Journées mathématiques X-UPS

Année 1993

Codes géométriques algébriques et arithmétique sur les corps finis

Michael A. Tsfasman

Algebraic curves and sphere packings

Journées mathématiques X-UPS (1993), p. 11-43.
https://doi.org/10.5802/xups.1993-02

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Journées mathématiques X-UPS
1993, p. 11–43 doi: 10.5802/xups.1993-02

ALGEBRAIC CURVES AND SPHERE PACKINGS

by

Michael A. Tsfasman

Contents

This talk is mostly devoted to problems which resemble greatly questions about codes, namely to quite a classical problem of dense packing of equal non-overlapping spheres in $\mathbb{R}^N$. It comes out that both direct application of algebraic-geometric codes and use of intuition developed while studying them are quite useful. Moreover, here one can see even better the marvelous integrity of mathematics, two more parts of which — number theory and that of packings — being added to coding theory and algebraic geometry.

In the first chapter we give necessary definitions and produce some beautiful examples. This chapter is quite classical and has nothing to do with either algebraic geometry or number theory.

Publication originelle dans Journées X-UPS 1993. Codes géométriques algébriques et arithmétique sur les corps finis. Prépublication du Centre de mathématique de l'École polytechnique, 1993.

The relations with the latter are discussed in the second chapter devoted to algebraic geometry and number theory constructions of lattices and packings.

Part I. Definitions and examples

How can one pack equal non-overlapping spheres in $\mathbb{R}^N$? What is the density of such packing and how the density behaves for small values of N? For large values of N? How to put the asymptotic problem for $N \to \infty$?

In §1 we give some basic definitions and introduce different parameters of sphere packings. Then we show how to put the problem rigorously. In §2 we give some examples of dense packings. Then, in §3 we discuss the asymptotic setting. The striking similarity between codes and packings is briefly discussed in §4.

1. Parameters

Packings. Let us consider the classical problem of *packing* equal non-overlapping spheres in $\mathbb{R}^N$. Let P be the set of centers and let

$$d = d(P) = \inf_{\substack{v,u \in L \\ v \neq u}} |u - v|,$$

d is the *minimum distance* of the packing, which equals the maximum possible diameter of non-overlapping spheres centered in P.

The *density* of P is the part of $\mathbb{R}^N$ covered by spheres; to be precise, it can be defined as

$$\Delta(P) = \limsup_{u \to \infty} v(S \cap B_u)/v(B_u),$$

where

$$\begin{aligned} S &= \left\{ x \in \mathbb{R}^N \;\middle|\; \exists y \in P,\ |x - y| < \frac{d}{2} \right\} \\ B_u &= \left\{ x \in \mathbb{R}^N \;\middle|\; |x| \leqslant u \right\} \end{aligned}$$

and $v(\cdot)$ is the standard volume in $\mathbb{R}^N$.

Lattices. If P is an additive subgroup of $\mathbb{R}^N$, we call the packing P a *lattice packing* (or just a *lattice*; in this case we use the letter L rather than P). Further on we suppose that the rank of L equals N since otherwise $\Delta(L) = 0$. If L is a lattice then any choice of a basis $e_1, \ldots, e_N$ in L defines a map $\mathbb{Z}^N \to \mathbb{R}^N$; its matrix is called a *generator matrix* of the lattice.

For lattices the definition of $\Delta(L)$ does not depend on the choice of origin and does not change if we replace the ball B_u by a cube (or by any homothetically increasing solid containing a neighbourhood of the origin).

The volume of the fundamental domain

$$F = \left\{ \sum_{i=1}^{N} x_i e_i \;\middle|\; 0 \leqslant x_i < 1 \right\} \subset \mathbb{R}^N$$

equals the absolute value of the determinant of the generator matrix. This volume is called the *determinant* of the lattice and is denoted by $\det(L)$; we define the discriminant $\operatorname{discr}(L)$ of L as the determinant of the matrix of inner products $\|(e_i, e_j)\|$, $i, j = 1, \ldots, N$. It is easy to check that

$$\operatorname{discr} L = (\det L)^2.$$

Let $V_N = \pi^{N/2}/\Gamma(N/2+1)$ be the volume of unit ball in $\mathbb{R}^N$.

For a lattice there is exactly one sphere in each fundamental domain, or — to be more precise — the pieces of spheres in the fundamental domain, being shifted, form just one sphere. Therefore

$$\Delta(L) = \frac{d(L)^N V_N}{2^N \det L}.$$

Note that by the Stirling formula we have

$$\log_2 V_N = \frac{N}{2} \cdot \log_2 \left(\frac{2\pi e}{N} \right) - \log_2 \sqrt{\pi \cdot N} + o(1);$$

we write this as

$$\frac{1}{N} \cdot \log_2 V_N \sim \frac{1}{2} \cdot \log_2 \left(2\pi e/N \right).$$

Thus for $N \to \infty$ we get

$$-\frac{1}{N} \cdot \log_2 \Delta(L) \sim -\log_2 \sqrt{\frac{\pi \cdot e}{2}} + \log_2 \sqrt{N} - \log_2 d(L) + \frac{1}{N} \cdot \log_2 (\det L).$$

Other parameters. Let us define some other parameters of packings (which are often more convenient than Δ) setting

$$\begin{aligned}\delta(P) &= \Delta(P)/V_N,\\ \lambda(P) &= -(\log_2 \Delta(P))/N,\\ \nu(P) &= \log_2 \delta(P);\end{aligned}$$

we call $\delta(P)$ the *center density*, and $\lambda(P)$ the *density exponent*. Clearly,

$$\Delta(P) = 2^{-\lambda(P)\cdot N}.$$

For root lattices it is convenient to use $\delta(P); \nu(P)$ is useful to compute the density of lattices obtained by some specific constructions. The density exponent $\lambda(P)$ is especially important for asymptotic problems.

Densest packings. Set

$$\lambda(N) = \inf_{P\subset\mathbb{R}^N} \lambda(P), \quad \Delta(N) = \sup_{P\subset\mathbb{R}^N} \Delta(P), \dots$$

A natural problem of finding the densest possible packing in a given dimension can be decomposed into two problems:

(A) Find the precise value of $\lambda(N)$ (or, what is the same, of $\Delta(N)$ or of $\delta(N), \dots$).

(B) Find a packing P with $\lambda(P) = \lambda(N)$.

These problems are completely solved only for $N = 1$ and $N = 2$.

Since $\Delta(P) \leqslant 1$, we get

$$\lambda(P) \geqslant 0$$

for any packing.

For $N = 1$ the answer is obvious: equal segments cover the whole line, and hence for this packing L_1 one has $\Delta(L_1) = 1$, i.e.,

$$\Delta(1) = 1, \quad \lambda(1) = 0.$$

For $N = 2$ the problem is not so simple but one can prove that

$$\Delta(2) = \pi/2\sqrt{3}.$$

It is easy to check that for the lattice $L_2 \subset \mathbb{R}^2 = \mathbb{C}$ generated by 1 and $(1+\sqrt{-3})/2$ we have $\Delta(L_2) = \Delta(2); L_2$ is called the *hexagonal* lattice.

Strangely enough, $\lambda(N)$ is unknown for any $N \geqslant 3$.

The figures 1, 2, 3 show the densest known packings in dimensions 1, 2, and 3.

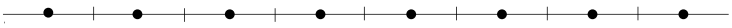

Figure 1. : dim $= 1$, $\Delta = 1$

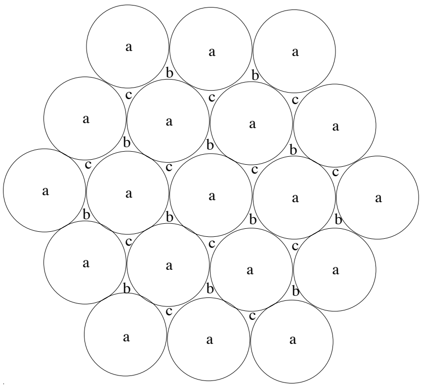

Figure 2. dim $= 2$, $\Delta = \dfrac{\pi}{\sqrt{12}} = 0.9069\cdots$

In fact, the packing in dimension 2 is obtained by taking a line, putting spheres of dimension two at the centers of the best packing in dimension one along this line, then taking a similar row next to it as close as possible, then another row, and so on. It can be shown that it is essentially unique.

We can do the same in dimension three. Take a plane, put three-dimensional spheres at the centers "a" of the best two-dimensional packing. Then we have to choose the next layer. It can be centered either over "b" points, or over "c" points. Continuing like this we

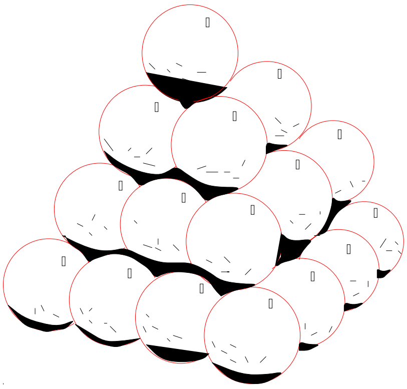

Figure 3. $\dim = 3$, $\Delta = \dfrac{\pi}{\sqrt{18}} = 0.7405\cdots$

have continually many choices corresponding to binary sequences, the density being the same. One of these choices gives the lattice packing you see on the figure.

