Representation of Quadratic Forms

Rainer Schulze-Pillot

Universität des Saarlandes, Saarbrücken, Germany

Beijing, September 27, 2012

Outline

1. Introduction
   - Theorem of Kloosterman and Tartakovskii
   - Theorem of Ellenberg and Venkatesh
2. Arithmetic and ergodic method
3. The analytic method

Representation of sufficiently large numbers

Theorem (Kloosterman 1924, Tartakovskii 1929)

Let $A \in M_m^{\mathrm{sym}}(\mathbb{Z})$ be a positive definite integral symmetric $m \times m$-matrix with $m \geq 5$. Then for every sufficiently large integer t for which

$$ {}^t\mathbf{x}_p A \mathbf{x}_p = t $$

is solvable with $\mathbf{x}_p \in \mathbb{Z}_p^m$ for all primes p the equation

$$ Q_A(\mathbf{x}) := {}^t\mathbf{x} A \mathbf{x} = t $$

is solvable with $\mathbf{x} \in \mathbb{Z}^m$
In other words:
Every sufficiently large integer t which is representable by the quadratic form Q_A locally everywhere is representable by Q_A globally.

Proof.

The original proof uses the Hardy-Littlewood circle method.
An alternative proof uses modular forms instead; we'll come back to that. □

A modified result of the same type is true for $m = 4$, for primitive solutions (the gcd of the components of the local/global solution vectors is 1) instead of arbitrary solutions, or more generally for solution vectors with bounded imprimitivity.

For $m = 3$ exceptions occur due to spinor genera. Again we'll come back to that.

Representation of matrices, simplest case

Theorem (Ellenberg, Venkatesh 2007)

Let $A \in M_m^{\mathrm{sym}}(\mathbb{Z})$ be a positive definite integral symmetric $m \times m$-matrix, let $n \leq m-5$.
Then there is a constant C such that for each positive definite matrix $T \in M_n^{\mathrm{sym}}(\mathbb{Z})$ with $\det(T)$ square free the equation

$$^tXAX = T$$

is solvable with $X \in M_{m,n}(\mathbb{Z})$
provided T satisfies:

1. *For each prime p the equation*

$$^tX_pAX_p = T$$

   is solvable with $X_p \in M_{m,n}(\mathbb{Z}_p)$.
2. $\min(T) := \min\{{}^t\mathbf{y}T\mathbf{y} \mid \mathbf{0} \neq \mathbf{y} \in \mathbb{Z}^n\} > C$

Outline of talk

- Arithmetic and ergodic approach
- Analytic approach

Representations in lattice notation

$(V, Q), (W, Q')$ quadratic spaces over $\mathbb{Q}$,
$(Q(x) = B(x, x)$, B symmetric bilinear form on $V)$,
$\dim(V) = m \geq \dim(W) = n$,
M a $\mathbb{Z}$-lattice on V, N a $\mathbb{Z}$-lattice on W.

Definition

W is represented by V if there is an isometric embedding $\varphi : W \to V$.
W is represented by V over $\mathbb{Q}_p$ if there is an isometric embedding $\varphi_p : W \otimes \mathbb{Q}_p \to V \otimes \mathbb{Q}_p$.
N is represented by M if there is an isometric embedding $\varphi : W \to V$ with $\varphi(N) \subseteq M$.
N is represented by M over $\mathbb{Z}_p$ if there is an isometric embedding $\varphi_p : W \otimes \mathbb{Q}_p \to V \otimes \mathbb{Q}_p$ with $\varphi(N \otimes \mathbb{Z}_p) \subseteq M \otimes \mathbb{Z}_p$.

The representation φ resp. φ_p of N by M is primitive if $M \cap \varphi(W) = \varphi(N)$.

Equivalence of notations

As above, $(V, Q), (W, Q')$ quadratic spaces over $\mathbb{Q}$,
$M = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_m$ a $\mathbb{Z}$-lattice with basis $(e_1, \ldots, e_m)$ on V,
$N = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_n$ a $\mathbb{Z}$-lattice with basis $(f_1, \ldots, f_n)$ on W.
$A = (B(e_i, e_j))$ the Gram matrix of Q with respect to the given basis of M,
$T = (B'(f_i, f_j))$ the Gram matrix of Q' with respect to the given basis of N.

Proposition

$N =: \langle T \rangle$ is represented (primitively) by $M = \langle A \rangle$ (over $\mathbb{Z}_p$) if and only if T is represented (primitively) by A (over $\mathbb{Z}_p$).
(T is represented primitively by A means: ${}^tXAX = T$ is solvable with an integral matrix X with elementary divisors equal to 1.)

