

is injective. The unique element $F_{\mathcal{M}} \in \mathcal{M}$ with q-expansion

$$F_{\mathcal{M}} = 1 + \sum_{m \geq d} a_m q^m$$

is then called the **extremal modular form** in $\mathcal{M}$.

b) Let L be an even lattice of dimension $2k$ and level ℓ and $\mathcal{M}$ be a subspace of $\mathcal{M}_k(\ell, \varepsilon)$ with $\Theta_L \in \mathcal{M}$ (where ε denotes the character defined by the determinant of L). We say that L is **extremal with respect to** $\mathcal{M}$ if extremality is definable with respect to $\mathcal{M}$ and $\Theta_L = F_{\mathcal{M}}$.

Informally, a lattice is extremal if its minimum is as large as the space of modular forms where its theta series lives allows.

The following has been proposed by H.-G. Quebbemann.

Definition 2.2 (Modular extremal lattices)

Consider a genus $\mathcal{G}$ of even dimension $n = 2k$, level $\ell \in \{\, 1, 2, 3, 5, 7, 11, 23\}$, determinant ℓ^k. A lattice L in $\mathcal{G}$ is called **modular of level** ℓ if it is isometric to its rescaled dual lattice ${}^{\ell}(L^{\#})$.
Such a lattice is called **(modular) extremal** if it is extremal with respect to the subspace of $\mathcal{M} \subset \mathcal{M}_k(\ell, \varepsilon)$ of forms "invariant" (up to sign, as predicted by the general transformation formula for the dual lattice) under the Fricke involution.

Example: the Barnes lattice in dimension 6

There is a well-known self-dual hermitian $\mathbb{Z}[\alpha]$-lattice, $\alpha = \frac{1+\sqrt{-7}}{2}$, of dimension 3 and minimum 2, which we denote be J_3 (following [Coh76]). Its unitary group is $U(J_3) = 2 \times G_{168}$, where $G_{168} \cong L_3(2) \cong L_2(7)$ is the simple group of order 168.

The group $U(J_3)$ is a primitive irreducible complex reflection group, occurring as no. 24 in the list of such groups given by Shephard and Todd [ShTo54].

A natural Gram matrix for J_3 is

$$J_3 \cong \begin{pmatrix} 2 & \overline{\alpha} & 1 \\ \alpha & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

It also occurs in the work of Mimura [Mim82], where hermitian lattices over imaginary quadratic fields, generated by norm 2 vectors, are classified in a "direct" approach.

A 7-modular $\mathbb{Z}$-lattice is obtained from J_3 by ordinary "transfer" (trace of the hermitian form). The modularity comes from multiplying with $\sqrt{-7}$. It has minimum 4 and is therefore extremal. It is isometric to the Barnes lattice P_6 and to the Craig lattice $A_6^{(3)}$.

The minimum $m_{\mathrm{ext}}(n, \ell)$ of (hypothetical) extremal lattices

n	ℓ	1	2	3	5	6	7	11	14	15	23
4		–	2	2	2	2	2	**4**	**4**	**4**	**6**
6		–	–	2	–	–	**4**	4	–	–	(8)
8		2	2	2	**4**	**4**	4	**6**	**6**	**6**	(10)
10		–	–	2	–	–	4	6	–	–	(12)
12		–	2	**4**	4	4	**6**	**8**	**8**	**8**	
14		–	–	4	–	–	**6**	8	–	–	
16		2	**4**	4	6	**6**	**6**	(10)	10	10	
18		–	–	4	–	–	**8**	10	–	–	
20		–	4	4	?6	6	8	(12)	12	12	
22		–	–	4	–	–	8				
24		**4**	4	**6**	**8**	**8**	10				

n	ℓ	1	2	3	5	6	7	11	14	15	23
28		–	4	6	8	8	10				
32		4	**6**	6	10	10	12				
36		–	6	?**8**	10	10					
40		4	6	8	12	12					
44		–	6	8	12	12					
48		**6**	**8**	10							
52		–	8	10							
56		6	8	10							
60		–	8	12							
64		6	10	12							
72		**8**	10								
80		8	12								

See [SchaSchu99] for more detailed information about the tables above.

Existence of extremal lattices

Extremal lattices with minimum 4

For each pair (n, ℓ) such that ℓ is as before, and $m_{\text{ext}}(n, \ell) = 4$, there exists an extremal lattice.

In the smallest dimension $n = n(\ell) = 24, 16, 12, 8, \ldots$, the extremal lattice is unique: Leech, Barnes-Wall, Coxeter-Todd, Q_8, Barnes, ...