It is conjectured that this packing is the densest possible. Recently a proof has been announced, but as yet the mathematical community does not believe in it.

Densest lattices. For lattice packings we know slightly more. Let

$$\lambda_\ell(N) = \inf_{L\subset\mathbb{R}^N} \lambda(L), \quad \Delta_\ell(N) = \sup_{L\subset\mathbb{R}^N} \Delta(L), \dots$$

Clearly

$$\lambda_\ell(N) \geqslant \lambda(N), \quad \Delta_\ell(N) \leqslant \Delta(N), \dots$$

A lattice L is called *unimodular* iff $\det L = 1$. The *dual lattice*

$$L^\perp = \left\{x \in \mathbb{R}^N \;\middle|\; (x,\ell) \in \mathbb{Z} \quad \text{for any} \quad \ell \in L\right\}$$

is in this case also unimodular.

The inner product in $\mathbb{R}^N$ induces on L a positively definite bilinear form.

In fact, any integral positively definite bilinear form can be obtained from a lattice.

Let now $\varphi(x,y)$ be a positively definite bilinear form in N integral variables, and let $f(x) = \varphi(x,x)$ be the corresponding quadratic form.

Suppose that φ is unimodular, i.e., $\operatorname{discr}\varphi = 1$. Such forms are in bijection with unimodular lattices L in $\mathbb{R}^N$. Set

$$\gamma(L) = \gamma(\varphi) = \min_{x \in \mathbb{Z}^N - \{0\}} f(x).$$

In lattice terms it is the squared length of the shortest non-zero vector. It is easy to check that

$$\begin{aligned} \Delta(L) &= V_N \cdot (\gamma(L)/4)^{N/2}\,; \\ \gamma(L) &= 4 \cdot (\Delta(L)/V_N)^{2/N} = 4 \cdot (\delta(L))^{2/N}. \end{aligned}$$

One can naturally extend the definition of $\gamma(\varphi)$ to non-unimodular case:

$$\gamma(L) = \gamma(\varphi) = \min_{x \in \mathbb{Z}^N - \{0\}} (f(x)/\operatorname{discr}\varphi)^{1/N}\,.$$

Now let us put

$$\gamma(N) = \max_{\varphi} \gamma(\varphi),$$

where maximum is taken over all positively definite bilinear forms in N variables; $\gamma(N)$ and $\Delta_\ell(N)$ are related by formulas similar to those given above.

Note that for $N \to \infty$ we obtain

$$\lambda(N) \sim \log_2 \sqrt{\frac{2N}{\pi \cdot e \cdot \gamma(N)}},$$

$$\log_2(\gamma(N)) \sim \log_2 \left((2N/\pi e) \cdot \Delta^{2/N} \right) = -2 \cdot \lambda(N) + \log_2 (2N/\pi e)\,.$$

Precise values of $\Delta_\ell(N)$ are known for $1 \leqslant N \leqslant 8$; see the table where we have collected the values of all the above parameters for these N.

N	1	2	3	4	5	6	7	8
$\Delta_\ell(N)$	1	0.907	0.740	0.617	0.465	0.373	0.295	0.254
$\delta_\ell(N)$	0.5	0.229	0.177	0.125	0.088	0.072	0.063	0.063
$\lambda_\ell(N)$	0	0.070	0.144	0.174	0.221	0.237	0.251	0.247
$\nu_\ell(N)$	-1	-1.792	-2.5	-3	-3.5	3.792	-4	-4
$\gamma_\ell(N)$	1	1.155	1.260	1.414	1.516	1.665	1.811	2
$\delta_\ell(N)^{-2}$	4	12	32	64	128	192	256	256

Note that within the table $\Delta_\ell(N)$ increases and $\gamma_\ell(N)$ decreases. It is interesting to know whether it is the case for any N.

In the table the integrality of $\delta_\ell(N)^{-2}$ attracts attention. We do not know whether $\delta_\ell(N)^{-2}$ is integral for any N; note however that the densest lattice of a given rank can be generated by a matrix with rational entries and the rationality of $\delta_\ell(N)^{-2}$ follows.

2. Examples

Now we describe the densest lattices for $N \leqslant 8$ and introduce some interesting lattice families.

We construct families $L \subset \mathbb{R}^N$ and give the values of $d(L)$ and $\det(L)$. Other density parameters for these families are given in the table above.

The simplest family is

$$\mathbb{Z}^N \subset \mathbb{R}^N;$$

for these lattices

$$d(\mathbb{Z}^N) = 1, \quad \det(\mathbb{Z}^N) = 1.$$

Root lattices. Let us consider in $\mathbb{R}^{N+1}$ the following lattice A_N of rank N:

$$A_N = \left\{ \sum_{i=1}^{N+1} a_i e_i \;\middle|\; a_i \in \mathbb{Z}, \sum a_i = 0 \right\},$$

$\{e_i\}$ being the standard basis in $\mathbb{R}^{N+1}$.

The lattice A_N is generated by vectors

$$\alpha_1 = e_1 - e_2,\, \alpha_2 = e_2 - e_3, \ldots,\, \alpha_N = e_N - e_{N+1};$$

its parameters are

$$d(A_N) = \sqrt{2}, \quad \det(A_N) = \sqrt{N+1}.$$

The family $D_N \subset \mathbb{R}^N$ is defined by

$$D_N = \left\{ \sum_{i=1}^{N} a_i e_i \;\middle|\; a_i \in \mathbb{Z},\ \sum a_i \equiv 0 \bmod 2 \right\}.$$

The lattice D_N is generated by $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3$,$\ldots$, $\alpha_{N-1} = e_{N-1} - e_N$, and $\alpha_N = e_{N-1} + e_N$; its parameters are

$$d(D_N) = \sqrt{2}, \quad \det(D_N) = 2.$$

The following important family does exist only for $N = 4, 5, 6, 7, 8$. For such N define the lattice E_N in $\mathbb{R}^8$ by its basis:

$$\begin{aligned} \alpha_1 &= \frac{1}{2}(e_1 + e_8) - \frac{1}{2} \cdot (e_2 + \cdots + e_7), \\ \alpha_2 &= e_1 + e_2, \\ \alpha_i &= e_i - e_{i-1} \qquad \text{for} \quad i = 3, \ldots, N. \end{aligned}$$

The lattice E_8 can be given by

$$E_8 = \left\{ \sum_{i=1}^{8} a_i \cdot e_i \;\middle|\; 2 \cdot a_i \in \mathbb{Z},\ a_i - a_j \in \mathbb{Z},\ \sum_{i=1}^{8} a_i \in 2 \cdot \mathbb{Z} \right\};$$

and the rest E_N are intersections of E_8 with planes of codimension $(8-N)$. In particular,

$$E_7 = \left\{ x = \sum_{i=1}^{8} a_i \cdot e_i \;\middle|\; x \in E_8,\ a_7 = -a_8 \right\},$$

$$E_6 = \left\{ x = \sum_{i=1}^{8} a_i \cdot e_i \;\middle|\; x \in E_7,\ a_6 = -a_7 \right\}.$$

The parameters are $d(E_N) = \sqrt{2}$ and $\det(E_N) = 9 - N$.

Note that $A_1 = \mathbb{Z}, D_3 = A_3, E_4 = A_4, E_5 = D_5$. The lattice families A, D, and E are root lattices which arise in many questions: in the theory of Lie groups and algebras, in the singularity theory, in the theory of rational surfaces, etc.

Lattices Γ. Let now $N \geqslant 8, N \equiv 0 \bmod 4$. Set

$$\Gamma_N = \left\{ \sum_{i=1}^{N} a_i \cdot e_i \;\middle|\; 2 \cdot a_i \in \mathbb{Z},\ a_i - a_j \in \mathbb{Z},\ \sum_{i=1}^{N} a_i \in 2\mathbb{Z} \right\}.$$

The lattice Γ_N is generated by vectors $e_i + e_j$ and the vector $\frac{1}{2}\sum_{i=1}^{N} e_i$; its parameters are

$$d(\Gamma_N) \geqslant \sqrt{2}, \quad \det(\Gamma_N) = 1.$$

Note that $\Gamma_8 = E_8$.

The lattices $A_1 = \mathbb{Z}, A_2, A_3 = D_3, D_4, D_5, E_6, E_7, E_8 = \Gamma_8$ have the density coinciding with that from the table. They are the densest lattices in their dimensions. A proof of this fact can be obtained by the reduction theory of quadratic forms.

