Math 272y: Rational Lattices and their Theta Functions

4 September 2019: Overview of Math 272

Math 272y is a "graduate topics course"; here our main topic is *quadratic forms* $Q : \mathbf{Z}^n \to \mathbf{Q}$ (often specifically $Q : \mathbf{Z}^n \to \mathbf{Z}$, sometimes allowing $Q : \mathbf{Z}^n \to \mathbf{R}$). For example:

(i) $Q(\mathbf{x}) = x_1^2$;

(ii) $Q(\mathbf{x}) = x_1^2 + \cdots + x_n^2$, the restriction to $\mathbf{Z}^n$ of the standard quadratic form on $\mathbf{R}^n$;

(iii) $n = 2$ and $Q(\mathbf{x}) = 2x_1x_2$ (the "hyperbolic plane" form);

(iv) $Q(\mathbf{x}) = x_1^2 - x_1x_2 + x_2^2$ (the "A_2" form, within a factor of 2).

Any quadratic form Q on $\mathbf{Z}^n$ can be written uniquely as

$$Q(\mathbf{x}) = \mathbf{x}^{\mathsf{T}} A \mathbf{x}$$

for some symmetric $n \times n$ matrix A (the *Gram matrix* of Q). Here $\mathbf{x}$ is regarded as a *column* vector (so that matrices can act on vectors from the left) and $\mathbf{x}^{\mathsf{T}}$ is its transpose (same entries forming a row vector). In our examples above, for (i) the Gram matrix has $(1,1)$ entry 1 and all other entries zero; for (ii), A is the identity matrix I_n; for (iii), $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; and for (iv), $A = \frac{1}{2}\left(\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right)$.

We shall freely switch among three equivalent pictures:

- the quadratic form Q;
- the symmetric bilinear form $B : \mathbf{Z}^n \times \mathbf{Z}^n \to \mathbf{R}$ such that $B(\mathbf{x}, \mathbf{x}) = Q(\mathbf{x})$ for all $\mathbf{x}$, namely

  $$B(\mathbf{x}, \mathbf{y}) = \mathbf{x}^{\mathsf{T}} A \mathbf{y} = \frac{1}{2}\Big(Q(\mathbf{x}+\mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})\Big);$$

  and
- a real vector space V of dimension $n < \infty$ together with a quadratic form $Q : V \times V \to \mathbf{R}$ and an additive subgroup $L \subset V$ of rank n that spans V (paradigmatically $V = \mathbf{R}^n$ and $L = \mathbf{Z}^n$).

In this last picture L is a *lattice* in V. If the bilinear pairing (extended linearly to V) is positive-definite, so L is a lattice in a finite-dimensional Euclidean space; that will be our main topic (though we will sometimes need or want to allow also indefinite or degenerate quadratic forms). In our above four examples, (ii) and (iv) are positive-definite, and L is respectively the (hyper)cubic lattice and the hexagonal (a.k.a. triangular) lattice in $\mathbf{R}^2$. The form in (iii) is indefinite, and the form in (i) is positive semidefinite but degenerate (except when $n = 1$ when it is a special case of (ii)).

Why do we care?

Quadratic forms on $\mathbf{Z}^n$ originate in number theory, but turn out to be one of those core mathematical structures (such as Fourier analysis and the representation theory of finite groups and Lie groups) that they arise naturally in many mathematical contexts and fields. The following list is not exhaustive.