Number fields

Everything carries over with
$\mathbb{Q}, \mathbb{Q}_p$ replaced by F, F_v and
$\mathbb{Z}, \mathbb{Z}_p$ replaced by $\mathfrak{o}, \mathfrak{o}_v$,
where F is a number field with ring of integers $\mathfrak{o}$ and v runs through the places of F.

Notice however: An $\mathfrak{o}$-lattice is allowed to be not free as an $\mathfrak{o}$-module, hence it is not immediate how to define a Gram matrix. For lattices of rank m one can use degenerate Gram matrices of size $m+1$, this complicates arguments.

Therefore: Don't use matrix notation in the number field case.

Minkowski-Hasse Theorem and Genus

Theorem (Minkowski-Hasse)

(W, Q') is represented by (V, Q) if and only if (W_v, Q'_v) is represented by (V_v, Q_v) for all places v of F.

Definition

Denote by O_V the group of isometries of the space (V, Q).
Lattices M, M_1 on V are in the same genus if and only if there is $u = (u_v)_v \in O_V(\mathbb{A})$ (adelic orthogonal group) with $uM = M_1$.
Equivalently: M, M_1 are isometric locally everywhere.

Theorem (Local global principle for genera of lattices)

Assume that the lattice N on W is represented by the lattice M on V over $\mathfrak{o}_v$ for all places v of F. Then N is represented by some lattice M_1 on V in the genus of M.

Quantitative local global principle

If F is totally real and M is totally definite, the number $r(M,N) := \#\{\sigma : N \to M \mid \sigma \text{ is isometric embedding}\}$ is finite, so is $\#O(M)$.

Put $r(\mathrm{gen}(M),N) := \dfrac{1}{\sum_{\{M'\}} \frac{1}{\#O(M')}} \sum_{\{M'\}} \dfrac{r(M',N)}{\#O(M')}$,

(sum over isometry classes of M' in the genus of M).

Theorem (Siegel's theorem)

$$r(gen(M),N) = c \cdot (\det N)^{\frac{m-n-1}{2}} (\det M)^{\frac{n}{2}} \prod_v \alpha_v(M,N),$$

with some constant c depending only on m,n. Here v runs over the nonarchimedean primes of F, the local densities $\alpha_v(M,N)$ measure the $\mathfrak{p}_v$-adic representations of N_v by M_v.

If M is indefinite, one has the same result for representation measures. These are defined via Haar measure on the orthogonal group.

They also occur as limits over numbers of representations inside a box (Duke/Rudnick/Sarnak).

Spinor genus

Definition

Consider lattices M, M_1 on V that are in the same genus (there is $u = (u_v)_v \in O_V(\mathbb{A})$ with $uM = M_1$).
Then M_1 is in the spinor genus of M if and only if

$$u \in O_V(F)\,\mathrm{Spin}_V(\mathbb{A})O_M(\mathbb{A}),$$

where $\mathrm{Spin}_V(\mathbb{A})$ is identified with its image in $O_V(\mathbb{A})$ under the covering map, $O_M(\mathbb{A})$ is the stabilizer in $O_v(\mathbb{A})$ of M.

Theorem (Eichler, 1952, strong approximation)

If V is indefinite spinor genus and isometry class coincide.
If V is definite and w a place where $V_w = V \otimes F_w$ is isotropic (represents zero nontrivially) then a lattice M_1 in the spinor genus of M is isometric to a lattice M_1' with $M_1' \otimes \mathfrak{o}_v = M \otimes \mathfrak{o}_v$ for all places $v \neq w$.

Representations in the spinor genus

Theorem (Kneser, Weil, 1961/62)

Assume $m \geq n+3$. Let N (on W') be represented by M (on V) locally everywhere (primitively).
Then N is represented globally (primitively) by some lattice M_1 in the spinor genus of M (is represented by the spinor genus of M), and the representation measures are the same for all spinor genera.

If $m = n+2$, there are finitely many square classes $c_i(F^\times)^2$ such that the same assertion holds for all N on W with $\det(W) \notin c_i(F^\times)^2$ for all i. Lattices N with $\det(W)$ in one of the exceptional square classes (and represented by M locally everywhere) are represented either by all spinor genera in the genus of M or by half of them.
The latter are called spinor exceptions.