Note that for all the described families

$$\lambda(L_N) \sim \log_2 \sqrt{N} \longrightarrow \infty \quad \text{for} \quad N \longrightarrow \infty.$$

We shall see that there are lattices which asymptotically behave significantly better.

For $N \geqslant 9$ we do not know the precise value of $\lambda_\ell(N)$ and only some bounds are known. As in the case of codes it is natural to call upper bounds for $\Delta(N)$ and $\Delta_\ell(N)$ *possibility bounds* and lower ones *existence bounds* (note however that for $\lambda(N)$ possibility bounds are lower ones, and existence bounds are upper ones).

We do not describe here various methods of constructing dense packings in dimensions from 9 up to 100000. We need here only the Leech lattice which is a very beautiful object arising in many questions.

Leech lattice. There exists a unique integral even unimodular lattice of dimension 24 which has no vector of length $\sqrt{2}$ (recall that a lattice is called *even* iff the scalar square of any of its vectors is even). This lattice is called *Leech lattice* and is denoted by Λ_{24}; it is closely connected with Golay $[24, 12, 8]_2$-code C_{24}. It can be constructed in many ways. Here is one of the simplest.

The lattice Λ_{24} is generated by vectors

$$V_{i,c} = \frac{1}{\sqrt{8}} \cdot u_{i,c}, \quad 1 \leqslant i \leqslant 24,\ c \in C_{24},$$

where $u_{i,c}$ has ∓ 3 in i-th position and ± 1 in all other positions, and the upper sign is chosen for a position where the codeword c has 1.

The parameters of the Leech lattice are

$$\det(\Lambda_{24}) = 1, \quad d(\Lambda_{24}) = 2;$$

therefore,

$$\begin{gathered} \delta(\Lambda_{24}) = 1,\ \nu(\Lambda_{24}) = 0,\ \gamma(\Lambda_{24}) = 4, \\ \Delta(\Lambda_{24}) \approx 0.00193 \quad \text{and} \quad \lambda(\Lambda_{24}) \approx 0.376. \end{gathered}$$

The covering radius of the Leech lattice equals $2\sqrt{2}$, i.e., balls of radius $2\sqrt{2}$ centered at lattice points cover the whole space $\mathbb{R}^{24}$. One can describe "deep holes" of the Leech lattice, i.e., points with distance $2\sqrt{2}$ from the nearest lattice point.

The automorphism group Co_0 of the Leech lattice is enormous:

$$|Co_0| = 8315553613086720000.$$

The maximal sporadic simple group, the Fischer-Gries group (the Monster), can be realized as the automorphism group of an algebra closely connected to the Leech lattice.

Kissing number. There is another nice problem concerning sphere packings, of slightly a different nature (local). How many spheres can touch the given sphere in an N-dimensional space (all spheres being equal)? This number is called the *kissing number.*

The answer is known only in dimensions 1, 2, 3, 8, and 24, the kissing numbers being respectively 2, 6, 12, 240, and 196560. The examples are given by local arrangements in the lattices A_1, A_2, A_3, D_4, E_8, and Λ_{24}.

3. Asymptotic problems

For asymptotic problems it is convenient to consider

$$\widetilde{\lambda} = \liminf_{N\to\infty} \lambda(N).$$

To compute $\widetilde{\lambda}$, i.e., to understand what is the maximum asymptotic density $\widetilde{\Delta} = 2^{-\widetilde{\lambda}N}$ of a high-dimensional packing, is most likely a very hard problem. We are interested in bounds for this value. The situation here is similar to that in coding theory, and $\widetilde{\lambda}$ is an analogue of $\alpha_q(\delta)$.

A *family* of packings is a set $\{P_N\}$ of packings, $P^N \subset \mathbb{R}^N$ where N runs over an infinite subset of $\mathbb{N}$.

Let

$$\lambda(\{P_N\}) = \liminf \lambda(P_N).$$

We call families with $\lambda(\{P_N\}) < \infty$ *good families* (they are analogues of good families of codes, i.e., those with $k/n \to R > 0$ and $d/n \to \delta > 0$).

One can show that $\inf\limits_{\{P_N\}} \lambda(\{P_N\}) = \widetilde{\lambda}$.

Similarly for lattices we set

$$\widetilde{\lambda}_\ell = \liminf_{N\to\infty} \lambda_\ell(N) = \inf_{\{L_N\}} \lambda(\{L_N\}).$$

Bounds. Here are the best known estimates of $\widetilde{\lambda}$:

Theorem. $1 \geqslant \widetilde{\lambda}_\ell \geqslant \lambda \geqslant 0.599.$

The upper bound which is an existence bound is called the Minkowski bound, the lower one (a possibility bound) the Kabatyansky-Levenstein bound.

The Kabatyansky-Levenstein bound can be obtained by technique similar to that of the Mc Eliece-Rodemich-Ramsey-Welch bound in coding theory. The proof of the former consists of two parts : the first is the linear programing bound for packing of spheres on $S^N \subset \mathbb{R}^{N+1}$ and the second provides a way to pass from S^N to $\mathbb{R}^N$, which is based on the following simple construction. Let Λ_N be a packing in $\mathbb{R}^N$ and let us embed $\mathbb{R}^N$ into $\mathbb{R}^{N+1}$ in the natural way (i.e., assuming that vectors from $\mathbb{R}^N$ have zero for the last coordinate). Thus $\mathbb{R}^N \cap S^N = S^{N-1}$; let us consider those balls from Λ_N which are contained in the unit $(N-1)$-ball. Lifting their centers to S^N we obtain a packing of S^N and its parameters can be estimated through the parameters of Λ_N.

Here is another bound (Rogers):

Proposition. *$\Delta(N) \leqslant \sigma_N$, where σ_N is the ratio of the volume of the intersection $\left(\bigcup_{i=1}^{N+1} B_i \cap \Sigma_N\right)$ to the volume of Σ_N, where Σ_N is the perfect simplex of edge length 2 and $B_1, \ldots, B_{N+1}$ are unit balls centered at the vertices of Σ_N.*

The Rogers bound gives $\widetilde{\lambda} \geqslant 0.5$ but it is quite useful for moderate values of N.

The Minkowski bound (which is an analogue of the Gilbert-Varshamov bound) can be obtained by a technique similar to the code-theoretic one. As in the case of codes almost all linear codes asymptotically lie on the Gilbert-Varshamov bound, here almost all lattice families have $\lambda(\{L_N\}) = 1$.

Thus it is known that there exists lattices of density $\Delta \sim 2^{-N}$ but we do not know how to construct them explicitly. The problem of explicit construction of dense packings naturally arises.

4. Codes and packings

Between codes and packings there exists a system of beautiful analogies. Indeed, one can consider an $[n,k,d]_q$-code $C \subseteq \mathbb{F}_q^n$ as the set of centers of a sphere packing (of radius $t = [(d-1)/2]$) in the Hamming metric. Minimum distance of a code corresponds to the diameter $d(L)$ of a sphere packing.

Linear codes correspond to lattice packings. Indeed, a linear code is a subset in $\mathbb{F}_q^n$ which is closed under addition and under multiplication by elements of $\mathbb{F}_q$, and lattice is closed under addition and multiplication by integers. Strictly speaking, we can consider "quasi-linear" codes, i.e., subsets which are closed under addition and under multiplication by elements of $\mathbb{F}_p$ (rather than $\mathbb{F}_q$) as an analogue of lattices, but we do not pursue this idea here.

Let C be a linear $[n, k, d]_q$-code. Then the volume (the cardinality) of the factor-space $\mathbb{F}_q^n/C$ equals q^{n-k}. For a lattice $L \subset \mathbb{R}^N$ the volume of the factor-space $\mathbb{R}^N/L$ equals $\det(L)$, i.e., $\log(\det L)$ is an analogue of the code codimension $(n-k)$. To be definite we shall assume that in the expression $\log(\det L)$ the log symbol corresponds to the binary logarithm.

There are two possible analogues of the dimension N of a lattice (which equals its rank): the length n and the dimension k of a code. We use the first one; nevertheless we think that the second can be also of some use.

The density of a packing corresponds to the density of a packing in the Hamming metric. Note that the density of a lattice packing equals the volume of the ball of radius d divided by $\det L$. For the density of a packing in the Hamming metric the analogous statement is also true if we assume the ball volume to be normalized:

$$\text{the ball volume} = (\text{number of points in the ball})/q^n.$$

An analogy between code and lattice parameters is not complete. Indeed, the density of packing does not change under a homothety $L \mapsto a \cdot L$. Hence one can assume that $d(L) = 1$ (or $\det L = 1$) and thus a packing has two essential parameters N and Δ, whence a code has three essential parameters n, k, and d. Thus the unique asymptotic parameter λ is an analogue of the pair of code asymptotic parameters (δ, R).