- **Number theory, algebra**: numerous places, starting with the classical n-square problem: Which numbers are the sum of n squares, and in how many ways? (Theorems of Fermat, Legendre, Lagrange, Jacobi, etc.) That is, which integers are $Q(\mathbf{x})$ for some $\mathbf{x} \in \mathbf{Z}^n$? Analogous theorems for other lattices, such as the A_2 lattice introduced above. Also a basic tool of computational number theory via lattice reduction algorithms such as LLL.
- **Algebraic topology**: pairings on (co)homology groups $H_k(X, \mathbf{Z})$ and $H^k(X, \mathbf{Z})$, when k is even (so the pairing is symmetric) and $2k = \dim X$ (so H_{2k} or H^{2k} is canonically identified with $\mathbf{Z}$; here X is a compact manifold). Indeed some of the fundamental theorems on quadratic forms answer questions that first arose in algebraic topology, and were obtained by topologists, not number theorists.
- **Algebraic geometry**, via intersection theory, e.g. $\mathrm{NS}(X)$ when X is an algebraic surface (if $X/\mathbf{C}$ then this is contained in the $k = 2$ case of the "algebraic topology" item).
- **Group theory**: for example, about half of the sporadic finite simple groups are contained in the Conway group $Co_1 = \mathrm{Aut}(\Lambda)/\{\pm 1\}$ where Λ is the Leech lattice (see e.g. the extensive entry for Co_1 in the ATLAS of Conway et al.), and the structure of several of the larger sporadics, including the Monster, is intimately connected with the geometry of Λ. See also B.H. Gross's article "Group representtations and lattices" (*J. AMS* **3** #4 (Oct. 1990), 929–960).
- **Real world$^{\text{TM}}$ applications** of positive-definite lattices, some going well beyond the visible applications in crystallography etc. for $n \leq 3$; for instance, signal processing (the Leech lattice was worth millions of dollars to AT&T — it's no accident that N.J.A. Sloane worked in Bell Labs for many years), numerical integration in high dimensions, and cryptography.
- **etc.**, e.g. Milnor's first example of isospectral manifolds used a pair of lattices in $\mathbf{R}^{16}$ with the same theta series. (The minimal dimension for such a pair is now known to be 4; the last step of the proof was obtained only in 1997 (Schiemann, *Math. Ann.* **308**, 507–517)).

Equivalence and classification of quadratic forms

A basic difficulty is that the Gram matrix A is not canonical, because there are many choices of basis for $\mathbf{Z}^n$. Matrices A, A' yield isomorphic lattices iff $A' = M^{\mathsf{T}} A M$ for some matrix $M \in \mathrm{GL}_n(\mathbf{Z})$ [i.e. $M \in \mathrm{Mat}_{n \times n}(\mathbf{Z})$ with $\det M = \pm 1$]. For large enough n it is computationally intractable to decide whether such M exists for two given matrices A, A', and if so to exhibit one M, at least if A, A' are positive-definite. Easy invariants: signature (Sylvester's "law of inertia"); the discriminant $\det A$ (canonical because $(\det M)^2 = 1$). But if A, A' are positive-definite with the same discriminant (and matching local invariants) the problem can still be hard.

A closely related problem is the *classification* of positive-definite forms with given rank and discriminant. Key example: positive-definite forms with $\operatorname{disc} A = 1$ and $A \in \mathrm{Mat}_{n\times n}\mathbf{Z}$, up to equivalence:

n	1	2	3	$\cdots$	7	8	$9, 10, 11$	12	$\cdots$	24	$\cdots$
L	$\mathbf{Z}$	$\mathbf{Z}^2$	$\mathbf{Z}^3$	$\cdots$	$\mathbf{Z}^7$	$\mathbf{Z}^8, E_8$	$\mathbf{Z}^n, \mathbf{Z}^{n-8} \oplus E_8$	$\mathbf{Z}^{12}, \mathbf{Z}^4 \oplus E_8, D_{12}^+$	$\cdots$	(297)	$\cdots$

Here E_8 is the quadratic form

$$Q(\mathbf{x}) = 2\Big(\sum_{j=1}^{8} x_j^2 - \sum_{j=1}^{6} x_j x_{j+1} - x_5 x_8\Big)$$

(an important quadratic form for which we shall give many other descriptions, constructions, and characterizations during this course). This is an *even* quadratic form, i.e. an integral form for which the homomorphism $\mathbf{Z}^n \to \mathbf{Z}/2\mathbf{Z}$, $\mathbf{x} \mapsto Q(\mathbf{x}) \bmod 2$ is the zero map. We shall see that a positive-definite even form on $\mathbf{Z}^n$ with discriminant-1 exists if and only if $n \equiv 0 \bmod 8$.

