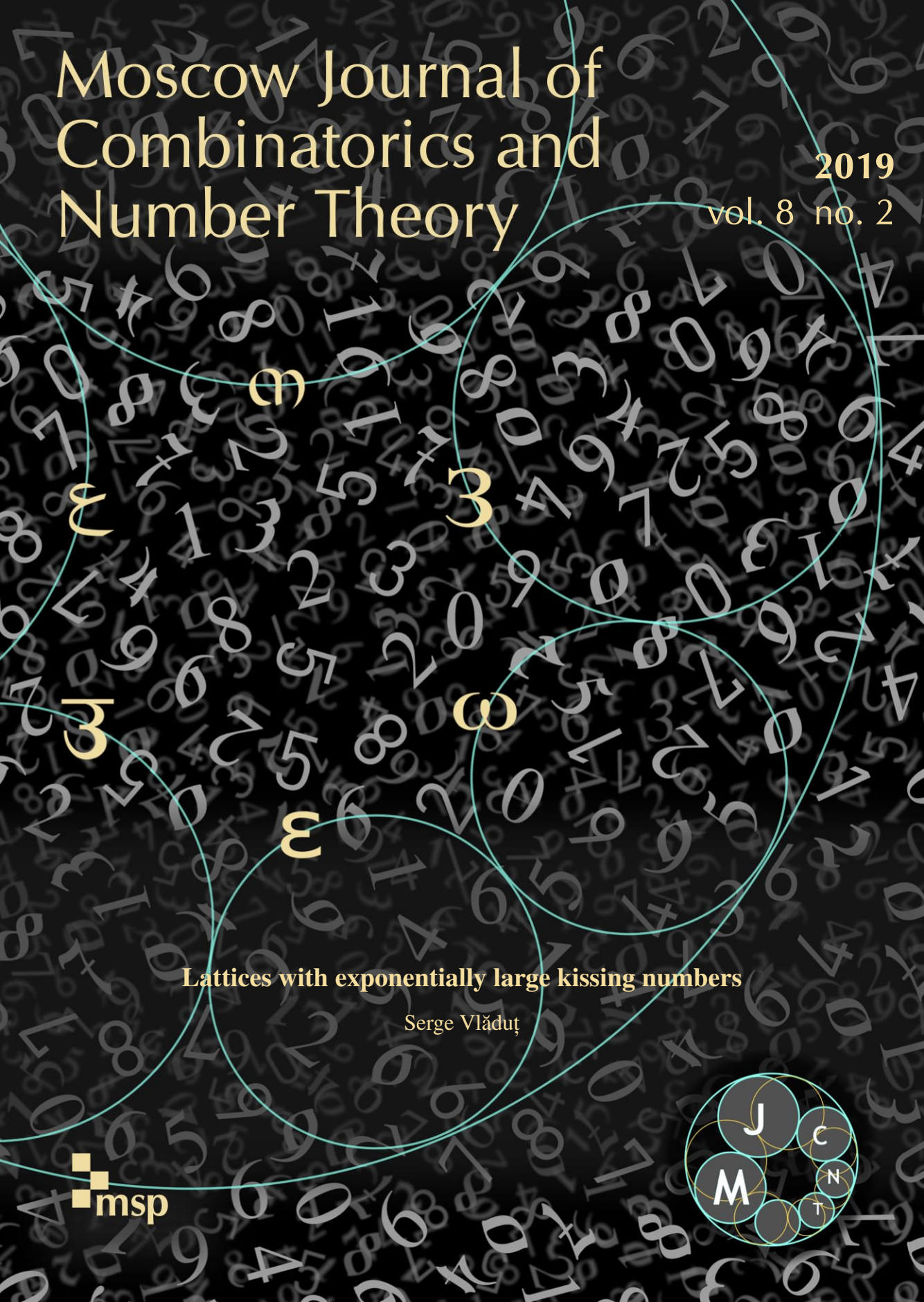
Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 2



Lattices with exponentially large kissing numbers

Serge Vlăduț

msp

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 2, 2019
dx.doi.org/10.2140/moscow.2019.8.163

Lattices with exponentially large kissing numbers

Serge Vlăduț

We construct a sequence of lattices $\{L_{n_i} \subset \mathbb{R}^{n_i}\}$ for $n_i \to \infty$ with exponentially large kissing numbers, namely, $\log_2 \tau(L_{n_i}) > 0.0338 \cdot n_i - o(n_i)$. We also show that the maximum lattice kissing number τ_n^l in n dimensions satisfies $\log_2 \tau_n^l > 0.0219 \cdot n - o(n)$ for any n.