An asymptotic by good packing family (i.e., with $\lambda < \infty$ for $N \to \infty$) is an analogue of an asymptotically good code family (i.e., with $R \cdot \delta > 0$ for $n \to \infty$).

The Gilbert-Varshamov bound corresponds to the Minkowski bound; and the Hamming bound to the condition $\lambda \geqslant 0$. It is no clear which is a reasonable analogue of the Plotkin bound in coding theory (this is an interesting question). The Kabatyansky-Levenstein bound corresponds to the Mc Elice-Rodemich-Ramsey-Welch bound.

Packings on a sphere correspond to constant-weight codes.

An interesting question about analogies between concrete code families and lattice families is mostly open. For instance, parity check codes correspond either to lattices A_N, or to D_N.

The θ-function of a lattice corresponds to the code enumerator; this analogy is quite useful.

Unimodular lattices correspond to self-dual codes.

We are interested in analogues of algebraic-geometric codes. Below we shall describe some of them. These analogies are closely connected to a very deep analogy between algebraic curves over finite fields and algebraic number fields.

Part II. Curves, number fields and packings

To construct sphere packing starting from curves over finite fields or from algebraic number fields one should first recall the main notions of these two domains. That of curves was already recalled in the previous talks, §1 is devoted to algebraic number theory. We also stress the parallelism between number fields and curves over finite fields.

Then we can give some sphere packing constructions, choosing only those that look both simple, natural and beautiful. Each of then can be used to produce many interesting examples of lattice packing. To show that they are really good we study these packing for N tending to infinity.

1. Algebraic number fields

A finite extension k of $\mathbb{Q}$ is called an algebraic number field. Its degree $n = [k : \mathbb{Q}]$ equals the dimension of k as a $\mathbb{Q}$-vector space.

Algebraic integers. If $x \in k$ satisfies the relation

$$x^m + a_{m-1} \cdot x^{m-1} + \cdots + a_1 \cdot x + a_0 = 0, \quad a_i \in \mathbb{Z}$$

then x is called an algebraic integer or an integral element of k.

Proposition. *The sum and the product of algebraic integers are also algebraic integers.*

Corollary. *The subset of integers of k is a ring.*

This ring O_k is called the ring of integers of k or its maximal order. Any subring $O \subseteq O_k$ of finite index $[O_k : O]$ is called an order.

Proposition. *For any $z \in k$ there exists $c \in \mathbb{Z}$ such that $c \cdot z$ is an algebraic integer.*

Therefore we have

$$O_k = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$$

for some basis $\{w_1, \ldots, w_n\}$ of k over $\mathbb{Q}$: such a basis is called a *fundamental basis* of k.

Trace and norm. Let now $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ be the set of distinct embeddings of k into $\mathbb{C}$. Since for any embedding σ_i such that $\sigma_i(k)$ does not lie in $\mathbb{R}$ the embedding $\overline{\sigma}_i$ does not coincide with σ_i, these embeddings are present in the set Σ in pairs $(\sigma_i, \overline{\sigma}_i)$. Thus if s is the number of embeddings $\sigma_i : k \hookrightarrow \mathbb{C}$ with $\sigma_i(k) \subset \mathbb{R}$ (such embeddings are called real) and t is the number of pairs $(\sigma_i, \overline{\sigma}_i)$ where $\sigma_i \neq \overline{\sigma}_i$ (such embeddings are called complex) then $s + 2t = n$.

Let us set

$$\mathrm{Tr}(x) = \mathrm{Tr}_{k/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x), \quad N(x) = N_{k/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

$\mathrm{Tr}(x)$ is called the $(k/\mathbb{Q})$-*trace* of x, and $N(x)$ the $(k/\mathbb{Q})$-*norm* of x.

If $a_m \cdot x^m + \cdots + a_0 = 0$ is the minimal equation of x over $\mathbb{Q}$ then $m|n$, moreover

$$\mathrm{Tr}(x) = -na_{m-1}/(ma_m) \quad \text{and} \quad N(x) = (-1)^n (a_0/a_m)^{n/m}.$$

The bilinear form $\mathrm{Tr}(x \cdot y)$ is non-degenerate; $N(x) \in \mathbb{Z}$ if and only if $x \in O_k$.

Discriminant. Let k be an algebraic number field of degree n and let $\{w_1, \ldots, w_n\}$ be its fundamental basis. The integer

$$D_k = \det(\mathrm{Tr}(w_i \cdot w_j))$$

is called the (absolute) *discriminant* of k.

It can be checked that this definition does not depend on the choice of $\{w_1, \ldots, w_n\}$.

Theorem. *If* $n > 1$, *i.e.,* $k \neq \mathbb{Q}$, *then* $|D_k| > 1$.

One can give another definition of D_k which follows. Let s be the number of real embeddings σ_i and t be the number of conjugate pairs $(\sigma_j, \overline{\sigma}_j)$ of complex embeddings of k. Let $A = \mathbb{R}^s \times \mathbb{C}^t$ be a commutative $\mathbb{R}$-algebra of rank $n = s + 2t$, and let σ be the following ring embedding

$$\begin{aligned} &k \xrightarrow{\sigma} \mathbb{R}^s \times \mathbb{C}^t, \\ &a \longmapsto (\sigma_1(a), \ldots, \sigma_s(a); \sigma_{s+1}(a), \ldots, \sigma_{s+t}(a)). \end{aligned}$$

The image $\sigma(k)$ generates A (over $\mathbb{R}$); check also that $\sigma(O_k)$ is a lattice in $A \simeq \mathbb{R}^n$.

The following proposition will be used later.

Proposition. $|\det \sigma(O_k)| = 2^{-t} \cdot \sqrt{|D_k|}$.

Proof. Let $\{w_1, \ldots w_n\}$ be a fundamental basis of k, let $\sigma_j(w_i) = x_{ji} \in \mathbb{R}$ for any $i, j = 1, \ldots, s$, and let $\sigma_{s+j}(w_i) = y_{ji} + \sqrt{-1} \cdot z_{ji}$ for any $i, j = 1, \ldots, t$, where y_{ji} and $z_{ji} \in \mathbb{R}$. Then

$$d = \det \sigma(O_k) = \det \begin{bmatrix} x_{11} & \cdots & x_{s1} & y_{11} & z_{11} & \cdots & y_{t1} & z_{t1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ x_{1n} & \cdots & x_{sn} & y_{1n} & z_{1n} & \cdots & y_{tn} & z_{tn} \end{bmatrix}$$

It is clear that $d = d^*/(-2\sqrt{-1})^t$, where

$$d^* = \det \begin{bmatrix} x_{11} & \cdots & x_{s1} & y_{11} + \sqrt{-1} \cdot z_{11} & y_{11} - \sqrt{-1} \cdot z_{11} & \cdots \\ \vdots & & \vdots & \vdots & \vdots & \\ x_{1n} & \cdots & x_{sn} & y_{1n} + \sqrt{-1} \cdot z_{1n} & y_{1n} - \sqrt{-1} \cdot z_{1n} & \cdots \end{bmatrix}$$

i.e., $D^* = \det(\sigma_i(w_j))$, where $\{\sigma_1, \ldots, \sigma_n\}$ is the full set of embeddings of k into $\mathbb{C}$. Since by the definition of the trace

$$\mathrm{Tr}(w_i \cdot w_j) = \sum_{\ell=1}^{n} \sigma_\ell(w_i) \cdot \sigma_\ell(w_j)$$

for $1 \leqslant i, j \leqslant n$, one has a matrix equality

$$(\mathrm{Tr}(w_i \cdot w_j)) = {}^{\mathrm{trans}}(\sigma_\ell(w_i)) \cdot (\sigma_\ell(w_j))$$

where *trans* denotes transposition, whence

$$D_k = \det(\mathrm{Tr}(w_i \cdot w_j)) = (d^*)^2$$

and we are done. □

Units. An element $a \in O_k$ is called a *unit* if and only if $a^{-1} \in O_k$. Clearly all the units form a group which is denoted O_k^*. Torsion elements of O_k^* are roots of unity. One easily checks that $a \in O_k^*$ if and only if $N_{k/\mathbb{Q}}(a) = \pm 1$.

The structure of the group O_k^* is rather simple, it is described by the famous Dirichlet theorem:

Theorem. *O_k^* is the product of its finite torsion subgroup by a free abelian group of rank $r = s + t - 1$.*

Sketch of proof. Let us consider the map

$$\begin{aligned} O_k^* &\xrightarrow{\log} \mathbb{R}^{s+t} \\ a &\longmapsto (\log|\sigma_1(a)|, \ldots, \log|\sigma_s(a)| \,;\, \log|\sigma_{s+1}(a)|^2, \ldots) \end{aligned}$$

Its kernel is the torsion subgroup of O_k^*, and its image $\log(O_k^*)$ is contained in the hyperplane $H \subset \mathbb{R}^{s+t}$ defined by $x_1 + \cdots + x_{s+t} = 0$.

