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 $V_N = \dfrac{\pi^{N/2}}{\Gamma(\frac{N}{2}+1)}$ 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 $L = \sigma(\mathcal{O}_K)$.

Parameters. For $x = (x_1, \ldots, x_s \; ; \; y_1 + iz_1, \ldots, y_t + iz_t) \in \mathbb{R}^s \times \mathbb{C}^t$ let $N(x) = x_1 \cdots x_s(y_1^2 + z_1^2) \cdots (y_t^2 + z_t^2)$. Then $N(\sigma(f)) = N_{K/\mathbb{Q}}(f)$ is the norm of $f \in K$. Let $\mathcal{D}_K$ be the discriminant of K.

LEMMA 1.1. *Let* $L = \sigma(\mathcal{O}_K)$. *Then*

(i) $\det L = 2^{-t}\sqrt{|\mathcal{D}_K|}$,

(ii) $\sqrt{s+t} \geq d(L) \geq \sqrt{\frac{s}{2} + t}$,

and if $t = 0$ *then* $d(L) = \sqrt{N}$. COROLLARY 1.2. *Suppose that* K *is either totally real, or totally complex. Then*

$$\delta(L) = \frac{N^{N/2}}{2^N\sqrt{|\mathcal{D}_K|}} ,$$

$$\lambda(L) = 1 - \tfrac{1}{2}\log N - \tfrac{1}{N}\log V_N + \tfrac{1}{N}\log\sqrt{|\mathcal{D}_K|}.$$

Proof of Lemma 1.1 : (i) is straightforward (see [LA], ch.5, §2, Lemma 2). (ii) Let $x = \sigma(f) = (x_1, \ldots, x_s \; ; \; y_1 + iz_1, \ldots, y_t + iz_t)$. 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

$$\sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t}(y_j^2 + z_j^2)} \geq \frac{1}{\sqrt{2}} \sqrt{\sum_{j=1}^{s} x_j^2 + 2\sum_{j=1}^{t}(y_j^2 + z_j^2)} \geq$$

$$\geq \sqrt{\frac{s+2t}{2}} \left(\prod_{j=1}^{s} x_j^2 \prod_{j=1}^{t}(y_j^2 + z_j^2)^2\right)^{1/2N} = \sqrt{\frac{s}{2} + t} \;\; |N_{K/\mathbb{Q}}(f)|^{1/N} \geq \sqrt{\frac{s}{2} + t} ,$$

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

$$\sqrt{\sum_{j=1}^{N} x_j^2} \geq \sqrt{N}\left(\prod_{j=1}^{N} x_j^2\right)^{1/2N} = \sqrt{N} \;\; |N_{K/\mathbb{Q}}(f)|^{1/N} \geq \sqrt{N}. \qquad \blacksquare$$

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

$$\lambda(L) \sim -\log\sqrt{\frac{\pi e}{2}} + \frac{1}{N}\log\sqrt{|\mathcal{D}_K|}.$$

If we want to construct good lattices the last term should be bound. 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 1.3. *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*

$$\lambda(\{L_N\}) \sim -\log\sqrt{\frac{\pi e}{2}} + \frac{1}{N_0}\log\sqrt{|\mathcal{D}_{K_0}|}. \qquad \blacksquare$$

For $K_0 = \mathbb{Q}(\cos\frac{2\pi}{11}, \sqrt{-46})$ we get $\lambda \sim 2.2218\ldots$ (for this field $[K_0 : \mathbb{Q}] = 10$, $|\mathcal{D}_{K_0}| = 2^{15} \cdot 11^8 \cdot 23^5$, and MARTINET proved that it has an infinite abelian tower). On the other hand, ODLYZKO-SERRE inequalities for the discriminant (based on the "explicit formulae") show that for any K we cannot get asymptotically less than $1.193\ldots$ (and $1.694\ldots$ assuming the generalizéd Riemann hypothesis).

Congruence lattices. Let $\mathfrak{a}$ be a fractional ideal in K. Consider the additive subgroup

$$L(\mathfrak{a}) = \mathfrak{a}^{-1} = \{f \in K \mid f\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

The corresponding lattice $L_\mathfrak{a} = \sigma(L(\mathfrak{a}))$ up to a multiplication by some $m \in \mathbb{Z}$ is a sublattice in L, and we can estimate its parameters more or less in the same manner as before. (This is the NALD-case).

2. Function field codes (FACD)

Construction. Here is a straightforward analogue. Let $K = \mathbb{F}_q(X)$ be a function field, X being a smooth projective curve over a finite field $\mathbb{F}_q$. Fix a set of points $\mathcal{P} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$ and let $M_\mathcal{P} = \{f \in K \mid f$ is regular at $\mathcal{P}\}$. There is a natural map

$$\varphi_\mathcal{P} : M_\mathcal{P} \to \mathbb{F}_q^n ,$$
$$\varphi_\mathcal{P}(f) = (f(P_1), \ldots, f(P_n)).$$

Let D be a divisor on X such that $\mathcal{P} \cap \operatorname{Supp} D = \emptyset$. Consider

$$L(D) = \{f \in K \mid (f) + D \geq 0\}.$$

The image $C = \varphi_{\mathcal{P}}(L(D)) \subseteq \mathbb{F}_q^n$ is a code.

Parameters. Let g be the genus of X and $a = \deg D$. Of course, the length n of C equals $|\mathcal{P}|$.

LEMMA 2.1. *Let $a < n$. Then for the code C*

(i) $d \geq n - a$,

(ii) $k = \dim L(D) \geq a - g + 1$,

and if $a \geq 2g - 1$ then $k = a - g + 1$.