Representations in the spinor genus, cont'd

Colliot-Thélène and Xu Fei interpret the occurrence of spinor exceptions as a Brauer-Manin obstruction.
In the case $m = 3, n = 1$ spinor exceptions have been classified explicitly (S-P 1977/1980 for unramified 2, Xu Fei general dyadic primes), one has for their representation number (or measures) a Siegel mass formula with characters.
Cases of codimension 0 or 1 have been treated by Chan and Xu Fei. They (and Xu Fei, Xu Fei/S-P) also obtain results about representation by the spinor genus of a fixed lattice.

In the indefinite case, due to all these results, the representation problem is essentially solved.
If the lattice representing lattice M is totally definite, the transition from spinor genus to isometry class is difficult.

The HKK theorem

Theorem (Hsia, Kitaoka, Kneser 1978)

*Let M be a positive definite $\mathfrak{o}$-lattice of rank $m \geq 2n+3$.
Then there is a constant $c(M)$ such that M represents all positive definite $\mathfrak{o}$-lattices N of rank n satisfying*

1. *M_v represents N_v for all places v of F*
2. *One has* $\min(N) \geq c(M)$

- The constant $c(M)$ can in principle be effectively computed.
- There is no statement about the number of representations.

Sketch of proof

Strong approximation allows to find a lattice M' in the spinor genus of M with $M'_v = M_v$ for all places v of F except a single place w (chosen suitably in advance) and such that M' represents N.
The proof in HKK then proceeds by constructing a representation of N by M itself starting from the given one by M', for this one has to first add another copy of N. This raises the bound on m from $n+3$ to $2n+3$.

Sketch of proof EV

Ellenberg/Venkatesh work group theoretically:
We have N embedded into $M' = uM$ which

$$u \in O_V(F) \prod_{v \neq w} O_M(\mathfrak{o}_v)\,\mathrm{Spin}_V(F_w),$$

we need the same with $u \in O_V(F)O_M(\mathbb{A})$ instead.

To achieve this, modify u by a suitable element of $O_{W_1}(F_w)$ where $W_1 = (FN)^{\perp}$.
This is accomplished using ergodic theory (for the spin group), technical difficulties are overcome using local arithmetic of (integral) quadratic forms.

Sketch of proof of EV, 2

Lemma

w a non-archimedean place of F, M_w an $\mathfrak{o}_w$-lattice of rank m on $V_w = V \otimes F_w$.
Let $\mathcal{W}$ be a set of regular subspaces of V_w, put $N_W := W \cap M_w$ for $W \in \mathcal{W}$
Assume that the (additive) w-adic valuation $\mathrm{ord}_w(disc(N_W))$ of the discriminants of the N_W is bounded by some $j \in \mathbb{N}$ independent of W.
Then the set $\mathcal{W}$ is contained in the union of finitely many orbits under the action of the compact open subgroup $\tilde{K}_w := \mathrm{Spin}_{M_w}(\mathfrak{o}_w) = \{\tau \in \mathrm{Spin}_V(F_w) \mid \tau(M_w) = M_w\}$ of $\mathrm{Spin}_V(F_w)$.

Sketch of proof EV, 3

Proposition

Put $\tilde{K}_v = \mathrm{Spin}_{M_v}(\mathfrak{o}_v)$ for finite places v of F
Let w be a fixed finite place of F and T_w a regular isotropic subspace of $V_w = V \otimes F_w$ with $\dim(T_w) \geq 3$.
Let $G_w = \mathrm{Spin}_V(F_w)$, $H_w = \mathrm{Spin}_{T_w}(F_w)$ and

$$\Gamma := \mathrm{Spin}_V(F) \cap \mathrm{Spin}_V(F_w) \prod_{v \neq w} \tilde{K}_v.$$

Let a sequence $(W_i)_{i \in \mathbb{N}}$ of subspaces W_i of V (over the global field F) be given such that $(W_i)_w^\perp = \xi_i T_w$ for each i with elements ξ_i from a fixed compact subset of G_w.

Then one has: If no infinite subsequence of the W_i has a nonzero intersection, the sets $\Gamma \backslash \Gamma \xi_i H_w$ are becoming dense in $\Gamma \backslash G_w$ as $i \to \infty$, i. e., for every open subset U of G_w one has $U \cap \Gamma \xi_i H_w \neq \emptyset$ for sufficiently large i.

Sketch of proof of EV, 4

The proposition is proved by Ellenberg and Venkatesh using ergodic methods, it is the heart of their proof.