Extremal lattices with minimum 6

For each pair (n, ℓ) such that ℓ is as before, and $m_{\text{ext}}(n, \ell) = 6$, there exists an extremal lattice, with the exception of $(12, 7^6)$ and possibly $(20, 5^{10})$.

The extremal lattice of minimum 6 is unique in the cases $(16, 5)$ (Bachoc, Nebe and Venkov [BaVeNe01]), $(8, 11), (8, 14), (4, 23)$ (minimal dimensions) and $(14, 7)$ (not minimal).

Explicit classification of large genera

General strategies for classification

Enumerate a set of representatives for a specified genus $\mathcal{G}$, following these steps:

1. Generate lattices in $\mathcal{G}$ by some algebraic procedure
2. Test for isometry with lattices already constructed
3. Verify the completeness of the list

Step 1 is typically handled by Kneser's method of neighbouring lattices: L and L' are neighbors, if their intersection $L \cap L'$ is of index 2 in both of them.
All neigbours of L can be efficiently generated from (certain) classes of $L/2L$.
Step 2 is a matter of invariants (theta series, order of automorphism group, successice minima, ...) and of sophisticated algorithms for testing isometry of a given pair of lattices (improved backtracking), by Plesken and Souvignier.
Step 3 is handled by the following:

Theorem 3.1 (Minkowski's mass formula)

Let $L = L_1, \ldots, L_h$ be a system of representatives for a genus $\mathcal{G}$ of positive definite lattices of dimension n. The sum of the inverses of the orders of their automorphism groups (the so-called **mass** *of $\mathcal{G}$) is the product of certain* **representation densities** *$\alpha_p(L, L)$, where p runs over all primes, with a certain factor "at infinity":*

$$\sum_{j=1}^{h} \frac{1}{|\operatorname{Aut}(L_j)|} = \gamma(n) \prod_p \alpha_p^{-1}(L, L).$$

Some genera of level 2, 5, 7, 11

Proposition 3.1 (Level 11, dimension 12)

The genus $II_{12}(11^6)$ has class number 67323. *It contains precisely*

- 27193 *lattices with minimum* 2
- 40036 *lattices with minimum* 4
- 94 *lattices with minimum* 6
- *no lattice with minimum* 8.

This reproves the absence of extremal lattices in this genus, first shown by Nebe and Venkov, using Siegel modular forms.

The automorphism groups for the genus $II_{12}(11^6)$:
consider $o(L) := |\operatorname{Aut}(L)|$:
There exist

- 16613 lattices (24.7%) with trivial group, i.e. $o(L) = 2$
- 50641 lattices for which $4 \mid o(L)$
- 6065 lattices for which $3 \mid o(L)$
- 421 lattices for which $5 \mid o(L)$
- 0 lattices for which $7 \mid o(L)$ or $13 \mid o(L)$
- 1 lattice for which $11 \mid o(L)$

Proposition 3.2 (Level 5, dimension 16, [GrLam10])

The genus $II_{16}(5^4)$ has class number 848. *It contains exactly one lattice with minimum* 4. *This lattice has* $2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$ *minimal vectors and* $288000 = 2^8 \cdot 3^2 \cdot 5^3$ *automorphisms.*

Further data for this genus: consider $o(L) := |\operatorname{Aut}(L)|$:

- for all lattices $2^5 \mid o(L)$
- 831 lattices for which $3 \mid o(L)$
- 529 lattices for which $5 \mid o(L)$
- 155 lattices for which $7 \mid o(L)$
- 8 lattices for which $11 \mid o(L)$
- 0 lattices for which $13 \mid o(L)$

Theorem 3.2 (B. Hemkemeier, R.S., 2010/11)

There exists a unique extremal lattice of dimension 14 and level 7.

It has $560 = 2^4 \cdot 5 \cdot 7$ *minimal vectors (of norm* 6*) and*
$1008 = 2^4 \cdot 3^2 \cdot 7$ *automorphisms,*
more precisely $\mathrm{Aut}(L) \cong \mathrm{PSL}(8) \times 2$.

In this genus, the existence of an extremal lattice had been open for a long time. The automorphism group is rather small; this might explain why the lattice was not found earlier.

Furthermore, there was no reason to expect uniqueness.

The following precise information on the genus $II_{14}(7^7)$ come from a long computation with the program `tn` finished in February 2011.

Proposition 3.3

The genus $II_{14}(7^7)$ *has class number* 83006. *It contains precisely*

- 46574 *lattices with minimum* 2
- 36431 *lattices with minimum* 4
- 1 *lattice with minimum* 6.