Indeed,

$$|\sigma_1(a)|\cdots|\sigma_s(a)|\cdot|\sigma_{s+1}(a)|^2\cdots|\sigma_{s+t}(a)|^2=|N(a)|=1.$$

One can show that $\log(O_k^*)$ is a lattice in H (of full rank) which gives the theorem.

The determinant of this lattice

$$R=R_k=\det\begin{bmatrix}\log|\sigma_1(u_1)| & \cdots & \log|\sigma_1(u_{s+t-1})| \\ \vdots & & \vdots \\ \log|\sigma_{s+t-1}(u_1)| & \cdots & \log|\sigma_{s+t-1}(u_{s+t-1})|\end{bmatrix}$$

where $\{u_1,\ldots,u_{s+t-1}\}$ is a basis of O_k^* modulo torsion, is called the *regulator* of k.

Places. A map $\|\cdot\|:k\to\mathbb{R}$ is called an *absolute value* if the following conditions hold :

- $\|0\|=0$, $\|x\|>0$ if $x\neq 0$;
- there exist $x,y\in k^*$ such that $\|x\|\neq\|y\|$;
- $\|x\cdot y\|=\|x\|\cdot\|y\|$;
- there exists a positive real λ such that $\|x+y\|\leqslant\lambda\cdot(\|x\|+\|y\|)$.

Two absolute values $\|\cdot\|_1$ and $\|\cdot\|_2$ are *equivalent* if there exists a positive real θ such that $\|\cdot\|_1=\|\cdot\|_2^\theta$. An equivalence class of absolute values is called a *place* of k.

There is a beautiful description of all places of a number field.

Let $\sigma:k\hookrightarrow\mathbb{C}$ be an embedding of fields. Let us put $\|x\|_\sigma=|\sigma(x)|$ if σ is a real embedding (i.e., $\mathrm{Im}\sigma\subset\mathbb{R}$), and $\|x\|_\sigma=|\sigma(x)|^2$ if σ is a complex embedding. These are absolute values. One can check that two such absolute values $\|\cdot\|_\sigma$ and $\|\cdot\|_{\sigma'}$ are equivalent if and only if either $\sigma'=\sigma$, or $\sigma'=\overline{\sigma}$. Thus we obtain s *real* and t *complex* places of k. These places are called *infinite* or *archimedean*, the set of infinite places is denoted by S_∞.

Let then $\mathfrak{p}$ be a maximal ideal of O_k. For $x\in k^*$ let

$$\mathrm{ord}_\mathfrak{p}(x)=\max\{n\mid x\in\mathfrak{p}^n\}.$$

One easily checks that

$$\operatorname{ord}_{\mathfrak{p}}(x \cdot y) = \operatorname{ord}_{\mathfrak{p}}(x) + \operatorname{ord}_{\mathfrak{p}}(y)$$

for any $x, y \in k^*$, and if also $x + y \in k^*$ then

$$\operatorname{ord}_{\mathfrak{p}}(x + y) \geqslant \min\{\operatorname{ord}_{\mathfrak{p}}(x), \operatorname{ord}_{\mathfrak{p}}(y)\}.$$

Let us define the corresponding absolute value: for $x \in k^*$ let

$$\|x\|_{\mathfrak{p}} = N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(x)},$$

where $N(\mathfrak{p}) = |O_k/\mathfrak{p}|$. For such an absolute value (and for any one equivalent to it) a stronger condition holds:

$$\|x + y\| \leqslant \lambda \cdot \max\{\|x\|, \|y\|\}$$

(which is wrong for archimedean absolute values). Such absolute values are called *non-archimedean.* If $\mathfrak{p} \neq \mathfrak{p}'$ then the corresponding absolute values are not equivalent, i.e., each maximal ideal (each closed point of $\operatorname{Spec} O_k$) corresponds to a place of k. Such places are called *finite* or *non-archimedean.*

It comes out that each place of a number field is either infinite or finite. If v is a place of k then the absolute values defined above are called *normalized* and denoted $\| \cdot \|_v$.

Let us recall that if there are no complex places, the number field is called *totally real*, if there are no real places, it is called *totally complex.*

Class group. Let $\mathfrak{a}$ be an ideal of O_k, and let $a \in k^*$. The set $\mathfrak{c} = a^{-1}\mathfrak{a}$ is called a *fractional ideal.* The set of non-zero fractional ideals is a group with the composition defined by

$$\mathfrak{a} \cdot \mathfrak{b} = \{x \cdot y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}.$$

Note that the inverse element is given by

$$\mathfrak{a}^{-1} = \{x \mid x^{-1} \in \mathfrak{a} - \{0\}\} \cup \{0\}.$$

We call fractional ideals $\mathfrak{c}$ and $\mathfrak{c}_1$ *equivalent* if $\mathfrak{c}_1 = a\mathfrak{c}$ for some $a \in k^*$. Equivalence classes of non-zero fractional ideals form a group Cl_k which is called the (ideal) *class group* of k.

Theorem. *The group* Cl_k *is finite for any algebraic number field* k*.*

The order of the class group $h = h_k = |\operatorname{Cl}_k|$ is called the *class number* of k.

Extensions. Sometimes it is necessary to consider field extensions $K/k, K$ and k being algebraic number fields. Let $[K:k] = \dim_k K = n$ and let O_K and O_k be the rings of integers in K and k, respectively. Any $x \in K$ is a root of an irreducible over k equation of the form

$$a_m \cdot x^m + \cdots + a_0 = 0$$

where $a_i \in O_k$ for $i = 0, \ldots, m$.

Let us define the (*relative*) *trace* and *norm* as

$$\begin{aligned} \operatorname{Tr}_{K/k}(x) &= -a_{m-1}/a_m, \\ N_{K/k}(x) &= (-1)^m a_0/a_m. \end{aligned}$$

Different. Let us consider the following subset in k:

$$\mathfrak{B}_{K/k} = \{x \in K \mid \operatorname{Tr}_{K/k}(x \cdot y) \in O_k \text{ for any } y \in O_k\}.$$

One can easily check that $\mathfrak{B}_{K/k}$ is a O_K-submodule in K which contains O_K. Hence there exist a unique ideal $\mathfrak{D}_{K/k}$ in O_k such that $\mathfrak{D}_{K/k} \cdot \mathfrak{B}_{K/k} = O_K$. The ideal $\mathfrak{D}_{K/k}$ is called the *different* of the extensions K/k. The ideal

$$D_{K/k} = \{N_{K/k}(x) \mid x \in \mathfrak{D}_{K/k}\}$$

in O_k is called the (relative) *discriminant* of the extension K/k.

The relative discriminant $D_{K/\mathbb{Q}}$ equals the ideal in $\mathbb{Z}$ generated by the absolute discriminant D_k. Thus D_k is defined by $D_{k/\mathbb{Q}}$ up to a sign.

Let $L \supset K \supset k$ be algebraic number fields. Then $\mathfrak{D}_{L/k} = \mathfrak{D}_{L/k} \cdot \mathfrak{D}_{K/k}$.

Proposition. *Let the degree of the extension L/K be equal to m. Then*

$$D_{L/k} = D_{K/k}^m \cdot N_{K/k}(D_{L/K}).$$

Unramified extensions. An algebraic field extension is called *unramified* if $D_{K/k} = (1)$. We have just seen that $\mathbb{Q}$ has no unramified extensions.

The rule $\mathfrak{a} \mapsto \mathfrak{a} \cdot O_K$ defines a group homomorphism $\mathrm{Cl}_k \to \mathrm{Cl}_K$; the norm map defines a homomorphism $\mathrm{Cl}_K \to \mathrm{Cl}_k$. If an extension K/k is unramified and abelian (i.e., normal with an abelian Galois group $\mathrm{Gal}(K/k)$) then the (global) class field theory gives

Theorem. $\mathrm{Gal}(K/k)$ *is isomorphic to the factor-group* $\mathrm{Cl}_k/N_{K/k}(\mathrm{Cl}_k)$.

Moreover there exists a maximal unramified abelian extension K_1 which is called the *Hilbert* or *absolute class-field* of k; $\mathrm{Gal}(K_1/k)$ is isomorphic to Cl_k.

Theorem. *Let K_1 be the absolute class field of an algebraic number field k. Then the canonical homomorphism* $\mathrm{Cl}_k \to \mathrm{Cl}_{K_1}$ *is trivial, i.e., all the ideals of O_k become principal in O_{K_1}.*

Class field towers. As we have seen above $\mathbb{Q}$ has no unramified extensions. There exist many algebraic number fields k with $h_k > 1$; for these fields the absolute class field K_1 is an unramified extension of degree h_K. If $h_{k_1} > 1$ we get the field $K_2 = (K_1)_1$ which is an unramified extension K_2/k (note that the extension K_2/k cannot be abelian). Iterating this construction we get either

(a) $h_{K_n} = 1$ for some n; hence we cannot obtain a larger unramified extension of k by our construction; or

(b) $h_{K_n} > 1$ for any n and hence we obtain an infinite unramified tower $k \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots$.

