Astérisque

MICHAEL A. TSFASMAN

Global fields, codes and sphere packings

Astérisque, tome 198-199-200 (1991), p. 373-396

<http://www.numdam.org/item?id=AST_1991__198-199-200__373_0>

GLOBAL FIELDS, CODES AND SPHERE PACKINGS

by

Michael A. TSFASMAN

Introduction

We are going to apply some simple algebraic geometry and number theory to codes and sphere packings. These constructions look rather exciting since on the one hand they lead to considerable progress in codes and packings, and on the other hand they concern rather deep properties of global fields. Moreover they look quite lucid and simple. Here we present *eight* constructions of this kind leading to asymptotically good families.

Section 0 provides some necessary definitions concerning codes and packings (this paper is addressed to those knowing what a global field is). Then (in §§1-8) we discuss eight constructions. Each of them is characterized by the following data : 1) we use either number (N), or function (F) fields ; 2) we use either additive (A), or multiplicative (M) structure ; 3) we obtain either lattice packings (L), or codes (C) ; 4) the construction either depends on a divisor (D), or not. These are the meanings of abbreviations we use in the titles of sections. For each construction we estimate parameters and try to produce asymptotically good families.

Section 1 is due to the author (it is exposed, e.g. in [LI/TS] §7, [CO/SL] ch.8 §7, [TS/VL] ch.5). The construction of §2 was historically the first and is due to GOPPA [GO 1], its asymptotic significance was first understood in [TS/VL/ZI] (for a detailed exposition see [TS/VL]). Section 3 is due to LENSTRA [LE]. The next four constructions (§§4-7) are due to ROSENBLOOM and the author [RO/TS]. The construction of §5 has been independently discovered by QUEBBEMANN [QU]. The construction of §8 is again due to GOPPA [GO 2]. The last section is devoted to some remarks and open problems.

I would like to thank all above-mentioned mathematicians for sending me preprints, and M. ROSENBLOOM for many stimulating discussions. This paper has been finished during my stay in France, and I would like to express my gratitude to the University of Paris 7, to C.I.R.M., and personally to J-L. COLLIOT-THÉLÈNE, G. LACHAUD, J-J. SANSUC, Cyrille and Anna VELIKANOV, and all my friends and colleagues for their kind hospitality.

0. Packings and Codes

Notation. In what follows log denotes $\log_2$, and ln denotes $\log_e$. By $\sim$ we mean asymptotic equality and by $\gtrsim$ asymptotic inequality (up to a function tending to 0).

Sphere packings. We first consider a classical problem of packing equal non-overlapping spheres in $\mathbb{R}^n$. Let L be the set of centers and set

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

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

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

$$\Delta = \Delta(L) = \limsup_{c \to \infty} \frac{\mathrm{vol}(S \cap B_c)}{\mathrm{vol}(B_c)} ,$$

vol being the standard volume in $\mathbb{R}^N$, $S = \{x \in \mathbb{R}^N | \ |x - u| < \frac{d}{2}$ for some $u \in L\}$, $B_c = \{x \in \mathbb{R}^N | \ |x| \leq c\}$.

Let $V_N = \frac{\pi^{N/2}}{\Gamma(\frac{N}{2}+1)}$ be the volume of unit sphere. We define some other parameters setting

$$\begin{aligned} \delta(L) &= \frac{\Delta(L)}{V_N} , \\ \nu(L) &= \log \delta(L) , \\ \gamma(L) &= 4(\delta(L))^{2/N} , \\ \lambda(L) &= -\frac{1}{N} \log \Delta(L) ; \end{aligned}$$

$\delta(L)$ is called the *center density*, and the most important (for our purposes) parameter $\lambda(L)$ is called the *density exponent.*

Lattices. The most interesting case is when L is an additive subgroup of $\mathbb{R}^N$, i.e. a lattice (we suppose that $d(L) > 0$ and $\Delta(L) > 0$). For a lattice L

$$\lambda(L) = -\frac{1}{N} \log \left(\frac{d(L)^N V_N}{2^N \det L} \right) ,$$

where $\det L = \mathrm{vol}(\mathbb{R}^N/L)$ is the volume of fundamental domain.