Proof : (i) follows from the fact that the number of zeroes of $f \in L(D)$ cannot exceed $\deg D$. It also shows that (for $a < n$) $\varphi_{\mathcal{P}}$ is monomorphic on $L(D)$.

(ii) follows from the Riemann-Roch theorem. ∎

Asymptotic behaviour. Lemma 2.1 shows that

$$\delta + R \geq 1 - \frac{g-1}{n} \cdot$$

Consider a family of curves of growing genus with

$$\frac{|X(\mathbb{F}_q)|}{g} \to A.$$

Then we get a family of codes with $n \to \infty$ and

$$\delta + R \gtrsim 1 - A^{-1} ,$$

if $A > 1$ these codes are asymptotically good. The DRINFELD-VLĂDUŢ theorem states that $A \leq \sqrt{q} - 1$, and it is known that for $q = p^{2m}$ there exist families of curves with $A = \sqrt{q} - 1$. Let $\mathcal{P} = X(\mathbb{F}_q)$ (to be scrupulous about $\mathcal{P} \cap \operatorname{Supp} D = \emptyset$ we can also put $\mathcal{P} = X(\mathbb{F}_q) - P_0$, $D = aP_0$; it does not influence asymptotics, we never mention such things below).

THEOREM 2.2. *A family of curves of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \to A > 1$$

yields an asymptotically good family of codes such that for any $\delta \leq 1 - A^{-1}$ *there is a subfamily* $\{C_n\}$ *with* $\delta(\{C_n\}) = \delta$ *and*

$$R(\{C_n\}) \geq 1 - A^{-1} - \delta.$$

For $q = p^{2m}$ *we can set* $A = \sqrt{q} - 1$. ∎

It is not difficult to see that on some segment of the d-axis for $q = p^{2m} \geq 49$ these codes are better than the GILBERT-VARSHAMOV bound.

3. Number field codes (NAC)

The construction of §1 can be generalized using non-archimedian places. Let $S = S_f \cup S_\infty$ be a fixed finite set of places of a number field K. For $v \in S_f$ let $k(v)$ be the residue field, for $v \in S_f$ let $k(v) = \mathbb{R}$ for real places and $k(v) = \mathbb{C}$ for complex ones. Let $\mathfrak{a}$ be a fractional ideal such that $S_f \cap \operatorname{Supp} \mathfrak{a} = \emptyset$. For any $v \in S$ there is a natural map $\sigma_v : L(\mathfrak{a}) \to k(v)$. Together they form a map

$$\sigma_S : L(\mathfrak{a}) \to \bigoplus_{v \in S} k(v).$$

Everything is quite natural, but what we get is neither a code, nor a lattice (except for the case $S = S_\infty$ discussed in §1). Here is a way out.

Construction. Let $[K : \mathbb{Q}] = N = s + 2t$. Fix two integers $q \geq r > 1$. Let S_f be the set of places v of K such that for some $c(v) \in \mathbb{Z}$

$$r \leq N(v)^{c(v)} \leq q \ ,$$

where $N(v) = |k(v)|$. Let $S = S_f \cup S_\infty$, S_∞ being the set of all archimedian places, let $n = |S| = |S_f| + s + t$. To make our consideration simpler we suppose that the field is totally real, i.e. t=0.

Let

$$U = \{x \in \mathbb{R}^N \mid 0 < x_i < r^{a/N}\}.$$

There exists a shift U' of U such that $|U' \cap \sigma(\mathcal{O}_K)| \geq r^a / \sqrt{|\mathcal{D}_K|}$, $\sigma(\mathcal{O}_K)$ being the lattice studied in §1. Divide each side of the cube U' into q equal parts, and identify the set of q^N small cubes with $\mathbb{F}_q^N$. Define $\varphi_\infty : U' \cap \sigma(\mathcal{O}_K) \to \mathbb{F}_q^N$ mapping each point to the small cube it lies in ; let φ_v be the component of φ_∞ corresponding to $v \in S_\infty$. For $v \in S_f$ let φ_v be the map

$$U' \cap \sigma(\mathcal{O}_K) \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K / v^{c(v)} \hookrightarrow \mathbb{F}_q \ ,$$

where we identify the place $v \in S_f$ with the corresponding prime ideal, and $\mathcal{O}_K/v^{c(v)} \hookrightarrow \mathbb{F}_q$ is some fixed embedding of sets.

Let $\varphi_S : U' \cap \sigma(\mathcal{O}_K) \to \mathbb{F}_q^n$ be defined as $\varphi_S = (\varphi_{v_1}, \varphi_{v_2}, \ldots)$ for all $v \in S$. The image $C = \varphi_S(U' \cap \sigma(\mathcal{O}_K)) \subseteq \mathbb{F}_q^n$ is a (non-linear) code of length n.

Parameters. The parameters are estimated by the following result reminding one of Lemma 2.1.

LEMMA 3.1. *Let $a \leq n$. Then*

(i) $d \geq n + 1 - a$,

(ii) $k \geq a \ \log_q r - \log_q \sqrt{|\mathcal{D}_K|}$.

Proof: (i) Let $f_1, f_2 \in U' \cap \sigma(\mathcal{O}_K)$. Set

$$A = \{v \in S_\infty \mid \varphi_v(f_1) = \varphi_v(f_2)\},$$
$$B = \{v \in S_f \mid \varphi_v(f_1) = \varphi_v(f_2)\}.$$

On one hand $|f_1 - f_2|_v \leq r^{a/N}$ for any $v \in S_\infty$ and $|f_1 - f_2|_v \leq \dfrac{r^{a/N}}{q}$ for $v \in A$. On the other hand $f_1 - f_2 \in v^{c(v)}$ for any $v \in B$, and $N(v^{c(v)}) \geq r$. Let $\alpha = |A|$, $\beta = |B|$. We have

$$r^\beta \leq N_{K/\mathbb{Q}}(f_1 - f_2) < \frac{r^a}{q^\alpha} \leq r^{a-\alpha}.$$

Therefore $\alpha + \beta < a$, i.e. $d > n - a$.