An algebraic number field which satisfies the last condition is called a field with an *infinite class field tower.*

Theorem. *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that if k is an algebraic number field of degree n and D_k has at least $f(n)$ distinct prime divisors then k has an infinite class field tower.*

On can give a precise formula for $f(n)$ but we do not need it here.

The discriminant D_k of a field satisfying the conditions of this theorem cannot be small. One can ask how to construct fields with infinite class field towers and small discriminants. To compare fields of various degrees one should use the parameter $|D_k|^{1/n}$ (note that it is constant in unramified towers). Here are the best examples discovered by J. Martinet.

Theorem. *The field*

$$k = \mathbb{Q}\left(\cos(2\pi/11), \sqrt{-46}\right)$$

of degree 10 *over* $\mathbb{Q}$ *has an infinite class field tower;*

$$|D_k| = 2^{15} \cdot 11^8 \cdot 23^5 \quad \textit{and} \quad |D_k|^{1/n} \approx 92.37.$$

The field

$$k = \mathbb{Q}\left(\sqrt{2}, \sqrt{3 \cdot 5 \cdot 7 \cdot 23 \cdot 29}\right)$$

of degree 4 *has an infinite class field tower of totally real fields;*

$$|D_k| = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 23^2 \cdot 29^2 \quad \textit{and} \quad |D_k|^{1/n} \approx 1058.57.$$

On the other hand using so-called “explicit formulas” one can obtain a lower bound for $|D_k|^{1/n}$:

Theorem. *let* k_i *be algebraic number fields and let* $n_i = [k_i : \mathbb{Q}] \to \infty$. *Let* s_i *be the number of real embeddings and* t_i *the number of pairs of complex embeddings of* k_i. *Suppose that the limits* $\sigma = \lim s_i/n_i$ *and* $\tau = \lim t_i/n_i$ *do exist. Then*

$$\liminf |D_{k_i}|^{1/n_i} \geqslant (4\pi e^{\gamma+1})^{\sigma} \cdot (4\pi e^{\gamma})^{2\tau},$$

γ *being the Euler constant. If the generalized Riemann hypothesis is valid then*

$$\liminf |D_{k_i}|^{1/n_i} \geqslant (8\pi e^{\gamma+\pi/2})^{\sigma} \cdot (8\pi e^{\gamma})^{2\tau}.$$

Curves and number fields. Algebraic number fields and fields of rational functions on curves over finite fields are called *global fields.* They have many features in common. Here we briefly describe some of them.

Let k be an algebraic number field and let O_k be its ring of integers. Let X be a curve over $\mathbb{F}_q$, $K = \mathbb{F}_q(X)$, let F be a finite set of closed points of X, $U = X - F$, and let $O_F = \mathbb{F}_q[U]$ be the ring of rational functions which are regular on U.

For both rings O_k and O_F any factor over a maximal ideal is a finite field.

For O_F all these fields contain $\mathbb{F}_q$ (the so-called “case of equal characteristics”), in the number field case among these fields there is an extension of $\mathbb{F}_p$ for any prime p (the “case of different characteristics”).

The notion of a place is in fact good for any global field. One can show that any place of $K = \mathbb{F}_q(X)$ is finite and corresponds to a closed point of X.

We can choose various finite sets F and get various rings O_F. In the number case we can choose a finite set S of maximal ideals of O_k and consider the ring O_S which is obtained from O_k by inverting non-zero elements of ideals from S; note that $\operatorname{Spec} O_S = \operatorname{Spec} O_k - S$ and $O_\phi = O_k$. Rings of the form O_S or O_F can be characterized as those having one-dimensional irreducible regular spectra of finite type over $\mathbb{Z}$.

The number field case is mostly more difficult than the function field case. Indeed, $\operatorname{Spec} O_F$ can be embedded into a proper scheme X and $\operatorname{Spec} O_k$ has no “good” embedding into a proper scheme. The last fact makes it indispensable to study infinite places of $\operatorname{Spec} O_k$.

The field $\mathbb{F}_q(T)$, T being a variable, is an analogue of $\mathbb{Q}$ since $k = \mathbb{F}_q(X)$ (where X is a curve over $\mathbb{F}_q$) is a finite extension of $\mathbb{F}_q(T)$; the ring $\mathbb{F}_q[T]$ is an analogue of $\mathbb{Z}$. Note however, that there is no canonical embedding of $\mathbb{F}_q(T)$ into $\mathbb{F}_q(X)$ and hence we cannot say that $[\mathbb{F}_q(X) : \mathbb{F}_q(T)]$ is an analogue of the degree of an algebraic number field.

One can suggest another analogue of the degree, namely, the number of $\mathbb{F}_q$-points of X. Indeed, if $|X(\mathbb{F}_q)| = N$, then the degree of a map $f : X \to \mathbb{P}^1$ (i.e., the degree of an extension $[\mathbb{F}(X) : \mathbb{F}_q(T)]$) can not be too small: $\deg f \geqslant N/(q + 1)$, since any $\mathbb{F}_q$-point of X is mapped to an $\mathbb{F}_q$-point of $\mathbb{P}^1$ and any fiber of f contains at most $\deg f$ $\mathbb{F}_q$-rational points.

Let a map $f : X \to \mathbb{P}^1$ be fixed, and let us fix an $\mathbb{F}_q$-point ∞ on $\mathbb{P}^1$. Then we have $\mathbb{P}^1 - \{\infty\} = \mathbb{A}^1$, $\mathbb{F}_q[\mathbb{A}^1] = \mathbb{F}_q[T]$ and we can regard the integral closure of $\mathbb{F}_q[T]$ in $\mathbb{F}_q(X)$ as an analogue of O_k. Note that this closure coincides with $O_{F_\infty} = \mathbb{F}_q[X - F_\infty]$ where $F_\infty = f^{-1}(\infty)$.

The ramification divisor B_f of the map f is an analogue of the different. The discriminant corresponds to the divisor $D = \sum e_p p$ where e_p is the ramification index of $P \in \mathbb{P}^1$. The value $\log \sqrt{|D_k|}$ is an analogue of the genus of a curve.

A fractional ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, where $\mathfrak{p}$ runs over prime ideals of O_k, corresponds to a divisor on X, $\mathfrak{a}^{-1}$ corresponds to $L(D)$ and the group $\operatorname{Pic} X$ is an analogue of Cl_k.

Note also that $\mathbb{F}_q(T)$ has no unramified extensions (just as $\mathbb{Q}$).

The value $\liminf(g/N)$ is an analogue of $\liminf \log |D_k|/n$. The "explicit formulas" technique gives estimates for both these values.

The question about an adequate analogue of the number of rational points on the Jacobian is rather delicate. One can suggest that its "genuine" analogue is the product $h_k R_k$ rather than h_k.

Units O_S^* of the ring O_S correspond to units O_F^* of O_F; the group μ_k is an analogue of $\mathbb{F}_q^*$. Moreover, just as in the number field case, $O_F^*/\mathbb{F}_q^*$ is a free abelian group of rank $|F|-1$ (note that $O_S^*/\mu_k \simeq \mathbb{Z}^{s+t+|S|-1}$).

There are some other analogies which are less clear but also useful, and we use them in the next section.

2. Number field and function field lattices

We are ready to present several constructions of lattices in the context of number theory and algebraic geometry and to calculate or estimate their parameters.

These results are quite recent and their discovery was stimulated by the theory of algebraic-geometric codes.

Additive lattices. Let k an be algebraic number field, of degree $N = s + 2t$, let O_k be its ring of integers, and let

$$\sigma : k \hookrightarrow \mathbb{R}^s \times \mathbb{C}^t$$

be the standard embedding. The image $L = \sigma(O_k)$ is a lattice of rank N.

Parameters. Let us compute the density of L. We have already seen above that

$$\det L = 2^{-t}\sqrt{|D_k|}.$$

Proposition.

$$\sqrt{s+t} \geqslant d(L) \geqslant \sqrt{s/2+t}$$

and if $t=0$ *then*

$$d(L) = \sqrt{N}.$$

Proof. Let

$$x = \sigma(f) = (x_1, \dots, x_s; y_1 + \sqrt{-1}\cdot z_1, \dots, y_t + \sqrt{-1}\cdot z_t).$$

We have

$$|\sigma(f)| = \sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t} (y_j^2 + z_j^2)}.$$

For $f=1$, $|\sigma(1)| = \sqrt{s+t}$.