The following proposition uses it to deduce a first result about existence of representations:

Proposition

Let $j \in \mathbb{N}$ and let w be a fixed finite place of F.
Let $(W_i)_{i\in\mathbb{N}}$ be a sequence of regular subspaces W_i of V of dimension $n \le m-3$ with isotropic orthogonal complement in V_w, with $\mathrm{ord}_w(\mathrm{disc}((W_i)_w \cap M_w)) \le j$ for all i, and such that no infinite subsequence has nonzero intersection.
Then $N_i = W_i \cap M$ is represented primitively by all lattices in the spinor genus $\mathrm{spn}(M)$ for sufficiently large i.

Proof of the proposition, 1

The proof proceeds as follows:
Put $\tilde{K}_v = \mathrm{Spin}_{\Lambda_v}(\mathfrak{o}_v)$ for all finite places v of F and
$\Gamma := \mathrm{Spin}_V(F) \cap \mathrm{Spin}_V(F_w) \prod_{v\neq w} \tilde{K}_w$.

By the lemma on orbits $(N_i)_w$ (and hence the $(W_i)_w$) fall into finitely many orbits under the action of the compact open group $\tilde{K}_w$; we can assume that they all belong to the same orbit:
With $T_w = (W_1)_w^\perp$ we have $(W_i)_w^\perp = \xi_i T_w$ with $\xi_i \in \tilde{K}_w$ for all i.

Any isometry class in $\mathrm{spn}(M)$ has a representative $\tilde{M} \subseteq V$ with $\tilde{M}_v = M_v$ for all finite places $v \neq w$ of F and $\tilde{M}_w = g_w M_w$ for some $g_w \in G_w = \mathrm{Spin}_V(F_w)$.

Proof of the proposition, 2

Remember: $(W_i)_w^\perp = \xi_i T_w$ with $\xi_i \in \tilde{K}_w$ and $\tilde{M}_w = g_w M_w$.

By the previous proposition for every open set $U \subseteq G_w$ there is an i_0 with $U \cap \Gamma \xi_i H_w \neq \emptyset$ for $i \geq i_0$.

Take $U = g_w \tilde{K}_w \subseteq G_w$ and obtain i_0 such that for all $i \geq i_0$ one has elements $\gamma_i \in \Gamma, \eta_i \in H_w, \kappa_i \in \tilde{K}_w$ with $g_w \kappa_i = \gamma_i \xi_i \eta_i$.

The lattice $M_i' := \gamma_i^{-1} \tilde{M}$ is in the isometry class of $\tilde{M}$; it satisfies $(M_i')_v = M_v$ for all finite $v \neq w$ and
$(M_i')_w = \gamma_i^{-1} g_w M_w = \xi_i \eta_i M_w = \xi_i \eta_i \xi_i^{-1} M_w$.

From this and $\xi_i \eta_i \xi_i^{-1}|_{(W_i)_w} = \mathrm{Id}_{(W_i)_w}$ we see $N_i = W_i \cap M_i'$, i.e., we have the requested primitive representation by a lattice in the given isometry class.

Sequences of lattices with growing minima

We can now turn the "no infinite subsequence with nonzero intersection"-condition into a condition about lattices with growing minima:

Proposition

Let $(N_i)_{i \in \mathbb{N}}$ be a sequence of $\mathfrak{o}$-lattices of rank $n \leq m - 3$. Assume: We can fix a finite place w of F and a $j \in \mathbb{N}$ with:

1. *N_i is represented locally everywhere primitively by M with isotropic orthogonal complement at the place w for all i.*
2. $\mathrm{ord}_w(\mathrm{disc}((M_i)_w)) \leq j$ *for all i.*
3. *The sequence $(\min(N_i))_{i \in \mathbb{N}}$ of the minima of the N_i tends to infinity.*

Then there is an $i_0 \in \mathbb{N}$ such that N_i is represented primitively by all isometry classes in the genus of M for all $i \geq i_0$.

Proof

Proof of proposition.