(ii) We see that if $a \leq n$ then φ_S is an embedding and

$$|U' \cap \sigma(\mathcal{O}_K)| \geq r^a/\sqrt{|\mathcal{D}_K|}. \qquad \blacksquare$$

This lemma is also valid for $t \neq 0$, but the proof is slightly more difficult.

Asymptotic behaviour. Fix q and r and consider a family of fields K of growing degree. Let

$$\gamma = \liminf_K \frac{\log_q \sqrt{|\mathcal{D}_K|}}{n} ,$$

where $n = s + t + |S_f|$. We get a family of non-linear codes with $n \to \infty$ and

$$R \gtrsim (1 - \delta) \log_q r - \gamma ,$$

if $\gamma < \log_q r$ then there exist asymptotically good codes among them.

It is possible to prove (using the "explicit formulae again") that $\gamma > (\sqrt{q}-1)^{-1}$ which shows that the parameters of these codes are worse than in §2. On the other hand for $r = \frac{q+1}{2}$ there exist fields with $\gamma \leq \text{const} \cdot \frac{\log q}{q^{1/4}}$, where const does not depend on q. Summing up we get THEOREM 3.2. *A family of number fields K of growing degree with* $\liminf \frac{\log_q \sqrt{|\mathcal{D}_K|}}{n} = \gamma < \log_q r$ *where $n = s + t + |S_f|$, S_f being the set of non-archimedian places v such that for some $c(v) \in \mathbb{Z}$, $r \leq N_{K/\mathbb{Q}}(v)^{c(v)} \leq q$*
(r and q being fixed), yields a family of asymptotically good non-linear codes with $\delta(\{C_n\}) = \delta$ and

$$R(\{C_n\}) \geq (1-\delta)\log_q r - \gamma.$$

We can set $\gamma =$ const $\frac{\log q}{q^{1/4}}$. ■

It is not difficult to see that for a large q on some segment of the δ-axis these codes are better than the GILBERT-VARSHAMOV bound, though worse than in §2.

4. Multiplicative lattices (NML)

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 the archimedian ones, let $n = |S|$. Let $\mathcal{O}_S^*$ be the set of S-units, i.e. $f \in \mathcal{O}_S^*$ iff all the prime divisors of its numerator and denominator belong to S.

There is a natural map

$$\varphi_S : \mathcal{O}_S^* \to \mathbb{R}^n , \quad f \mapsto \{\ln \|f\|_v\} ,$$

where $v \in S$, and $\| \ \|_v$ 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 $\ker \varphi_S = W$ is the group of roots of 1 in K, and that $\mathrm{Im}\, \varphi_S \subset H = \{x \in \mathbb{R}^n \mid \sum x_i = 0\}$ because of the product formula.

Parameters. Let R be the regulator of K and let h be its class number. Set $h(f) = \sum\limits_{v} |\ln \|f\|_v|$ for $f \in K^*$, this is the height function (sorry that it is denoted by the same letter as the class number) ; $h(f) = 0$ iff $f \in W$. We set $h(K) = \min\limits_{f \in K^* - W} h(a)$ and call it the *height* of the field K.

LEMMA 4.1. *Let* $L_S = \varphi_S(\mathcal{O}_S^*)$. *Then*

(i) $d(L_S) \geq \dfrac{1}{\sqrt{n}}\, h(K)$,

(ii) *if* K *is totally real, then*

$$d(L_S) \geq \frac{[K:\mathbb{Q}]}{\sqrt{n}} \ln\left(\frac{1+\sqrt{5}}{2}\right) ,$$

(iii) $rk\ L_S = n-1$ *and*

$$\det L_S \leq \sqrt{n}\ Rh \prod_{v \in S_f} \ln N(v).$$

Proof : (i) is obvious since $\sqrt{\sum\limits_{i=1}^{n} x_i^2} \geq \dfrac{1}{\sqrt{n}} \sum |x_i|$.

(ii) In [Sc] it is proved that for any totally real field K

$$h(K) \geq [K:\mathbb{Q}] \ln\left(\frac{1+\sqrt{5}}{2}\right) .$$

(iii) Let the first coordinates in $\mathbb{R}^n$ correspond to $v \in S_\infty$. Consider the orthogonal projection

$$T : H \to H_0 = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{s+t} x_i = 0 \right\} = H_1 \oplus \mathbb{R}^{n-s-t} ,$$

where $H_1 = \{x \in \mathbb{R}^{s+t} \mid \sum x_i = 0\}$, T multiplies volumes by $\sqrt{s+t}/\sqrt{n}$. Since $H_1 \cap T(L_S)$ is the lattice of units, $\det(T(L_S) \cap H_1) = \sqrt{s+t}\ R$ and $\det T(L_S) = \sqrt{s+t}\ R \det(pr_2\, T(L_S))$. Using the obvious

$$\left[\sum_{v \in S_f} \mathbb{Z} \ln N(v) : pr_2\, T(L_S) \right] \leq h$$

we get the answer. ∎

Asymptotic behaviour. We start, as in §1, considering unramified towers of fields. In such towers $\frac{1}{N}\log\sqrt{|\mathcal{D}_K|}$ is constant. To bound $\frac{Rh}{|W|}$ we can use standard estimates for the residue of ζ-function of K.

If we put $s = 2$ in the proof of Lemma 1 of [LA] ch.XVI, §.1, we get

$$\frac{Rh}{|W|} \leq \frac{2|\mathcal{D}_K|}{\pi^{s+2t}}$$

(this is not the best estimate but the most obvious one).