The arithmetic mean geometric mean inequality yields

$$\begin{aligned}\sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t} (y_j^2 + z_j^2)} &\geqslant \frac{1}{\sqrt{2}} \cdot \sqrt{\sum_{j=1}^{s} x_j^2 + 2\cdot \sum_{j=1}^{t} (y_j^2 + z_j^2)} \\ &\geqslant \sqrt{\frac{s+2t}{2}} \cdot \left[\prod_{j=1}^{s} x_j^2 \cdot \prod_{j=1}^{t} (y_j^2 + z_j^2)^2\right]^{1/2N} \\ &= \sqrt{\frac{s}{2} + t} \cdot |N_{K/\mathbb{Q}}(f)|^{1/N} \\ &\geqslant \sqrt{\frac{s}{2} + t},\end{aligned}$$

since $N_{K/\mathbb{Q}}(f) \in \mathbb{Z}$. In the totally real case

$$\sqrt{\sum_{j=1}^{N} x_j^2} \geqslant \sqrt{N} \cdot \left[\prod_{j=1}^{N} x_j^2\right]^{1/2N} = \sqrt{N} \cdot |N_{K/\mathbb{Q}}(f)|^{1/N} \geqslant \sqrt{N},$$

and we get the required result. □

Unramified towers. Now let the field K vary so that $N \to \infty$, and K is either totally real, or totally complex. Then

$$\lambda(L) \sim -\log_2 \sqrt{\frac{\pi e}{2}} + \frac{1}{N} \cdot \log_2 \sqrt{|D_K|}.$$

If we want to construct good lattices the last term should be bounded. It is definitely so if K runs over an unramified tower of fields over some K_0, in which case it is just constant. We get

Theorem. *If a number field K_0 of degree N_0 has an infinite unramified tower of fields $K \supset K_0$which are either totally real, or totally complex, then it yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with*

$$\lambda(\{L_N\}) \sim -\log_2 \sqrt{\pi e/2} + \frac{1}{N_0} \cdot \log_2 \sqrt{|D_{K_0}|}.$$

For $K_0 = \mathbb{Q}\left(\cos(2\pi/11), \sqrt{-46}\right)$ we get $\lambda \sim 2.2218$ (recall that K_0 has an infinite class field tower).

On the other hand, the above "explicit formulas" theorem shows that for any family of fields K we cannot get asymptotically less than $1.193\cdots$ (and $1.694\cdots$ assuming the generalized Riemann hypothesis).

Multiplicative number field lattices. Up to this moment we have used the additive groups of global fields. Now we are going to exploit their multiplicative structure.

Construction. We start with a number field K of degree $N = s + 2t$ and a finite number of its places $S = S_\infty \cup S_f$ which includes all archimedean ones, let $n = |S|$. Let O_S^* be the set of S-units, i.e., $a \in O_S^*$ if and only if all the prime divisors of its numerator and denominator belong to S_f.

There is a natural map

$$\begin{aligned} O_S^* &\xrightarrow{\varphi_S} \mathbb{R}^n, \\ f &\longmapsto \{\log \|f\|_v\}, \end{aligned}$$

where $v \in S$, and $\|\cdot\|_v$ is the normalized absolute value, i.e., $\|f\|_v = |\sigma_v(f)|$ for real places, $\|f\|_v = |\sigma_v(f)|^2$ for complex ones, and $\|f\|_v = N(v)^{-\mathrm{ord}_v(f)}$ for $v \in S_f$. It is clear that

$$\mathrm{Ker}\varphi_S = \mu_K$$

is the group of roots of 1 in K, and that

$$\mathrm{Im}\,\varphi_S \subset H = \left\{x \in \mathbb{R}^n \;\Big|\; \sum x_i = 0\right\}$$

because of the product formula.

Parameters. Let R be the regulator of K and let $h = h_K$ be its class number. Set $h(f) = \sum_v |\log \|f\|_v|$ for $f \in K^*$, this is the *height function* (sorry that it is denoted by the same letter as the class number); $h(f) = 0$ if and only if $f \in \mu_K$. We set

$$h(K) = \min_{f \in K^* - \mu_K} h(a)$$

and call it the *height of the field K*.

Proposition. *Let $L_S = \varphi_S(O_S^*)$. Then*

(a) $\quad d(L_S) \geqslant \dfrac{1}{\sqrt{n}} \cdot h(K),$

(b) $\quad \operatorname{rk} L_S = n - 1 \quad$ *and* $\quad \det L_S \leqslant \sqrt{n} \cdot R \cdot h \cdot \prod\limits_{v \in S_f} \log N(v).$

We do not prove it here because the function field case that follows is much simpler and gives better results.

Asymptotic behaviour. To obtain asymptotically good families of lattices we are going to consider unramified towers of fields. In such towers $\frac{1}{N} \cdot \log \sqrt{|D_K|}$ is constant. Let us for simplicity assume that all the fields in the tower are totally real.

Theorem. *If a number field K_0 of degree n_0 has an infinite unramified tower of totally real fields then the above construction with $S = S_\infty$ yields a family of asymptotically good multiplicative lattices $\{L_N = L_S \subset \mathbb{R}^N\}$ with $N \to \infty$ and*

$$\lambda(\{L_N\}) \leqslant -\log_2 \sqrt{\pi^3 e/2} - \log_2 \log_e \left[(1+\sqrt{5})/2\right] + \frac{1}{n_0} \cdot \log_2 |D_{K_0}|.$$

For $K_0 = \mathbb{Q}\left(\sqrt{2}, \sqrt{3 \cdot 5 \cdot 7 \cdot 23 \cdot 29}\right)$ we get $\lambda \lesssim 8.41$.

Function field lattices. Here is a direct function field analogue of the previous construction.

Construction. Let

$$O^*_{\mathcal{P}} = \{f \in K^* \,|\, \mathrm{Supp}(f) \subseteq \mathcal{P}\}.$$

Recall that $\mathcal{P} \subseteq X(\mathbb{F}_q)$ for a curve X over $\mathbb{F}_q$ and $K = \mathbb{F}_q(X)$. Let $\mathrm{Div}_{\mathcal{P}}(X)$ denote the group of divisors supported in $\mathcal{P}$, $\mathrm{Div}^0(X)$ of those of degree $0, P_{\mathcal{P}}(X)$ the subgroup of principal divisors. Let $J_X = \mathrm{Div}^0(X)/P(X)$ be the Jacobian of X.

There is a natural map

$$\begin{aligned} O^*_{\mathcal{P}} &\xrightarrow{\varphi_{\mathcal{P}}} \mathrm{Div}_{\mathcal{P}}(X) \simeq \mathbb{Z}^n, \\ f &\longmapsto (f). \end{aligned}$$

It is clear that $\ker \varphi_{\mathcal{P}} = \mathbb{F}^*_q$ is again the group of roots of 1 in K, and that

$$\mathrm{Im}\,\varphi_{\mathcal{P}} \subseteq \mathrm{Div}^0_{\mathcal{P}}(X) \simeq A_{n-1} = \left\{x \in \mathbb{Z}^n \mid \sum x_i = 0\right\}.$$

We set

$$L_{\mathcal{P}} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P}}) \subseteq A_{n-1} \otimes \mathbb{R} \simeq \mathbb{R}^{n-1}.$$

Parameters. Let us estimate the parameters of $L_{\mathcal{P}}$.

Theorem. *Let $L_{\mathcal{P}} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P}})$. Then*

(a) $$d(L_{\mathcal{P}}) \geqslant \min_{f \in O^*_{\mathcal{P}} - \mathbb{F}^*_q} \sqrt{2 \cdot \deg f} \geqslant \sqrt{\frac{2 \cdot |X(\mathbb{F}_q)|}{q+1}},$$

(b) $$\mathrm{rk}\, L_{\mathcal{P}} = n - 1 \quad \textit{and}$$

$$\det L_{\mathcal{P}} \leqslant \sqrt{n} \cdot |J_X(\mathbb{F}_q)| \leqslant \sqrt{n} \cdot \left[1 + q + \frac{|X(\mathbb{F}_q)| - q - 1}{g}\right]^g.$$

Proof

(a) Let $f \in O^*_{\mathcal{P}}$, $f \notin \mathbb{F}^*_q$,

$$\varphi_{\mathcal{P}}(f) = (x_1, \ldots, x_n) \in \mathbb{Z}^n.$$

Then

$$|\varphi_{\mathcal{P}}(f)| = \sqrt{\sum x_i^2} \geqslant \sqrt{\sum |x_i|} = \sqrt{2 \cdot \deg f},$$

since $x_i \in \mathbb{Z}$, $\sum x_i = 0$, $\deg f = \sum_{x_i > 0} x_i$. Any $f \in K$ maps $\mathbb{F}_q$-points to $\mathbb{F}_q$-points of $\mathbb{P}^1$. Therefore

$$|X(\mathbb{F}_q)| \leqslant (q+1) \cdot \deg f$$

and we get the second inequality.