1. Introduction

In this paper we consider lattice packings of spheres in real n-dimensional space $\mathbb{R}^n$ and their kissing numbers. Recall that the maximum kissing number is known only in a handful of dimensions, the largest being $n = 24$ for which the Leech lattice Λ_{24} gives the optimal kissing number $\tau(\Lambda_{24}) = 196560$. Recall also that the random choice procedure guarantees, see [Chabauty 1953; Shannon 1959; Wyner 1965], the existence of nonlattice packings P_n with

$$\frac{\log_2 \tau(P_n)}{n} \geq \log_2 \frac{2}{\sqrt{3}} \simeq 0.2075\ldots.$$

More precisely, it gives the existence of local arrangements of spheres touching one sphere which can be included then into a nonlattice packing. Note also that the upper bound of Kabatiansky and Levenstein [1978] is

$$\frac{\log_2 \tau(P_n)}{n} \leq 0.4041\ldots.$$

However, for lattice packings this procedure does not work, and as far as we know, no reasonable lower bound for the maximum lattice kissing number τ_n^l is known for $n \to \infty$. For instance, the Barnes–Wall lattices BW_n with $n = 2^m$ give the quasipolynomial bound $\tau_n^l \geq n^{c \log n}$, i.e., $\log \tau_n^l \geq c \log^2 n$, which can hardly be characterized as "reasonable". The main purpose of the present paper is to give an exponential lower bound for τ_n^l (however, these lattices are worse than nonlattice packing guaranteed by random choice). This is achieved by applying Constructions D and E from [Barnes and Sloane 1983] and [Bos et al. 1982], respectively, to codes from [Ashikhmin et al. 2001] having exponentially many light vectors. In order to apply Constructions D and E we need specific good curves (the curves in the Garcia–Stichtenoth towers [1995; 1996] do not perfectly match our construction) and some Drinfeld modular curves [Gekeler 2001; Elkies 2001] perfectly suit our purposes.

Our main result is:

MSC2010: 11H31, 11H71, 14G15, 52C17.
Keywords: lattices, algebraic geometry codes, kissing numbers, Drinfeld modular curves.

Theorem 1.1. *We have*

$$\frac{\log(\tau_N^l)}{N} \geq \tfrac{1}{20}\big(1-\tfrac{2}{31}\log 33\big) - \frac{2+2\log N}{N} \tag{1-1}$$

for $N = 5\cdot 2^{10n+2}$ *and any* $n \geq 2$,

$$\frac{\log(\tau_N^l)}{N} \geq \tfrac{1}{24}\big(1-\tfrac{2}{63}\log 65\big) - \frac{2+2\log N}{N} \tag{1-2}$$

for $N = 3\cdot 2^{12n+3}$ *and any* $n \geq 2$,

$$\frac{\log(\tau_N^l)}{N} \geq \tfrac{1}{28}\big(1-\tfrac{2}{127}\log 129\big) - \frac{2+2\log N}{N} \tag{1-3}$$

for $N = 7\cdot 2^{14n+2}$ *and any* $n \geq 2$, *where*

$$\tfrac{1}{20}\big(1-\tfrac{2}{31}\log 33\big)\simeq 0.033727\ldots, \quad \tfrac{1}{24}\big(1-\tfrac{2}{63}\log 65\big)\simeq 0.033700\ldots, \quad \tfrac{1}{28}\big(1-\tfrac{2}{127}\log 129\big)\simeq 0.0317709\ldots.$$

All our logarithms are binary.

Corollary 1.2. *We have*

$$\frac{\log(\tau_n^l)}{n} \geq c_0 \tag{1-4}$$

for some $c_0 > 0$ *and any* $n \geq 1$.

The exact value of c_0 is not clear, but $c_0 = 0.02$ is probably sufficient.