In the totally real case $|W| = 2$. Put $S = S_\infty$ and consider unramified towers of totally real fields. We get

THEOREM 4.2. *If a number field K_0 of degree N_0 has an unramified tower of totally real fields then it yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with*

$$\lambda(\{L_N\}) \leq -\log\sqrt{\frac{\pi^3 e}{2}} - \log\,\ln\left(\frac{1+\sqrt{5}}{2}\right) + \frac{1}{N_0}\,\log|\mathcal{D}_{K_0}|.$$

For $K_0 = \mathbb{Q}(\sqrt{2}\ ,\ \sqrt{70035})$ we get $\lambda \lesssim 8.4046$ (for this field $N_0 = 4$, $|\mathcal{D}_{K_0}| = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 23^2 \cdot 29^2$ and MARTINET proved that is has a required tower).

5. Function field lattices (FML)

Here is a direct function field analogue of the construction of §4.

Construction. In the notation of §2, let

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

Let $\mathrm{Div}_{\mathcal{P}}(X)$ denote the group of divisors supported in $\mathcal{P}$, $\mathrm{Div}_{\mathcal{P}}^{\circ}(X)$ of those of degree 0, $\mathrm{Pr}_{\mathcal{P}}(X)$ the subgroup of principal divisors. Let $J_X = \mathrm{Div}^{\circ}(X)/\mathrm{Pr}(X)$ be the Jacobian of X.

There is a natural map

$$\varphi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* \longrightarrow \mathrm{Div}_{\mathcal{P}}(X) \simeq \mathbb{Z}^n\ ,$$
$$f \longmapsto (f)\ .$$

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

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

We set

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

Parameters. Let us start with a bound for the number of points on the Jacobian :

LEMMA 5.1. $|J_X(\mathbb{F}_q)| \leq \left(1 + q + \dfrac{|X(\mathbb{F}_q)| - q - 1}{g}\right)^g$.

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

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

and the statement follows from

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

Now we can estimate the parameters of $L_{\mathcal{P}}$.

LEMMA 5.2. *Let* $L_{\mathcal{P}} = \varphi_{\mathcal{P}}(\mathcal{O}_{\mathcal{P}}^*)$. *Then*

(i) $d(L_{\mathcal{P}}) \geq \min\limits_{f \in \mathcal{O}_{\mathcal{P}}^* - \mathbb{F}_q^*} \sqrt{2 \deg f} \geq \sqrt{\dfrac{2|X(\mathbb{F}_q)|}{q+1}}$,

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

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

Proof : (i) Let $f \in \mathcal{O}_{\mathcal{P}}^*$, $f \notin \mathbb{F}_q^*$, $\varphi_{\mathcal{P}}(f) = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Then

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

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

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

and we get the second inequality.

(ii) We know that $\det A_{n-1} = \sqrt{n}$, and $\det L_{\mathcal{P}} = [A_{n-1} : L_{\mathcal{P}}] \det A_{n-1}$. Then $A_{n-1} \simeq \mathrm{Div}^{\circ}_{\mathcal{P}}(X) \subset \mathrm{Div}^{\circ}(X)$, and $L_{\mathcal{P}} = \mathrm{Pr}_{\mathcal{P}}(X) = \mathrm{Pr}(X) \cap \mathrm{Div}^{\circ}_{\mathcal{P}}(X)$. Therefore

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

Lemma 5.1 gives the second inequality. ∎

Asymptotic behaviour. As in §2 we consider families of curves of growing genus with $\frac{|X(\mathbb{F}_q)|}{g} \to A$, and set $\mathcal{P} = X(\mathbb{F}_q)$. We get

THEOREM 5.3. *A family of curves of growing genus g such that*

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

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

$$\lambda(\{L_N\}) \leq -\log\sqrt{\pi e} + \log\sqrt{q+1} + A^{-1}\log(1+q+A) \ . \qquad ∎$$

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 even do slightly better than Lemma 5.1 :

LEMMA 5.4. *For a family of curves X with*

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

there is an asymptotic equality

$$\frac{1}{g}\log|J_X(\mathbb{F}_q)| \sim \log q + (\sqrt{q}-1)\log\frac{q}{q-1} \ .$$

Proof : Let $N_r = |X(\mathbb{F}_{q^r})|$. Then

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \omega_i^r \ ,$$

where $\omega_i = \sqrt{q}\,\alpha_i$, $|\alpha_i| = 1$, and $\alpha_i^{-1} = \alpha_{g+i}$ for $i = 1, \ldots, g$. We are interested in $M = |J_X(\mathbb{F}_q)| = \prod_{i=1}^{2g}(1-\omega_i)$. Let $b = \log_q g$. Then

$$\frac{1}{g}\left|\sum_{m=b+1}^{\infty} \frac{q^{-m/2}}{m} \sum_{i=1}^{2g} \alpha_i^m\right| \le 2 \sum_{m=b+1}^{\infty} \frac{q^{-m/2}}{m} \to 0 \text{ when } g \to \infty .$$

Since $0 \le |\alpha_i^n + \alpha_i^{n-1} + \cdots + 1|^2 = (n+1) + \sum_{j=1}^{n}(n+1-j)(\alpha_i^j + \alpha_i^{-j})$, we have

$$n+1 \ge -\sum_{j=1}^{n}(n+1-j)(\alpha_i^j + \alpha_i^{-j}) ,$$

summing it over $i = 1, \ldots, 2g$ and using $\sum \alpha_i^j = \sum \alpha_i^{-j}$, and $-\sum_{i=1}^{2g} \alpha_i^j = N_j\, q^{-j/2} - q^{j/2} - q^{-j/2}$ we get

$$g(b+1) \ge \sum_{j=1}^{b} (b+1-j)[N_j\, q^{-j/2} - q^{j/2} - q^{-j/2}] ,$$

or

$$1 \ge \sum_{j=1}^{b} (1 - \frac{j}{b+1})\, \frac{N_1}{g}\, q^{-j/2} + \sum_{j=1}^{b} (1 - \frac{j}{b+1})\, \frac{(N_j - N_1)}{g}\, q^{-j/2} - \\ - \frac{1}{g} \sum_{j=1}^{b} (1 - \frac{j}{b+1})(q^{j/2} + q^{-j/2}) .$$