May consider only lattices in the spinor genus of M and assume $N_i \subseteq M$ primitive, let $W_i = FN_i$. By the previous proposition we must show: There is no infinite subsequence of the W_i with nonzero intersection. Otherwise:
Choose $\mathbf{0} \neq x \in M \cap \cap_{i \in I} W_i$ with I infinite. By primitivity:
$x \in N_i = M \cap W_i$ for infinitely many i.
This contradicts the assumption iii) that the minima of the M_i tend to infinity. $\square$

The main theorem

Theorem (Ellenberg and Venkatesh, slightly generalized)

Fix a finite place w of F and $j \in \mathbb{N}$.
Then there exists a constant $C := C(M, j, w)$ such that M primitively represents all $\mathfrak{o}$ - lattices N of rank $n \leq m - 3$ satisfying

1. *N is represented by M locally everywhere primitively with isotropic orthogonal complement at the place w.*
2. $\mathrm{ord}_w(\mathrm{disc}(N_w)) \leq j$
3. *The minimum of N is $\geq C$.*

The isotropy condition is satisfied automatically if $n \leq m - 5$ or if w is such that $\mathrm{disc}(M_w)$ *and* $\mathrm{disc}(N_w)$ *are units at w.*

The primitivity condition above may be replaced by bounded imprimitivity:
The representation φ of N by M has *imprimitivity bounded by $c \in \mathfrak{o}$* if $cx \in \varphi(N)$ for all $x \in F\varphi(N) \cap M$.

Matrix version of the main result

Here is a matrix version of the main result:

Theorem

Let $A \in M_n^{\mathrm{sym}}(\mathbb{Z})$ be a positive definite integral symmetric $m \times m$-matrix, fix a prime q and positive integers j, c.
Then there is a constant C such that a positive definite matrix $T \in M_n^{\mathrm{sym}}(\mathbb{Z})$ with $n \leq m - 3$ is represented by A (i.e., $T = {}^tXAX$ with $X \in M_{m,n}(\mathbb{Z})$) provided it satisfies:

1. *For each prime p there exists a matrix $X_p \in M_{nm}(\mathbb{Z}_p)$ with ${}^tX_pAX_p = T$ such that the elementary divisors of X divide c and such that the equations ${}^tX_qA\mathbf{y} = \mathbf{0}$ and ${}^t\mathbf{y}A\mathbf{y} = 0$ have a nontrivial common solution $\mathbf{y} \in \mathbb{Z}_q^m$*
2. $q^j \nmid \det(T)$
3. $\min\{{}^t\mathbf{y}T\mathbf{y} \mid \mathbf{0} \neq \mathbf{y} \in \mathbb{Z}^n\} > C$

The matrix X may be chosen to have elementary divisors dividing c.

Corollaries,1

Corollary

Let $F = \mathbb{Q}$, fix a prime q and $j \in \mathbb{N}$. In the following cases there exists a constant $C := C(M, j, q)$ such that M represents all $\mathbb{Z}$ - lattices N of rank n which are represented by M locally everywhere, have minimum $\geq C$ and satisfy $\mathrm{ord}_q(\mathrm{disc}(N)) \leq j$:

1. *$n \geq 6$ and $m \geq 2n$.*
2. *$n \geq 3$ and $m \geq 2n + 1$, with the additional assumption that in the case $n = 3$ the orthogonal complement of the representation of N_q in M_q is isotropic.*
3. *$n = 2$ and $m \geq 6$, with the additional assumption that in the case $m = 6$ the orthogonal complement of the representation of N_q in M_q is isotropic.*

Notice that in these cases we have no primitivity condition. In fact, work of Kitaoka implies that N can be replaced by a lattice N' which is represented locally primitively and has roughly the same minimum.

Corollaries, 2

Corollary

Let a positive definite $\mathbb{Z}$-lattice N_0 of rank $n \leq m - 3$ with Gram matrix T_0 be given. Let Σ be a finite set of primes with $q \in \Sigma$ such that one has

1. *M_p and N_p are unimodular for all primes $p \notin \Sigma$ and for $p = q$.*
2. *Each isometry class in the genus of M has a representative M' on V such that $M'_p = M_p$ for all primes $p \notin \Sigma$.*

Then there exists a constant $C := C(M, T_0, \Sigma)$ such that for all sufficiently large integers $a \in \mathbb{Z}$ which are not divisible by a prime in Σ, the $\mathbb{Z}$-lattice N with Gram matrix aT_0 is represented by M if it is represented by all completions M_p.

Again, work of Kitaoka implies that N can be replaced by a lattice N' which is represented locally primitively and has roughly the same minimum.

Remarks

- The main result also allows versions for representations with congruence conditions and for extensions of representations.
- The proof should also go through for hermitian forms.
- For applications it would sometimes be desirable to have a different condition than growing minimum of the lattices to be represented.
  It appears that at least the present method is not able to give such a result: If we consider an infinite sequence of lattices $N_i \subseteq M$ whose minimum is bounded, there must be infinite subsequences having a nonzero intersection, since there are only finitely many vectors of given length in M.