It is possible to ameliorate the constants slightly, if we do not insist on the effectiveness of results:

Theorem 1.3. *We have*

$$\frac{\log(\tau_N^l)}{N} \geq \tfrac{1}{20}\big(\tfrac{21}{31} - \log\tfrac{1024}{1023}\big) - o(1) \simeq 0.033800\ldots - o(1) \tag{1-5}$$

for $N = 5\cdot 2^{10n+2}$,

$$\frac{\log(\tau_N^l)}{N} \geq \tfrac{1}{24}\big(\tfrac{17}{21} - \log\tfrac{4096}{4095}\big) - o(1) \simeq 0.033715\ldots - o(1) \tag{1-6}$$

for $N = 3\cdot 2^{12n+3}$,

$$\frac{\log(\tau_N^l)}{N} \geq \tfrac{1}{28}\big(\tfrac{113}{127} - \log\tfrac{16384}{16383}\big) - o(1) \simeq 0.031774\ldots - o(1) \tag{1-7}$$

for $N = 7\cdot 2^{14n+2}$.

In fact, the implied functions in $o(1)$ terms can be made explicit, but they decrease slowly and their precise calculation is not justified.

Note also that using other finite fields $\mathbb{F}_q$ with a square q one can obtain infinitely many series of similar lattices in the corresponding dimensions, but for all of them the ratio $\log(\tau_N^l)/N$ is less than 0.03.

Corollary 1.4. *We have*

$$\limsup_{n\to\infty} \frac{\log(\tau_n^l)}{n} \geq \tfrac{1}{20}\big(\tfrac{21}{31} - \log\tfrac{1024}{1023}\big).$$

For the lower limit we can prove:

Theorem 1.5. *Let* $A = \log \frac{4096}{4095}$. *We have then*

$$\lim \inf_{n\to\infty} \frac{\log(\tau_n^l)}{n} \geq \tfrac{1}{504}(17 - 21A)\delta_0 \simeq 0.021937\ldots, \tag{1-8}$$

where $\delta_0 \simeq 0.6506627\ldots$ *is the unique root of the equation*

$$21H(\delta) = 2\delta(4 + 21A + (17 - 21A)\delta)$$

in the interval (0.5, 1).

One can think that c_0 in (1-4) can be chosen rather close to that value.

The rest of the paper is organized as follows: in Section 2 we recall some basic definitions and results on lattices and error-correcting codes. Section 3 is devoted to Constructions D and E from [Barnes and Sloane 1983] and [Bos et al. 1982], respectively, while Section 4 recalls and slightly modifies the constructions from [Ashikhmin et al. 2001]. We describe some known good curve families in Section 5 and prove our results in Section 6.

2. Preliminaries

In this section we recall some basic definitions and results on lattices and linear error-correcting codes.

2A. ***Lattice packings.*** A sphere packing is a configuration of nonintersecting equal open spheres in $\mathbb{R}^N$. Let d be the diameter of the spheres; then the distance between any two sphere centers is at least d. Thus a packing is a set of points P in $\mathbb{R}^N$ such that the minimum distance between any two of them is at least d. If P is an additive subgroup of $\mathbb{R}^N$, it is called a lattice or a lattice packing; below we are concerned mainly with such packings. For any packing P its density $\Delta(P)$ is defined as the fraction of space covered by spheres (which can be defined as the upper limit of this fraction inside a large cube whose size tends to infinity).

If L is a lattice then a choice of basis gives an embedding $e_L : \mathbb{Z}^n \to \mathbb{R}^n$; its matrix is called a generating matrix of the lattice. For the diameter of spheres one can take $d(L) = \min\{|v| : v \in L, v \neq 0\}$. For any packing $P \subset \mathbb{R}^n$ the ratio $\nu(P) = \Delta(P)/V_n$ is called its center density, where

$$V_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)}$$

is the volume of the unit sphere.

The ratio $\lambda(P) = \log \Delta(P)/n$ is called the density exponent of P; thus, $\Delta(P) = 2^{-\lambda(P)n}$. The Minkowski bound, which is a corollary of the Minkowski–Hlawka theorem, says that some lattice families $\{L_n \subset \mathbb{R}^n\}$ satisfy $\lambda(L_n) \leq 1$; however, no construction is known for such families. On the other hand, the Kabatiansky–Levenstein bound says that $\lambda(P_n) \geq 0.599\ldots - o(1)$ for any family of packings $\{P_n \subset \mathbb{R}^n\}$. Families of packings with $\liminf_{n\to\infty} \lambda(P_n) < \infty$ are called *asymptotically good.* It is not easy to construct such families, especially for lattice packings. The best known results in that direction use algebraic geometry codes and similar constructions; see [Litsyn and Tsfasman 1987; Rosenbloom and Tsfasman 1990].