Each lattice corresponds to a quadratic form $f(x)$ on a free $\mathbb{Z}$-module of rank N, and the problem of finding the smallest possible λ (i.e. the largest possible Δ) is equivalent to another classical problem of finding a form of discriminant 1 with the maximum value of $\gamma(L) = \min_{x \in \mathbb{Z}^N - \{0\}} f(x)$, cf. [Mi].

Asymptotic behaviour. In this paper we are interested in lattices of high rank. Let $\{L_N \subset \mathbb{R}^N\}$ be a family of lattices with $N \to \infty$. Set

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

A family of lattices is called *asymptotically good* iff $\lambda(\{L_N\}) < \infty$. Using the Stirling formula we see that

$$\lambda(\{L_N\}) \ \sim \ -\log \sqrt{\frac{\pi e}{2}} + \log \sqrt{N} - \log d(L) + \frac{1}{N} \log(\det L).$$

Note that asymptotically $\gamma \ \sim \ \dfrac{2N}{\pi e}\, 4^{-\lambda}$.

It is known that $\lambda(\{L_N\}) \geq 0.599$ (the Kabatianski-Levenshtein bound, valid also for non-lattice packings) and that there exist families of lattices with $\lambda(\{L_N\}) \leq 1$ (the Minkowski existence bound).

However it is in fact very difficult to construct asymptotically good lattices explicitly (cf.[Co/Sl] , [Li/Ts]), and each construction leading to good lattices is of interest. (Natural families of lattices, such as $\mathbb{Z}^N$ and root lattices A_N and D_N , are asymptotically bad).

Codes. Let $\mathbb{F}_q$ be a finite field. Being finite the space $\mathbb{F}_q^n$ is equipped with the natural notion of volume (the number of points) and with the *Hamming norm* $\|v\| = |\{i \mid v_i \neq 0\}|$. Hence for this space there also exists a packing problem. A *code* is a set of points $C \subseteq \mathbb{F}_q^n$, n is called its *length*, $k = \log_q |C|$ is its *log-cardinality*, $d = \min_{v,u \in C, v \neq u} \|u - v\|$ is its *minimum distance*. The relative parameters are the *rate* $R = R(C) = k/n$, and the *relative distance* $\delta = \delta(C) = d/n$.

Linear codes. A code is called *linear* iff it is a linear subspace. For such a code k is an integer and $d = \min_{v \in C - \{0\}} \|v\|$.

Asymptotic behaviour. Let $\{C_n \subseteq \mathbb{F}_q^n\}$ be a family of codes with $n \to \infty$. In contrast with sphere packings, codes have two asymptotic parameters δ and R (the reason is that in $\mathbb{R}^N$ rescaling is possible and we can always set $d(L) = 1$). Set

$$\delta(\{C_n\}) = \limsup_{n \to \infty} \delta(C_n),$$
$$R(\{C_n\}) = \limsup_{n \to \infty} R(C_n).$$

A family of codes is called *asymptotically good* iff $\delta(\{C_n\}) > 0$ and $R(\{C_n\}) > 0$.

It is known that for any $\delta \in \left[0, \frac{q-1}{q}\right]$ there exist families of linear codes $\{C_n\}$ with

$$\delta(\{C_n\}) = \delta$$

and

$$R(\{C_n\}) \geq 1 - H_q(\delta)$$

(the Gilbert-Varshamov existence bound) ; here

$$H_q(x) = x \ \log_q(q-1) - x \ \log_q x - (1-x)\log_q(1-x).$$

is the q-ary entropy function. There also exist upper bounds which we do not discuss here. Again it is difficult to construct good codes explicitly.

There are many interesting links between codes and lattices, cf.[Co/ Sl].

1. Additive lattices (NAL)

Construction. Let K be a number field and let $\mathcal{O}_K$ be its ring of integers, $[K : \mathbb{Q}] = N = s + 2t$ where s is the number of real embeddings $K \hookrightarrow \mathbb{R}$ and t is the number of conjugate pairs of complex embeddings $K \hookrightarrow \mathbb{C}$. Together they form the standard embedding

$$\sigma : K \hookrightarrow \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^N$$

which is a homomorphism of $\mathbb{Q}$-algebras. Let $L = \sigma(\mathcal{O}_K)$.