In general a quadratic form of discriminant ±1 is said to be "unimodular". The entry "(297)" in the above table indicates 297 inequivalent unimodular forms; these are tabulated in SPLAG[1], chapters 17 (by Borcherds) and 18 (by Venkov). The counts (Sequence A005134 in the OEIS,[2] from SPLAG p.49) are:

n	$1 \cdots 7$	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
#	$1 \cdots 1$	2	2	2	2	3	3	4	5	8	9	13	16	28	40	68	117	297	665
$\#_e$		1								2								24	

The "$\#_e$" line gives the count of even lattices when they exist. The two even unimodular lattices for $n = 16$ are $E_8^2 = E_8 \oplus E_8$ and D_{16}^+. The 24 even unimodulars for $n = 24$ (which include the Leech lattice) are the *Niemeier lattices*, whose classification will be one of our main results and then a key tool for other classification problems such as the $n < 24$ entries in the above table and similar problems such as describing all even definite lattices of rank 18 and discriminant 3 (there are six, corresponding to the six elliptic fibrations of the "singular K3 surface" $y^2 + (t^2 - t)^2 y = x^3$). That's about as far as one can hope to go in this direction, because the counts increase too quickly: it is known (see e.g. SPLAG p.50) that already for $n = 32$ just the number of even unimodular lattices already exceeds $8 \cdot 10^7$. But we shall see that there is still much to say even for considerably larger dimensions, even if it there is no hope for a full classification.

Theta functions

Our main tool (beyond elementary algebraic considerations), and the second part of the course title, are *theta functions* attached to positive-definite quadratic forms. These are generating functions that encode the distribution of lattice points. If L is the lattice corresponding to the positive-definite quadratic form Q, the generating function for the counts $N_m(L) = \#\{\mathbf{x} : Q(\mathbf{x}) = m\}$

---

[1] SPLAG = *Sphere Packings, Lattices, and Groups* by J.H. Conway and N.J.A. Sloane. This is an essential reference work for our topic and related areas; it might have been disrespectful to use an acronym such as "SPLAG" for this book, except that the authors themselves call it that. SPLAG will be our main source; we shall also refer often to Serre's *A Course in Arithmetic*, Chapters I–V and VII (which is all but Chapter VI, since that chapter concerns Dirichlet's theorem on primes in arithmetic progressions).

[2] OEIS = https://oeis.org = The On-Line Encyclopedia of Integer Sequences. For example, Sequence A005134 is https://oeis.org/A005134 .

is

$$\Theta_L(q) = \sum_{m \geq 0} N_m(L) q^{m/2} = \sum_{\mathbf{x} \in \mathbf{Z}^n} q^{\frac{1}{2}Q(\mathbf{x})} = 1 + \kappa_Q q^{\frac{1}{2}\min_L} + \cdots.$$

Here $\min_L$ is the *minimal (nonzero) norm* $\min\{Q(\mathbf{x}) : \mathbf{x} \in \mathbf{Z}^n,\ \mathbf{x} \neq 0\}$, and $\kappa_Q = N_{\min_L}(L)$, the *kissing number* of L, is the number of vectors attaining this minimum (so called because it is the number of balls touching any given ball in the sphere packing associated to L). The factor of $\frac{1}{2}$ in the exponent turns out to be a convenient normalization (as you might already expect from the special role of even lattices). The series converges absolutely for $q < 1$. The remarkable and fruitful fact is that if Q has rational coefficients then Θ_L becomes a *modular form* $\theta_L(z)$ of weight $n/2$ under the transformation $q = e^{2\pi i z}$ (which also lets us make sense of $\theta_L(q)$ as a function of a complex variable in the upper half-plane $z \in \{x + iy \in \mathbf{C} : y > 0\}$). The nicest and best-known case (see e.g. Chapter VII of Serre's *A Course in Arithmetic*) is when L is an even unimodular lattice, in which case Θ_L is a modular form for the full modular group $\mathrm{PSL}_2(\mathbf{Z})$. This, together with the fact that $N_0(L) = 1$, gives very precise information about the counts $N_m(L)$. For example $N_m(E_8) = 240 \sum_{d|m} d^3$ for all $m \geq 1$; and if L is any even unimodular lattice of rank 16 then $N_m(L) = 480 \sum_{d|m} d^7$ for all $m \geq 1$. There are two such lattices; the coincidence between their counts $N_m(L)$ was noted by Witt, and used by Milnor to give the first example of isospectral manifolds. Going one step further, if L is any even unimodular lattice of rank 24 each $N_m(L)$ is a linear polynomial in $N_2(L)$, namely $N_4(L) = 196560 - 24N_2(L)$, $N_6(L) = 16773120 + 252N_2(L)$, "etc." (in general $N_{2m}(L) = N_{2m}(\Lambda) + \tau(m)N_2(L)$ where Λ is the Leech lattice and τ is the Ramanujan tau function). We shall obtain similar formulas for rank 32 and 40 even though the classification problem for such L is surely hopeless.