Another important parameter of a packing $P \subset \mathbb{R}^n$ is its kissing number

$$\tau(P) = \max_{x \in P} |\{y \in P : |x - y| = d\}|.$$

A random choice argument gives, see [Chabauty 1953; Shannon 1959], the existence of (nonlattice) packings $P_n \subset \mathbb{R}^n$ with

$$\liminf_{n\to\infty} \frac{\log \tau(P_n)}{n} \geq \log \frac{2}{\sqrt{3}} \simeq 0.2075\ldots,$$

whereas the Kabatiansky–Levenstein bound [1978] for τ says that

$$\limsup_{n\to\infty} \frac{\log \tau(P_n)}{n} \leq 0.4041\ldots.$$

We will say that a family of packings $P_n \subset \mathbb{R}^n$ is *τ-asymptotically good* whenever

$$\limsup_{n\to\infty} \frac{\log \tau(P_n)}{n} > 0.$$

Since the random choice argument does not work for lattices, it is not clear whether τ-asymptotically good lattice families exist, and our main purpose is to prove their existence.

2B. ***Error-correcting codes.*** Let us recall several facts about (linear error-correcting) codes; for additional information we refer to [MacWilliams and Sloane 1977a; 1977b]; see also [Tsfasman et al. 2007, Chapter 1]. We fix a finite field $\mathbb{F}_q$.

A q-ary linear code is simply a subspace $C \subseteq \mathbb{F}_q^n$, where n is called the length of C, and the ratio $R = k/n$ for $k = \dim C$ is called the rate of C. The minimum distance $d = d(C)$ is the minimum Hamming weight $\mathrm{wt}(c)$, i.e., the number of nonzero coordinates, of $c \in C \setminus \{0\}$; the ratio $\delta = d/n$ is called the relative minimum distance. We say in this case that C is an $[n, k, d]_q$-code. A choice of basis in C defines a linear map $\varphi_C : \mathbb{F}_q^k \to \mathbb{F}_q^n$ and its matrix is called a generating matrix of C. A set of codes $C_1 \subset \cdots \subset C_m \subseteq \mathbb{F}_q^n$ is called a nested family. For $C \subseteq \mathbb{F}_q^n$ its dual code $C^\perp$ is the orthogonal complement of C:

$$C^\perp = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ for all } c \in C\},$$

where $v \cdot c = v_1c_1 + \cdots + v_nc_n$; $C^\perp$ is an $[n, n-k, d^\perp]_q$-code for some $d^\perp$.

A random choice argument shows that asymptotically for $n \to \infty$ and fixed δ the rate R of the best linear codes satisfies the Gilbert–Varshamov bound

$$R = R_q(\delta) \geq 1 - H_q(\delta) = 1 - \frac{\delta \log(q-1) + H(\delta)}{\log q},$$

where $H(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$ is the binary entropy function.

2C. ***Algebraic geometry codes.*** All our curves here and below are smooth projective absolutely irreducible over a finite field $\mathbb{F}_q$; let X be such a curve of genus g, let D be an $\mathbb{F}_q$-rational divisor of degree $a \geq g - 1$, and let, see, e.g., [Tsfasman et al. 2007, Section 2.2],

$$L(D) = \{f \in \mathbb{F}_q(X) : (f) + D \geq 0\}$$

be the associated function space. For a set $\mathcal{P}=\{P_1,\dots,P_n\}$ of $\mathbb{F}_q$-rational points on X with $\mathcal{P}\cap\operatorname{Supp} D=\varnothing$ the evaluation map

$$\mathrm{ev}_{\mathcal{P}} : L(D)\to\mathbb{F}_q^n,\quad \mathrm{ev}_{\mathcal{P}}(f)=(f(P_1),\dots,f(P_n)),$$

is well-defined. Whenever $a<n$, this map is injective and its image is a linear q-ary code $C(X,D,\mathcal{P})$ of length n, dimension $k\ge a-g+1$ (by the Riemann–Roch theorem), and distance $d>n-a$ (since the number of zeros of a function cannot exceed the number of poles). If $D=aP_0$ for an $\mathbb{F}_q$-rational point $P_0\ne P_i,\ i=1,\dots,n$, we get a nested family of codes C_a for $a=n-1,n-2,\dots,g-1$. In the particular case $g=0,\ a\ge 0,\ P_0=\infty$ (i.e., X is the projective line), we get nested Reed–Solomon codes with parameters $n=q,\ k=a+1,\ d=q-a$.