The automorphism groups for the genus $II_{14}(7^7)$:
consider $o(L) := |\mathrm{Aut}(L)|$:
There exist

- 12827 lattices (15.4%) with trivial group, i.e. $o(L) = 2$
- 70108 lattices for which $4 \mid o(L)$
- 11797 lattices for which $3 \mid o(L)$
- 353 lattices for which $5 \mid o(L)$
- 82 lattices for which $7 \mid o(L)$
- 0 lattices for which $11 \mid o(L)$ or $13 \mid o(L)$

Theorem 3.3 (Level 2, dimension 20)

The genus $II_{20}(2^{10})$ *has class number* 546. *It contains exactly three lattices with minimum* 4. *These lattices are modular and thus extremal. The orders of their automorphism groups are* $2^{14}3^6 5^1 11^1$, $2^8 3^3 5^1 11^1$, $2^{14}3^2 5^1$.

Bachoc and Venkov had shown already in 1998 that these three lattices are the only ones with minimum 4. There proof uses theta series with spherical coefficients and spherical designs and is rather long and complicated.

Work in progress and open tasks

Members of my group in Dortmund currently work on filling some of the remaining gaps in the above tables:

- For the genus $(14, 11^7)$, show that no (modular) lattice of minimum 8 exists.
- Investigate the case $(18, 11^9)$, minimum 10.
- Prove the existence or non-existence of an extremal lattice (with minimum 6) in the genus $(20, 5^{10})$
- Investigate the cases $(2k, 7^k)$ for $k \geq 11$ (minimum ≥ 8)
- Decide whether an extremal lattice exists in the case $(36, 3^{18})$.

Some related open tasks:

- Make isometry testing for lattices still faster: investigate more thoroughly the behaviour of the depth parameter for “vector sums” of B. Souvignier’s programs for automorphisms and isometry [PlSo97].
- Improve strategies for choosing the next lattice in the neighbour process.
- Study the successive minima, in particular the “well-roundedness” of p-elementary lattices.

- C. Bachoc, G. Nebe: Extremal lattices of minimum 8 related to the Mathieu group M_{22}. J. reine angew. Math. **494** (1998).
- C. Bachoc, B. Venkov Modular forms, lattices, and spherical designs. In: *Réseaux eudliciens, designs sphériques et forms modulaires*, Monogr. Enseignement Math., Geneva 2001, 87–111.
- C. Batut, H.-G. Quebbemann, R. Scharlau: Computations of cyclotomic lattices. Experimental Math. **4**, No. 3 (1995), 175–179.
- A. M. Cohen: Finite complex reflection groups. Ann. Sci. Ecole Norm. Sup. **9** (1976), 379–436.
- J. H. Conway, N.J.A. Sloane: *Sphere packings, lattices and groups.* Springer-Verlag New York, 1988.
- R.L. Griess Jr., Ching Hung Lam: A moonshine path for 5A and associated lattices of ranks 8 and 16. arXiv:1006.3907v1 [math.GR]

- G. Nebe: An even unimodular 72-dimensional lattice of minimum 8. arXiv:1008.2862v3 [math.NT] (August 2010).
- W. Plesken, B. Souvignier: Computing isometries of lattices. J. Symbolic Comp. **24**, no. 3/4 (1997), 327–334.
- H.-G. Quebbemann: Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung. J. reine angew. Math. **326** (1981), 158–170.
- H.-G. Quebbemann: Modular Lattices in Euclidean Spaces. J. of Number Theory **54** (1995), 190–202.
- H.-G. Quebbemann: Atkin-Lehner eigenforms and strongly modular lattices. L’Enseignement Mathématique **43** (1997), 55–65.

- R. Scharlau, B. Hemkemeier: Classification of integral lattices with large class number. Math. of Comput. (1997).
- R. Scharlau, R. Schulze-Pillot: Extremal Lattices, In *Algorithmic Algebra and Number Theory*, edited by B.H. Matzat, G.-M. Greuel, G. Hiss, Springer Verlag 1999.
- G. C. Shephard, J. A. Todd: Finite unitary reflection groups. Canad. J. Math. **6** (1954), 274–304.
- D. Stehlé, M. Watkins: On the Extremality of an 80-Dimensional lattice. Proceedings from ANTS-IX, Springer 2010.
- M. Watkins: Another 80-dimensional extremal lattice. To appear in Journal de Théorie des Nombres de Bordeaux.