Extensions

Corollary

Fix a finite place w of F and $j \in \mathbb{N}, c \in \mathfrak{o}$.
Let $R \subseteq M$ be a fixed $\mathfrak{o}$-lattice of rank r with R_w unimodular, $\sigma : R \longrightarrow M$ a representation of R by M.
Then there exists a constant $C := C(M, R, j, w, c)$ such that one has: If $N \supseteq R$ is an $\mathfrak{o}$-lattice of rank $n \leq m - 3$ and

1. *For each place v of F there is a representation $\tau_v : N_v \longrightarrow M_v$ with $\tau_v|_{R_v} = \sigma_v$ with imprimitivity bounded by c and with isotropic orthogonal complement in M_w*
2. $\mathrm{ord}_w(\mathrm{disc}(N_w)) \leq j$
3. *The minimum of $N \cap (FR)^\perp$ is $\geq C$,*

then there exists a representation $\tau : N \longrightarrow M$ with $\tau|_R = \sigma$.
The representation may be taken to be of imprimitivity bounded by c.
The isotropy condition is satisfied automatically if $n \leq m - 5$ or if w is such that $\mathrm{disc}(M_w)$ and $\mathrm{disc}(N_w)$ are units at w.

Asymptotic formula

Always: $A \in M_m^{\mathrm{sym}}(\mathbb{Z})$ and $T \in M_n^{\mathrm{sym}}(\mathbb{Z})$, A positive definite, T positive semidefinite.

Idea: Prove the existence of a solution of ${}^tXAX = T$ (a *representation of T by A*) by proving more, namely an
asymptotic formula
for the *representation number*

$$r(A, T) := |\{X \in M_{m,n}(\mathbb{Z}) \mid {}^tXAX = T\}|,$$

i. e., a formula of the type

$$r(A, T) = \text{main term}(T) + \text{error term}(T)$$

where the main term grows faster than the error term if T grows in a suitable sense, e.g., $\min(T) := \min\{{}^t\mathbf{y}T\mathbf{y} \mid \mathbf{0} \neq \mathbf{y} \in \mathbb{Z}^n\}$ tends to ∞.

Theta series

A as always (symmetric of size m, positive definite). In addition: A has even diagonal.

Definition

The theta series (of degree 1) of A is

$$\vartheta(A,z) := \sum_{t=0}^{\infty} r(A,t)\exp(\pi i t z), \quad z \in H = \{z \in \mathbb{C} \mid \Re(z) > 0\}.$$

It is a modular form of weight $k = \frac{m}{2}$ for the group $\Gamma_0(N)$ where NA^{-1} is integral with even diagonal:
$\vartheta(A,\cdot) \in M_k(\Gamma_0(N),\chi)$ with χ depending on $\det(A)$.

Siegel theta series extend this to the theta series of degree n, encoding representation numbers of $n \times n$-matrices.

Siegel theta series

Write $\mathfrak{H}_n = \{Z = X + iY \in M_n^{\mathrm{sym}}(\mathbb{C}) \mid X, Y \text{ real}, Y > 0\}$ (Siegel's upper half space).

Definition

The Siegel theta series of degree n of A is

$$\vartheta^{(n)}(A,Z) := \sum_{T} r(A,T)\exp(\pi i \operatorname{tr}(TZ)), \quad Z \in \mathfrak{H}_n,$$

where T runs over positive semidefinite symmetric matrices of size n with even diagonal.
It is a Siegel modular form of weight $k = \frac{m}{2}$ for the group $\Gamma_0^{(n)}(N)$ where NA^{-1} is integral with even diagonal:

$\vartheta^{(n)}(A,\cdot) \in M_k^n(\Gamma_0^{(n)}(N),\chi)$ with χ depending on $\det(A)$.

Genus theta series

Definition

The genus theta series of degree n of A is

$$\vartheta^{(n)}_{\text{gen}}(A, Z) := \frac{\sum_{A'} \frac{\vartheta^{(n)}(A',Z)}{o(A')}}{\sum_{A'} \frac{1}{o(A')}},$$

where the summation runs over representatives A' of the integral equivalence classes in the genus of A and $o(A')$ denotes the number of automorphs (units) of A'.
We write

$$\vartheta^{(n)}_{\text{gen}}(A, Z) = \sum_T r(\text{gen}(A), T) \exp(\pi i \text{tr}(TZ))$$

and call the $r(\text{gen}(A), T)$ the average representation numbers for the genus.

Siegel's theorem, analytic

Theorem (Siegel's theorem)

The genus theta series $\vartheta^{(n)}_{gen}(A, Z)$ is in the space of Eisenstein series.