Algebraic geometry codes (AG-codes below) have good parameters when the ratio of the number of $\mathbb{F}_q$-rational points on the curve to its genus is high enough. The Drinfeld–Vlăduţ bound says that asymptotically this ratio cannot exceed $\sqrt{q}-1$. For $q=p^{2h}$ there exist many families of curves over $\mathbb{F}_q$ attaining this bound (see, e.g., Section 5 below), which implies the lower bound

$$R_q(\delta)\ge 1-\frac{1}{\sqrt{q}-1}$$

for the best asymptotical rate of $\mathbb{F}_q$-linear codes; see, e.g., [Tsfasman et al. 2007, Section 4.5]. If $q\ge 49$, it improves (on some interval) the Gilbert–Varshamov bound.

One can dispense with the above condition $\mathcal{P}\cap\operatorname{Supp} D=\varnothing$ without spoiling the parameters of the codes $C(X,D,\mathcal{P})$; for instance, if $P_i\in\operatorname{Supp} D$ we can replace the term $f(P_i)$ in $\mathrm{ev}_{\mathcal{P}}$ by $f_i(P_i)$ with $f_i=t_i^s f$, where t_i is some fixed local parameter at P_i and s is a suitable integer (see [Tsfasman et al. 2007, Section 4.1, pp. 194–197], where the H- and P-constructions are discussed).

3. Constructions D and E

We recall now two constructions from [Barnes and Sloane 1983] and [Bos et al. 1982] (see also Chapter 8 in [Conway and Sloane 1988]), which permit us to construct good lattices from good codes.

3A. ***Construction D.*** Let $C_0=\mathbb{F}_2^n\supset C_1\supset\cdots\supset C_a$, $a\ge 1$ be a finite decreasing family of linear binary codes with parameters $[n,k_i,d_i]$ for $C_i,\ i=0,\dots,a$, where $d_i=4^i$ (we will need only the case $n=2^{2a+1}$ and thus $\delta_a=d_a/n=\frac{1}{2}$). We can and will consider C_0 as a subset of $\mathbb{R}^n$. We choose a basis $c_1,\dots,c_n$ for $\mathbb{F}_2^n$ such that $c_1,\dots,c_{k_i}$ span C_i for $i=0,\dots,a$ and define L as the lattice in $\mathbb{R}^n$ generated by $(2\mathbb{Z})^n$ and the vectors $\{c_j\cdot 2^{1-i}\}$ for $i=1,\dots,a,\ k_{i+1}+1\le j\le k_i$. Then we have [Barnes and Sloane 1983, Theorem 1]:

Proposition 3.1. *The lattice L has minimum distance $d_L=2$ and its center density satisfies*

$$\delta\ge 2^{K-n}$$

for $K=\sum_{i=1}^a k_i$.

Note that we will need only the statement $d_L=2$, which is easy in view of the minimum distances d_i of C_i for $i=0,\dots,a$.

3B. ***Construction E.*** Here we need more elaborate techniques.

First we define T-lattices as follows [Barnes and Sloane 1983; Bos et al. 1982]; see also [Litsyn and Tsfasman 1987]. A lattice $\Lambda \subset \mathbb{R}^m$ is a *T-lattice* if it satisfies the following four conditions:

(i) The minimal vectors of Λ span Λ.

(ii) There is a linear map T from $\mathbb{R}^m$ to $\mathbb{R}^m$ that sends all the minimal vectors of Λ into elements of Λ which have norm R^2 and are at a distance R from Λ for some $R > 0$.

(iii) There is a positive integer ν dividing m and an element $A \in \mathrm{Aut}(\Lambda)$ such that

(iii)$_1$ $T^\nu = \frac{1}{2}A$ and

(iii)$_2$ $\frac{1}{2}(A^2 - A) = \sum_{i=0}^{\nu-1} a_i T^i$, $a_i \in \mathbb{Z}$.