The theta function Θ_L encodes the radial distribution of lattice vectors. We shall also use "weighted theta functions" $\theta_{L,P}$ to study those vectors' angular distribution, meaning the distribution of the norm-m lattice vectors on the sphere $Q(\mathbf{x}) = m$. We expect that for each Q those vectors should be asymptotically equidistributed as $m \to \infty$; we shall prove it for lattices of sufficiently large rank, say $n > 4$ and also some instances of $n \leq 4$.[3] Here P is a "spherical polynomial", i.e., a homogeneous polynomial of some degree d that is in the kernel of the laplacian $\Delta : \mathcal{P}_d \to \mathcal{P}_{d-2}$, e.g. $x_j^2 - x_k^2$ or $x_j x_k$ for distinct indices j, k of orthonormal coordinates on $\mathbf{R}^n$. The weighted theta function $\Theta_{L,P}$ is defined by

$$\Theta_{L,P}(q) = \sum_{\mathbf{x} \in L} P(\mathbf{x}) q^{\frac{1}{2}Q(\mathbf{x})},$$

and we shall show that this is a modular form of weight $(n/2) + d$.[4] We shall also use this to get some exact equidistribution results. Notably, each shell of the E_8 lattice is a "spherical 7-design": for each even integer $m \geq 2$ and any polynomial P of degree at most 7, the average of P over the lattice vectors of norm m exactly equals the integral of P over the sphere $Q(\mathbf{x}) = m$. Even more notably, each shell of the Leech lattice is a spherical 11-design.

---

[3] One indication of the difficulty of the problem for $n \leq 4$ is that equidistribution may fail for some natural L and m; even for the sum-of-four-squares form $Q(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, asymptotic equidistribution must fail for $m = 2^k$ because there are only 8 representations.

[4] Here d might as well be even, because $\Theta_{L,P} = 0$ for P homogeneous of odd degree; but we shall also consider theta functions of rational lattice translates, for which odd-degree P can be of use too.

Plan for the course

- Basic definitions, constructions, and properties of lattices
- Theta functions, their properties, and uses
- Spherical harmonics and weighted thetas
- Applications to classications of structure of positive-definite lattices
- Further connections, e.g. error-correcting codes and their weight enumerators and design properties

Sources

We already mentioned two key sources: Serre's *A Course in Arithmetic* I–V and VII, and Conway and Sloane's *Sphere Packings, Lattices, and Groups*. You might also have a look at my "Lattices, Linear Codes, and Invariants, Part I" (*Notices of the American Math. Society* **47** *(2000), 1238–1245*) for an introduction to my take on this area. Beyond those, there will be a few pages of lecture notes (including references to further relevant literature) for each lecture.

Further directions

The introductory lecture concluded with some sample topics of final papers for students who need a letter grade for Math 272. Even if there are none (i.e. even if everybody who is officially taking the class is a graduate student eligible for an EXCused grade), this list can still be used for further directions of study and research.

- Further classifications of definite lattices; mass formulas; lattice algorithms
- Variants of $\mathbf{Z}$-lattices, such as lattices over $\mathbf{Z}[i]$, $\mathbf{Z}[e^{2\pi i/3}]$, or the Hurwitz quaternions
- Higher (Siegel) theta functions

  $$\sum_{\mathbf{x}_1,\ldots,\mathbf{x}_g \in L} \left[\prod_{1\leq j\leq k\leq g} q_{jk}^{\frac{1}{2}\langle \mathbf{x}_j,\mathbf{x}_k\rangle} \right]$$

  (for $q_{jk} = \exp(2\pi i z_{jk})$ with $(q_{jk})_{1\leq j\leq k\leq g}$ in the "Siegel upper half-space" of complex dimension $(g^2+g)/2$). These encode the relative positions of g-tuples of lattice vectors.
- Sphere-packing bounds (Cohn-NDE, Cohn-Kumar, Viazovska et al.)
- Connections and analogies with error-correcting codes