Asymptotic formula for $n = 1, m \geq 5$

Proof of the theorem of Kloosterman/Tartakovskii via modular forms.

The difference $\vartheta(A, z) - \vartheta_{\text{gen}}(A, z)$ is a cusp form of weight $m/2$.

We write

$$r(A, t) = r(\text{gen}(A), t)) + (r(A, t) - r(\text{gen}(A), t)).$$

The main term $r(\text{gen}(A), t)$ grows at least like $t^{\frac{m}{2}-1}$ for t that are represented locally everywhere
(estimate $\prod_p \alpha_p(A, t)$ from below by a constant or use an estimate for Fourier coefficients of Eisenstein series).

The error term $r(A, t) - r(\text{gen}(A), t)$ is the Fourier coefficient at t of a cusp form, hence grows at most like $t^{\frac{m}{4}}$. □

Asymptotic formula for $n = 1, m = 4, 3$

The same approach works for $m = 4$, with the following modifications:

1. The growth of the main term is only true for t which are represented primitively (with bounded imprimitivity) locally everywhere.
2. For the error term use the sharper Ramanujan-Petersson estimate.

Theorem (Duke/S-P 1990, S-P 2000)

Let M be a positive definite $\mathbb{Z}$-lattice of rank 3. Then every sufficiently large integer t which is represented with bounded imprimitivity by all completions M_p is represented by M unless one of the following cases occurs:

1. *t is not represented by the spinor genus of M.*
2. *t is not itself a spinor exception, but t/p^2 is a spinor exception for some "large" prime p (which then has to be inert in $\mathbb{Q}(-t\det(M))$).*

Complements

1. The analogues for totally real number fields are true for lattices of rank $m \geq 4$. The analogue for rank 3 is partly proven by Cogdell/Piatetskii-Shapiro/Sarnak (square free integers), the remaining part is work in progress by Chan and Hanke.
2. For function fields only the low dimensional cases give “definite” forms. Altug and Tsimerman (2012) prove the above result for $m = 3$ and square free integers.
3. All these results have versions for representations with congruence conditions and for representations in prescribed cones (use inhomogeneous theta series and theta series with spherical harmonics).

The 15, 290, and 451-Theorems

Theorem (451-Theorem, Rouse 2011)

Suppose the following is true (Conjecture of Kaplansky): Each of the ternary quadratic forms
$x^2+2y^2+5z^2+xz, x^2+3y^2+6z^2+xy+2yz, x^2+3y^2+7z^2+xy+xz$
represents all odd positive integers.
Then a positive definite integer valued quadratic form represents all odd positive integers if and only if it represents the following 46 *numbers:*
$1, 3, 5, 7, 11, 13, 15, 17, 19, 21, 23, 29, 31, 33, 35, 37, 39, 41, 47, 51,$
$53, 57, 59, 77, 83, 85, 87, 89, 91, 93, 105, 119, 123, 133, 137,$
$143, 145, 187, 195, 203, 205, 209, 231, 319, 385, 451.$

This varies the 15-Theorem (Conway/Schneeberger 1993) and the 290-Theorem (Bhargava/Hanke 2008-?) for representation of all positive integers by integral matrix resp. integer valued forms.

General n: Obstacles

For general n, the approach for $n = 1$ needs some modifications:

- An estimate of local densities from below shows: The main term grows like $\det(T)^{\frac{m-n-1}{2}}$ for $m \geq 2n+3$; this is in general not valid for smaller m.
- for small m, obtaining the required estimate from below for the product of densities is impossible, particularly bad examples arise if one does not require the existence of local primitive representations (X_p has trivial elementary divisors).
- The difference $\vartheta^{(n)}(A, \cdot) - \vartheta^{(n)}_{\text{gen}}(A, \cdot)$ vanishes at all zero dimensional boundary components of $\mathfrak{H}_n$, but it is not a cusp form. Instead it is a sum of a cusp form and of Eisenstein series of Klingen type associated to cusp forms in degree $r < n$. This makes it more difficult to estimate the Fourier coefficients.