The last term is less than

$$\frac{1}{g}\sum_{j=1}^{b} q^{j/2} + \frac{1}{g}\sum_{j=1}^{b} q^{-j/2}$$

which tends to 0 when $g \to \infty$. The first term tends to

$$\frac{N_1}{g}\sum_{j=1}^{\infty} q^{-j/2} = \frac{N_1}{g}\,(\sqrt{q}-1)^{-1} \to 1 ,$$

therefore

$$\sum_{j=1}^{b} \frac{N_j - N_1}{g}\, q^{-j/2} \to 0 .$$

Now we are able to estimate

$$\frac{1}{g}\ln M = \frac{1}{g}\ln\prod_{i=1}^{2g}(1-\omega_i) = \frac{1}{g}\ln\left(q^g\prod_{i=1}^{2g}(1-\alpha_i\,q^{-1/2})\right)$$

$$= \ln q + \frac{1}{g}\sum_{i=1}^{2g}\ln(1-\alpha_i\,q^{-1/2}) = \ln q - \frac{1}{g}\sum_{m=1}^{\infty}\frac{q^{-m/2}}{m}\sum_{i=1}^{2g}\alpha_i^m$$

$$= \ln q + \frac{1}{g}\sum_{m=1}^{b}\frac{q^{-m/2}}{m}\,[N_m q^{-m/2} - q^{m/2} - q^{-m/2}]$$

$$-\frac{1}{g}\sum_{m=b+1}^{\infty}\frac{q^{-m/2}}{m}\sum_{i=1}^{2g}\alpha_i^m\ .$$

The last term tends to 0, and the second term is

$$\frac{1}{g}\sum_{m=1}^{b}\frac{q^{-m/2}}{m}\,[N_m q^{-m/2} - q^{m/2} - q^{-m/2}] =$$

$$= \sum_{m=1}^{b}\frac{N_1}{g}\frac{q^{-m}}{m} + \sum_{m=1}^{b}\frac{q^{-m}}{m}\frac{(N_m - N_1)}{g} - \frac{1}{g}\sum_{m=1}^{b}\frac{1}{m} - \frac{1}{g}\sum_{m=1}^{b}\frac{q^{-m}}{m}\ .$$

The first term tends to

$$(\sqrt{q}-1)\sum_{m=1}^{\infty}\frac{q^{-m}}{m} = (\sqrt{q}-1)\ln\frac{q}{q-1}$$

and all the rest tend to zero. ■

Using Lemma 5.4 we get

THEOREM 5.5. *A family of curves of growing genus g such that*

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

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

$$\lambda(\{L_N\}) \le -\log\sqrt{\pi e} + \log\frac{\sqrt{q+1}}{q-1} + \frac{\sqrt{q}}{\sqrt{q}-1}\log q\ . \qquad ■$$

For $q = 9$ we get $\lambda \lesssim 1.8687\ldots$

6. Congruence sublattices (FMLD)

The construction of §5 can be slightly elaborated. We consider some specific sublattices of $L_{\mathcal{P}}$.

Construction. Let D be a positive divisor on X, $D = a_i P_i$, $r_i = \deg P_i$, $N(P_i) = q^{r_i}$, $a = \deg D = \sum a_i r_i$. We identify D and P_i with the corresponding ideals. Suppose that $\mathcal{P} \cap \operatorname{Supp} D = \emptyset$. Let

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

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

Parameters. Here are the estimates.

LEMMA 6.1. *Let $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(\mathcal{O}^*_{\mathcal{P},D})$. Then*

(i) $d(L_{\mathcal{P},D}) \geq \sqrt{2a}$,

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

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

Proof: (i) We use the first inequality of Lemma 5.2 (i), which in our case reads $d(L_{\mathcal{P},D}) \geq \min_{f \in \mathcal{O}^*_{\mathcal{P},D} - \{1\}} \sqrt{2 \deg f}$, and notice that $\deg f = \deg(f-1) \geq \deg D = a$.

(ii) Lemma 5.2 (ii) estimates $\det L_{\mathcal{P}}$, and we have only to estimate $[L_{\mathcal{P}} : L_{\mathcal{P},D}]$. Look at the embedding $\mathcal{O}^*_{\mathcal{P}} \hookrightarrow \prod \widehat{\mathcal{O}}^*_{P_i}$, where $\widehat{\mathcal{O}}^*_{P_i}$ is the group of units in the completion of the local ring at P_i.
Let $\widehat{\mathcal{O}}^*_{P_i,a_i} = \{x \in \widehat{\mathcal{O}}^*_{P_i} \mid x \equiv 1 (\operatorname{mod} P_i^{a_i})\}$. We have

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

and

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

Then $\operatorname{Ker} \varphi_{\mathcal{P}} = \mathbb{F}^*_q$ and $\mathcal{O}^*_{\mathcal{P},D} \cap \operatorname{Ker} \varphi_{\mathcal{P}} = \{1\}$, therefore $[\mathcal{O}^*_{\mathcal{P}} : \mathcal{O}^*_{\mathcal{P},D}] = (q-1)[L_{\mathcal{P}} : L_{\mathcal{P},D}]$. ∎

Asymptotic behaviour. Consider the same family of curves as in §5, let $\mathcal{P} = X(\mathbb{F}_q)$ and let D be such that $\lim \dfrac{\deg D}{|X(\mathbb{F}_q)|} = (2 \ln q)^{-1}$ (this choice appears to be optimal). We get

THEOREM 6.2. *A family of curves of growing genus g such that*

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

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

$$\lambda(\{L_N\}) \leq -\log\sqrt{\frac{\pi}{2}} + \frac{1}{2}\log(\ln q) + \frac{\sqrt{q}}{\sqrt{q}-1}\log q - \log(q-1)\ . \qquad \blacksquare$$

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

7. Number field case (NMLD)

Now we return to the number field case and discuss an analogue of congruence lattices of §6. Here we also obtain good lattices.