(b) We know that $\det A_{n-1} = \sqrt{n}$ and

$$\det L_{\mathcal{P}} = [A_{n-1} : L_{\mathcal{P}}] \cdot \det A_{n-1}.$$

Then

$$A_{n-1} \simeq \mathrm{Div}^0_{\mathcal{P}}(X) \subset \mathrm{Div}^0(X),$$

and

$$L_{\mathcal{P}} \simeq P_{\mathcal{P}}(X) = P(X) \cap \mathrm{Div}^0_{\mathcal{P}}(X).$$

Therefore

$$[A_{n-1} : L_{\mathcal{P}}] \leqslant [\mathrm{Div}^0(X) : P(X)] = |J_X(\mathbb{F}_q)|.$$

To prove the second inequality it is sufficient to establish the following bound for the number of points on the Jacobian:

$$|J_X(\mathbb{F}_q)| \leqslant \left[1 + q + \frac{|X(\mathbb{F}_q)| - q - q}{g}\right]^g.$$

Indeed, $|J_X(\mathbb{F}_q)| = \prod\limits_{i=1}^{2g}(1-\omega_i)$, ω_i being the Frobenius roots, $|\omega_i| = \sqrt{q}$, $\omega_{g+i} = \overline{\omega}_i$. The arithmetic mean geometric mean inequality yields

$$\prod_{i=1}^{2g}(1 - \omega_i) = \prod_{i=1}^{g}(q + 1 - \omega_i - \overline{\omega}_i) \leqslant \left[\frac{\sum_{i=1}^{g}(q + 1 - \omega_i - \overline{\omega}_i)}{g}\right]^g,$$

and the estimate for $|J_X(\mathbb{F}_q)|$ follows from

$$-\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = |X(\mathbb{F}_q)| - q - 1. \qquad \square$$

Asymptotic behaviour. We consider families of curves of growing genus with

$$\frac{|X(\mathbb{F}_q)|}{g} \longrightarrow A,$$

and set $\mathcal{P} = X(\mathbb{F}_q)$. We get

Theorem. *A family of curves X over $\mathbb{F}_q$ of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \longrightarrow A > 0$$

yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with

$$\lambda(\{L_N\}) \leqslant -\log_2 \sqrt{\pi e} + \log_2 \sqrt{q+1} + A^{-1} \log_2(1 + q + A).$$

We are again interested to take the largest possible A. Let $q = p^{2m}$, then we can consider curves with $A = \sqrt{q} - 1$. For such curves we can in fact do better than for an arbitrary family.

Proposition. *For a family of curves X over $\mathbb{F}_q$ with*

$$\frac{|X(\mathbb{F}_q)|}{g} \longrightarrow \sqrt{q} - 1$$

there is an asymptotic equality

$$\frac{1}{g} \cdot \log_2 |J_X(\mathbb{F}_q)| \sim \log_2 q + (\sqrt{q} - 1) \cdot \log_2 \left(q/(q-1)\right).$$

Using this result we get

Theorem. *A family of curves X over $\mathbb{F}_q$ of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \longrightarrow \sqrt{q} - 1$$

yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with

$$\lambda(\{L_N\}) \leqslant -\log_2 \sqrt{\pi e} + \log_2 \frac{\sqrt{q+1}}{q-1} + \frac{\sqrt{q}}{\sqrt{q}-1} \cdot \log_2 q.$$

For $q = 9$ we get $\lambda \lesssim 1.8687 \cdots$.

Congruence constructions. Now we shall discuss some constructions depending on a divisor.

Multiplicative congruence sublattices. The construction of multiplicative lattices can be slightly elaborated. We consider some specific sublattices of $L_{\mathcal{P}}$. Let D be a positive divisor on X, $D = \sum a_i P_i$, $r_i = \deg P_i$, $N(P_i) = q^{r_i}$,

$$a = \deg D = \sum a_i r_i.$$

We write $f \equiv 1 \mod D$ if $\mathrm{ord}_{P_i}(f - 1) \geqslant a_i$ for any $P_i \in \operatorname{Supp} D$. Suppose that $\mathcal{P} \cap \operatorname{Supp} D = \varnothing$. Let

$$O^*_{\mathcal{P},D} = \{f \in O^*_{\mathcal{P}} \mid f \equiv 1 \mod D\},$$

and consider the lattice $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P},D}) \subseteq L_{\mathcal{P}}$.

Parameters. Here are the estimates.

Proposition. *Let $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P},D})$. Then*

(a) *$d(L_{\mathcal{P},D}) \geqslant \sqrt{2a}$,*

(b) *$\operatorname{rk} L_{\mathcal{P},D} = n-1$ and*

$$\det L_{\mathcal{P},D} \leqslant \sqrt{n} \cdot |J_X(\mathbb{F}_q)| \cdot \frac{q^a}{q-1} \cdot \prod \left(1 - q^{-r_i}\right).$$

Proof

(a) As above we have

$$d(L_{\mathcal{P},D}) \geqslant \min_{f \in O^*_{\mathcal{P},D-\{1\}}} \sqrt{2 \cdot \deg f},$$

and we notice that $\deg f = \deg(f-1) \geqslant \deg D = a$.

(b) We have already estimated $\det L_{\mathcal{P}}$, and we only need to estimate $[L_{\mathcal{P}} : L_{\mathcal{P},D}]$. Look at the embedding $O^*_{\mathcal{P}} \hookrightarrow \prod \widehat{O}^*_{P_i}$ is the group of units in the completion of the local ring at P_i. Let

$$\widehat{O}^*_{P_i,a_i} = \{x \in \widehat{O}^*_{P_i} \mid x \equiv 1 \mod a_i P_i\}.$$

We have $O^*_{\mathcal{P},D} = O^*_{\mathcal{P}} \cap (\prod \widehat{O}^*_{P_i,a_i})$ and

$$[O^*_{\mathcal{P}} : O^*_{\mathcal{P},D}] \leqslant \left[\prod \widehat{O}^*_{P_i} : \prod \widehat{O}^*_{P_i,a_i}\right] = \prod \left[(q^{r_i} - 1)^{r_i(a_i-1)}\right].$$

Then $\ker \varphi_{\mathcal{P}} = \mathbb{F}^*_q$ and $0^*_{\mathcal{P},D} \cap \ker \varphi_{\mathcal{P}} = \{1\}$, therefore

$$[O^*_{\mathcal{P}} : O^*_{\mathcal{P},D}] = (q-1) \cdot [L_{\mathcal{P}} : L_{\mathcal{P},D}].$$ □

Asymptotic behaviour. Consider the same family of curves as above, let $\mathcal{P} = X(\mathbb{F}_q)$ and let D be such that

$$\lim \frac{\deg D}{|X(\mathbb{F}_q)|} = (2 \cdot \log_e q)^{-1}$$

(this choice appears to be optimal). We get

Theorem. *A family of curves X over $\mathbb{F}_q$ of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \longrightarrow \sqrt{q} - 1$$

with the appropriate choice of divisors yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with

$$\lambda(\{L_N\}) \leqslant -\log_2 \sqrt{\frac{\pi}{2}} + \frac{1}{2} \cdot \log_2(\log_e q) + \frac{\sqrt{q}}{\sqrt{q}-1} \cdot \log_2 q - \log_2(q-1).$$

For $q = 2209 = 47^2$ we get $\lambda \lesssim 1.3888\cdots$.

Number field case. We can now return to number fields and give a parallel theory, which is as usual more difficult.

For the totally complex field $\mathbb{Q}(\cos(2\pi/11), \sqrt{-46})$ and $S_0 = S_\infty$ we get $\lambda \lesssim 11.1512\ldots$ For the totally real field $\mathbb{Q}(\sqrt{2}, \sqrt{3{\cdot}5{\cdot}7{\cdot}23{\cdot}29})$ and $S_0 = S_\infty$ we get $\lambda \lesssim 8.80$. These are not best choices but what we get is always much worse than for the function field case.

Another approach. Algebraic curves can also be used to construct lattices indirectly, that is we construct lattices using algebraic geometric codes. The construction is less elegant and we come to families of lattices with $\lambda \lesssim 2.30\cdots$ and families of non-lattice packings with $\lambda \lesssim 1.31\cdots$.

References

[1] J. H. Conway & N. J. A. Sloane – *Sphere packings, lattices and groups*, third ed., Grundlehren Math. Wiss., vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[2] M.A. Tsfasman – “Global fields, codes and sphere packings”, in *Journées Arithmétiques (Luminy, 1989)*, Astérisque, vol. 198-200, Société Mathématique de France, Paris, 1991, p. 373–396.

[3] M.A. Tsfasman & S.G. Vladut – *Algebraic-geometric codes*, Kluwer Academic Publishers, Dordrecht/Boston/London, 1991.

Michael A. Tsfasman, Institute for Information Transmission Problems, 19
Ermolovoi Street, GSP-4 Moscow 101447, Russia
& Laboratoire de Mathématiques Discrètes, Luminy - Case 930, 13288 Marseille
cedex 9, France
E-mail : mtsfasman@yandex.ru