Results of Raghavan and Kitaoka, I

Theorem (Raghavan, Annals 1959)

Assume $m \geq 2n+3$. Then for T running through positive definite integral $n \times n$-matrices with $\det(T) \to \infty$ and $\min(T^{-1}) \geq c \det(T)^{-\frac{1}{n}}$ for some constant $c > 0$ one has with $m = 2k$

$$r(A, T) = r(gen(A), t) + \mathrm{O}((\min(\mathrm{T}))^{\frac{\mathrm{n}+1-\mathrm{k}}{2}} \det(\mathrm{T})^{\frac{\mathrm{m}-(\mathrm{n}+1)}{2}}),$$

where $r(gen(A), T)$ grows like $\det(T)^{\frac{m-(n+1)}{2}}$).
In particular, all T which are represented over all $\mathbb{Z}_p$ by A, have sufficiently large minimum, and satisfy the condition on $\min(T^{-1})$ above are represented by A over $\mathbb{Z}$.

It should be noted that examples constructed with the help of the Leech lattice show that the error term can indeed grow as fast as the main term $r(gen(A), T)$ with respect to $\det(T)$ alone.

Results of Raghavan and Kitaoka, II

Theorem (Kitaoka 1982)

Assume $m \geq 2n+3$. Then for T running through positive definite integral $n \times n$-matrices with $\det(T) \to \infty$ and $\min(T) \geq c\det(T)^{\frac{1}{n}}$ for some constant $c > 0$ one has with $m = 2k$

$$r(A, T) = r(gen(A), t) + \mathrm{O}((\min(\mathrm{T}))^{\frac{n+1-k}{2}} \det(\mathrm{T})^{\frac{m-(n+1)}{2}}),$$

where $r(gen(A), T)$ grows like $\det(T)^{\frac{m-(n+1)}{2}}$).
In particular, all T which are represented over all $\mathbb{Z}_p$ by A, have sufficiently large determinant and satisfy the condition on $\min(T)$ above are represented by A over $\mathbb{Z}$.

Notice that by reduction theory one has $\min(T) = \mathrm{O}(\det(\mathrm{T})^{\frac{1}{n}})$.

Results of Raghavan and Kitaoka, III

Method of proof: Compute the Fourier coefficient $b(T)$ of $g(Z) := \vartheta^{(n)}(A, Z) - \vartheta^{(n)}_{\mathrm{gen}}(A, Z)$ as

$$\int_{\mathfrak{E}} g(Z)\exp(-2\pi i \mathrm{tr}(TZ))dX,$$

where the variable $Z = X + iT^{-1}$ runs over a cube of side length 1 with one corner in T^{-1} and use a generalized Farey dissection of this cube introduced by Siegel in order to compute the integral.
Another method, due to Kitaoka, uses the decomposition of g into a cusp form and Klingen Eisenstein series. It gives a similar result with a better exponent at the minimum if $m > 4n + 4$ and A is even unimodular.

Representation of binaries by quaternaries

In a lecture I heard this January, P. Michel announced joint work with Einsiedler, Lindenstrauss, Venkatesh:

B a definite quaternion algebra over $\mathbb{Q}$, *M* an ideal of a maximal order in *B*, with reduced norm as quadratic form.

Associated to an integral definite binary quadratic form of fundamental discriminant $-d < 0$ is the class of an ideal *I* in $K = \mathbb{Q}(\sqrt{-d})$, choose *I* integral of minimal norm.

Then:

1. Under GRH there is $c > 0$ such that for all $\delta > 0$ one has: If *I* is locally representable with $c \leq N(I) \leq d^{1/2-\delta}$, then *I* is represented by *M*.
2. Fix a prime *p* splitting *B*. Then GRH can be replaced by the condition that *p* splits in *K* (Linnik's condition).
3. Fix $\delta > 0$, for each *d* satisfying Linnik's condition let S_d be a set of size d^δ of ideals *I* of discriminant $-d$. Then for large enough *d* at least one $I \in S_d$ is represented by *M*.

The proof uses ergodic theory.

Representation of binaries by quaternaries, analytic

Theorem (S-P, 2012)

Let M be a positive definite lattice of rank 4*, prime level p and discriminant* p^2*.*
For a certain explicit constant K depending on p and for all $\kappa < 1$ *there is a constant* $c > 0$ *depending on* κ *and p such that the number of binary lattices N of "eligible" fundamental discriminant* $-d$*,* $d > c$*, which are represented by M is* $\geq K\kappa h(-d)$*.*
In particular, for large enough d a positive proportion of the binaries of "eligible" discriminant $-d$ *is represented by M.*

A version of this is true for square free level, hopefully even more general.

The proof uses a connection between averages of numbers of representations of binaries of fixed discriminant $-d$ by *M* and representations of *d* by a pair of ternary lattices associated to the left and right orders of the corresponding quaternionic ideal (Böcherer/S-P 1992).