Construction. In the notation of §4 let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal, $\mathfrak{a} = \prod v_i^{a_i}$, such that $v \notin S_f$ (i.e. $S_f \cap$ Supp $\mathfrak{a} = \emptyset$).
Let

$$\mathcal{O}^*_{S,\mathfrak{a}} = \{f \in \mathcal{O}^*_S \mid f \equiv 1(\text{mod } \mathfrak{a})\}$$

and consider the lattice $L_{S,\mathfrak{a}} = \varphi_S(\mathcal{O}^*_{S,\mathfrak{a}}) \subseteq L_S$.

Parameters. Everything is quite similar to §6, though the estimates are slightly worse. Let $W_\mathfrak{a} = W \cap \mathcal{O}^*_{S,\mathfrak{a}}$.

LEMMA 7.1. *Let $L_{S,\mathfrak{a}} = \varphi_S(\mathcal{O}^*_{S,\mathfrak{a}})$. Then*

(i) $d(L_{S,\mathfrak{a}}) \geq \dfrac{2}{\sqrt{n}}\,(\ln N_{K/\mathbb{Q}}(\mathfrak{a}) - (s+2t)\ln 2)$,

(ii) $rk\, L_{S,\mathfrak{a}} = n-1$ *and*

$$\det L_{S,\mathfrak{a}} \leq (\det L_S) N_{K/\mathbb{Q}}(\mathfrak{a}) \prod\Big(1 - \frac{1}{N_{K/\mathbb{Q}}(v_i)}\Big)[W : W_\mathfrak{a}]^{-1} \leq$$
$$\sqrt{(s+t)(n-s-t)}\mathrm{Rh}\Big(\prod_{v\in S_f} \ln N(v)\Big) N_{K/\mathbb{Q}}(\mathfrak{a})\Big(\prod\big(1 - \frac{1}{N_{K/\mathbb{Q}}(v_i)}\big)\Big)[W : W_\mathfrak{a}]^{-1}\ .$$

Proof: (i) Let $\varphi_S(f) = (x_1, x_2, \ldots, x_n)$, $x_i = \ln\|f\|_{v_i}$. Then

$$|\varphi_S(f)| = \sqrt{\sum x_i^2} \geq \frac{1}{\sqrt{n}}\sum|x_i| = \frac{2}{\sqrt{n}}\sum_{x_i>0} x_i.$$

We have

$$\sum_{x_i>0} x_i = \sum_{\substack{v\in S\\ \|f\|_v>1}} \ln\|f\|_v = \sum_{\substack{v\in S_\infty\\ \|f\|_v>1}} \ln\|f\|_v + \sum_{\substack{v\in S_f\\ \mathrm{ord}_v(f-1)<0}} (-\mathrm{ord}_v(f-1))\ln N(v)$$

$$= \sum_{\substack{v\in S_\infty\\ \|f\|_v>1}} \ln\|f\|_v - \sum_{\substack{v\in S_\infty\\ \|f-1\|_v>1}} \ln\|f-1\|_v + \sum_{\substack{v\in S_\infty\\ \|f-1\|_v<1}} (-\ln\|f-1\|_v) +$$

$$+ \sum_{\substack{v\notin S_\infty\\ \|f-1\|_v<1}} (\mathrm{ord}_v(f-1))\ln N(v)$$

(we have used the equality $\mathrm{ord}_v(f-1) = \mathrm{ord}_v f$ for $\mathrm{ord}_v f < 0$, and the product formula). We omit the third term (it is non-negative), the fourth term is at least $\ln N_{K/\mathbb{Q}}(\mathfrak{a})$ since $f-1 \in \mathfrak{a}$, and the sum of the first two terms is at least $-\sum_{v\in S_\infty} \ln\|2\|_v$ since $\max\{0,\ln\|z\|\}+\max\{0,\ln\|1-z\|\}$ is minimum for $z=-1$ (both for $z\in\mathbb{R}$ and $z\in\mathbb{C}$).

(ii) Knowing Lemma 4.1 (ii) we have only to estimate $[L_S : L_{S,\mathfrak{a}}]$. Note that $\mathrm{Ker}\,\varphi_S = W$, $\mathrm{Ker}\,\varphi_S \cap \mathcal{O}^*_{S,\mathfrak{a}} = W_\mathfrak{a}$, and proceed as in the proof of Lemma 6.1 (ii). ∎

Asymptotic behaviour. The proof of Lemma 7.1 (i) shows also that if $\log N_{K/\mathbb{Q}}(\mathfrak{a}) > s+2t$ then $W_\mathfrak{a} = \{1\}$ since $\varphi_S(f) = 0$ for $f\in W_\mathfrak{a}$. We choose $\mathfrak{a}$ in such a way that $\frac{1}{n}\log N_{K/\mathbb{Q}}(\mathfrak{a}) \sim \frac{s+2t}{n} + \log e$ (it is in fact optimal), K runs over an unramified tower.

As in §4 we have $\frac{Rh}{|W|} \leq \frac{2|\mathcal{D}_K|}{\pi^{s+2t}}$. Let us choose S in such a way that $\frac{s+2t}{n}$ is constant in the tower and that both S and Supp $\mathfrak{a}$ completely split in it (of course this restricts the choice of the tower). We get

THEOREM 7.2. *If a number field K_0 of degree N_0 has an infinite unramified tower in which sets of its places S_0 (with $n_0 = |S_0|$) and* Supp $\mathfrak{a}_0$ *split completely then it yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with*

$$\lambda(\{L_N\}) \leq -\log\sqrt{\frac{2\pi}{e}} + \frac{1}{n_0}\log|\mathcal{D}_{K_0}| - \frac{N_0}{n_0}(\log\pi - 1) +$$
$$+\frac{1}{n_0}\sum_{v\in S_{0f}} \log(\ln N(v)) + \frac{1}{n_0}\sum_{v_i|\mathfrak{a}} \log\left(1 - \frac{1}{N_{K_0/\mathbb{Q}}(v_i)}\right)\cdot \qquad ∎$$

For the totally complex field $\mathbb{Q}\,(\cos\frac{2\pi}{11}, \sqrt{-46})$ and $S_0 = S_\infty$ we get $\lambda \lesssim 11.1512$.

For the totally real field $\mathbb{Q}(\sqrt{2}, \sqrt{70035})$ and $S = S_\infty$ we get $\lambda \lesssim 8.7920$. These are not best choices, but what we get is always much worse than in §6.

8. Congruence codes (FMCD)

The construction we are now going to expose corresponds to function field congruence lattices of §6 in the same way as number field codes of §3 correspond to additive number field lattices of §1.

Construction. In the notation of §6 suppose that $D = pD'$ for some positive divisor D' (where p is the characteristic of $\mathbb{F}_q$, $q = p^m$).

Let $C = L_{\mathcal{P},D}/((p\mathbb{Z})^n \cap L_{\mathcal{P},D}) \subseteq (\mathbb{Z}/p)^n = \mathbb{F}_p^n$. It is a p-ary code of length n.

To study C we have to give another construction of the same code. Let $\Omega(\sum\limits_{P_i \in \mathcal{P}} P_i - D)$ be the space of differential forms ω on X such that $(\omega) + \sum P_i - D \geq 0$.

There are natural maps

$$d\log : \mathcal{O}^*_{\mathcal{P},D} \to \Omega(\textstyle\sum P_i - D) \ , \qquad f \mapsto \frac{df}{f}$$

(here we use the condition $D = pD'$, it yields $\dfrac{df}{f} \equiv 0 (\mathrm{mod}\ D)$) and

$$\mathrm{Res}_{\mathcal{P}} \ : \Omega(\textstyle\sum P_i - D) \to \mathbb{F}_q^n \ , \qquad \omega \mapsto (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega)) \ .$$

It is well known that $C' = \mathrm{Im}\ \mathrm{Res}_{\mathcal{P}}$ is a code dual to that of §2 (and its parameters are $d' \geq a - 2g + 2$, $k' \geq n - a + g - 1$, $k' = n - a + g - 1$ for $a < n$). We have the following obvious commutative diagram

$$\begin{tikzcd}
\mathcal{O}^*_{\mathcal{P},D} \arrow[r, "\varphi_{\mathcal{P}}"] \arrow[d, "d\log"'] & L_{\mathcal{P},D} \arrow[r] & C \arrow[r, hook] & \mathbb{F}_p^n \arrow[d] \\
\Omega(\sum P_i - D) \arrow[rrr, "\mathrm{Res}_{\mathcal{P}}"] & & & \mathbb{F}_q^n
\end{tikzcd}$$

i.e. $C = C' \cap \mathbb{F}_p^n$.

Parameters. Now we are ready to estimate parameters.

LEMMA 8.1. *Let* $C = L_{\mathcal{P},D}/((p\mathbb{Z})^n \cap L_{\mathcal{P},D}) = C' \cap \mathbb{F}_p^n \subseteq \mathbb{F}_p^n$. *Then*

(i) $d \geq d' \geq a - 2g + 2$;

(ii) $k \geq n - 1 - m \,\dfrac{p-1}{p}\, a.$

Proof: (i) The first inequality is obvious. Let $\omega \in \Omega(\sum P_i - D)$, then the number of non-zero residues of ω equals the number of its poles (all poles being simple) which is at least $\deg D - 2g + 2$.

(ii) Let $B = L_{\mathcal{P},D} \cap (p\mathbb{Z})^n$. Then

$$\begin{aligned} p^k = |C| = [L_{\mathcal{P},D} : B] = \\ &= [A_{n-1} : A_{n-1} \cap (p\mathbb{Z})^n][A_{n-1} \cap (p\mathbb{Z})^n : B][A_{n-1} : L_{\mathcal{P},D}]^{-1} \,. \end{aligned}$$

We have $[A_{n-1} : A_{n-1} \cap (p\mathbb{Z})^n] = p^{n-1}$. The multiplication by p maps isomorphically A_{n-1} onto $A_{n-1} \cap (p\mathbb{Z})^n$ and $L_{\mathcal{P},D'}$ onto B. Therefore

$$\begin{aligned} [A_{n-1} \cap (p\mathbb{Z})^n : B][A_{n-1} : L_{\mathcal{P},D}]^{-1} = \\ &= [A_{n-1} : L_{\mathcal{P},D'}][A_{n-1} : L_{\mathcal{P},D}]^{-1} = [L_{\mathcal{P},D'} : L_{\mathcal{P},D}]^{-1} \,. \end{aligned}$$

Proceeding as in the proof of Lemma 6.1 (ii) we see that

$$[L_{\mathcal{P},D'} : L_{\mathcal{P},D}] \leq q^{\deg D - \deg D'} = p^{m \frac{p-1}{p} a} \,.$$

Summing up we get $k \geq n - 1 - m \,\dfrac{p-1}{p}\, a.$ ∎

Asymptotic behaviour. As usual the best results are obtained for $\dfrac{|X(\mathbb{F}_q)|}{g} \to A$, A being as large as possible (always $A \le \sqrt{q} - 1$).

THEOREM 8.2. *A family of curves over $\mathbb{F}_q$, $q = p^m$, of growing genus g such that $\dfrac{|X(\mathbb{F}_q)|}{g} \to A > \dfrac{2m(p-1)}{p}$ yields an asymptotically good family of p-ary codes such that for any $\delta < \dfrac{p}{m(p-1)} - 2A^{-1}$ there is a subfamily $\{C_n\}$ with $\delta(\{C_n\}) = \delta$ and*

$$R(\{C_n\}) \ge 1 - m\,\frac{p-1}{p}\,(2A^{-1} + \delta)\ . \qquad \blacksquare$$

One easily checks that for $m = 1$ this result is worse than that of Theorem 2.2. The result of Theorem 8.2 can be generalized to p^r-ary codes (just change p by p^r), but the construction using $L_{\mathcal{P},D}$ goes out (cf. [KA/TS]).

9. Remarks and open problems

Here we list some natural remarks and questions, without any particular order.

1. What are the best constants in §4 and §7 ?

2. We have mostly restricted ourselves (in the function field case) to $\mathcal{P} \subseteq X(\mathbb{F}_q)$. All the constructions in fact work for any set of places of K, though places of high degree usually spoil parameters. Can places of higher degree be of any use ?

3. In the number field case we have usually supposed that $S \supseteq S_\infty$. Can we get anything good without this condition ?

4. Each section of this paper was encoded by three or four letters. Formally speaking there are 16 possibilities. What can we say about those we have not mentioned ?

5. In §2 we have an asymptotic equality for λ, and in all the other cases but estimates. What are the true values of λ (asymptotically) ?

6. Can we use "explicit formulae" plus some other considerations to give *lower* bounds of the density exponent of what we are able to get by our constructions ?

7. In the function field case the best families of curves (those with $\frac{|X(\mathbb{F}_q)|}{g} \to \sqrt{q}-1$) are provided by modular curves which form *ramified* towers (the ramification being rather "small"). What are their analogues in the number field case ?

8. The results we have obtained concern packings either in $\mathbb{R}^N$ or in $\mathbb{F}_q^N$. Our constructions also lead to natural lattices in $\mathbb{F}_q((T))^N$ and in products of p-adic fields. What are the correct parameters (how to put the problem) in those cases ?

9. Function field multiplicative lattices can be also constructed starting from curves over any field, provided that we know the finiteness of the subgroup in Jacobian generated by $\mathcal{P}$. Consider modular curves (say, over $\mathbb{C}$) and $\mathcal{P}$ consisting of cusp points which are of finite order (the MANIN-DRINFELD theorem). How to estimate parameters ?

10. What can be done with varieties (over $\mathbb{F}_q$ and arithmetic) of dimension more than 1 ? For example what are the densities of MORDELL-WEIL lattices on abelian varieties ?

11. $K^* = K_1(K)$ and the map we have used in §§4-7 is the regulator map. What can be done with the help of higher regulators on $K_i(K)$?

REFERENCES

[Co/Sl] J.H. CONWAY, N.J.A. SLOANE, *Sphere packings, lattices and groups*, Springer, N.Y., 1988.

[Go 1] V.D. GOPPA, Codes on algebraic curves, *Soviet Math. Dokl.,* **24** (1981), 170-172.

[Go 2] V.D. GOPPA, *Geometry and codes*, Kluwer Acad. Publ., 1988.

[Ka/Ts] G.L. KATSMAN, M.A. TSFASMAN, A remark on algebraic-geometric codes, *Contemp. Math.,* **93** (1989), 197-199.

[La] S. LANG, *Algebraic number theory*, Addison-Wesley, 1970.

[Le] H.W. LENSTRA JR., *Codes from algebraic number fields*, in : Fundamental contributions in the Netherlands since 1945, North-Holland, Amsterdam, v.II (1986), 95-104.

[Li/Ts] S.N. LITSYN, M.A. TSFASMAN, Constructive high-dimensional sphere packings, *Duke Math. J.,* **54** (1987), 147-161.

[Mi] J. MILNOR, *Hilbert's problem 18 : on crystallographic groups, fundamental domains, and on sphere packings*, Proc. Symp. Pure Math., AMS, Providence RI, **28** (1976), 491-506.

[Qu] H.-G. QUEBBEMANN, *Lattices from curves over finite fields*, Preprint, 1989.

[Ro/Ts] M. YU. ROSENBLOOM, M.A. TSFASMAN, Multiplicative lattices in global fields, *Invent. Math.,* **101** (1990), 687-696.

[Sc] A. SCHINZEL, On the product of the conjugates outside the unit circle of an algebraic number, *Acta Arithm.,* **24** (1973), 385-399. Addendum, *Acta Arithm.,* **26** (1975), 329-331.

[Ts/Vl] M.A. TSFASMAN, S.G. VLĂDUŢ, *Algebraic-geometric codes*, Kluwer Acad. Publ., 1990.

[Ts/Vl/Zi] M.A. TSFASMAN, S.G. VLĂDUŢ, TH. ZINK, Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound, *Math. Nachr.,* **109** (1982), 21-28.

M.A. TSFASMAN
Institute for Problems
of Information Transmission
19, Ermolovoi st.
MOSCOW 101447
U.S.S.R.