We set $b = m/\nu$ and $q = 2^b$.

(iv) $\Lambda \subseteq T\Lambda$ and

(iv)$_1$ $[T\Lambda : \Lambda] = q$.

It follows from (iii)$_1$ that $T = tP$, where $t = 2^{1/\nu}$ and P is an orthogonal transformation satisfying $P^\nu = A$. If M is the minimal square norm of Λ, we have $t = R/\sqrt{M}$, and from (iv)$_1$ we get

(v) $t^m = |\det T| = 2^{-b} = q^{-1}$.

Note that the square lattice $\mathbb{Z}^2$ is a T-lattice with $T = (1/\sqrt{2})R_{\pi/4}$ for the rotation $R_{\pi/4}$ through the angle $\pi/4 = 45°$.

Construction E produces from a T-lattice, together with a nested family of linear codes $C_0 = \mathbb{F}_{2^b}^n \supset C_1 \supset \cdots \supset C_a$ over $\mathbb{F}_{2^b}$, another T-lattice $L \subset \mathbb{R}^{mn}$ in the following way.

We suppose that the parameters of the code C_i, $0 \le i \le a$ are $[n, k_i, d_i]$ and we choose a basis $c_1, \ldots, c_n$ for $\mathbb{F}_{2^b}^n$ such that $c_1, \ldots, c_{k_i}$ span C_i for $i = 0, \ldots, a$. Define then the lattices Λ_i as follows. Let $v_i, \ldots, v_m$ be minimal vectors of Λ that span Λ. Then $Tv_i, \ldots, Tv_m$ span $T\Lambda$ and $T\Lambda/\Lambda$ is an elementary abelian group of order q, so that there are b vectors $u_i^{(1)} = Tv_{r_1}, \ldots, u_b^{(1)} = Tv_{r_b}$, for appropriate $r_1, \ldots, r_b$, such that $T\Lambda/\Lambda$ is isomorphic to the $\mathbb{F}_2$-span of $u_i^{(1)}, \ldots, u_b^{(1)}$. Let

$$\Lambda_i = T^i\Lambda, \qquad u_j^{(i)} = T^i v_{r_j}, \quad j = 1, \ldots, b, \qquad \text{for all } i \in \mathbb{Z}.$$

The lattice Λ_i has minimal square norm $t^{2i}M$, and $\mathrm{dist}(u_i^{(1)}, \Lambda_i) \ge t^{i-1}R$.

Define now the maps $\sigma_i : \mathbb{F}_q \to \Lambda_i$ by

$$\sigma_i\left(\sum_{j=1}^{b} \alpha_j \omega_j\right) = \sum_{j=1}^{b} \alpha_j u_j^{(i)}$$

for some generators $\omega_1, \ldots, \omega_b$ for $\mathbb{F}_q$ over $\mathbb{F}_2$ and any $\alpha_j \in \mathbb{F}_2$, $j = 1, \ldots, b$; those maps define the maps $\sigma_i : \mathbb{F}_q^n \to \mathbb{R}^{mn}$.

The construction. The lattice $L \subset \mathbb{R}^{mn}$ consists of all vectors of the form

$$x = l + \sum_{i=1}^{a} \sum_{j=1}^{bk_i} \alpha_j^{(i)} \sigma_i(c_j)$$

for $l \in \Lambda^n$, $\alpha_j^{(i)} \in \mathbb{F}_2$. Note that L is a T-lattice, since it inherits T from Λ; the parameter t remains the same, while b becomes nb; see also Proposition 3.2 below. The main property of this Construction E, which coincides with Construction D for $\Lambda = 2\mathbb{Z}$, is [Barnes and Sloane 1983, Theorem 3]:

Proposition 3.2. *The lattice L is fixed under the transformation $\hat{A}$, which applies A simultaneously to each component, and its minimum distance equals*

$$\sqrt{\overline{M}} \quad \text{for } \overline{M} = \min_{i=1,\dots,a} \{M, d_i R^{2i} M^{1-i}\}.$$

Theorem 3 of [Barnes and Sloane 1983] gives also the density of L, but we do not need it.

Applying Construction E to $\mathbb{Z}^2$ with $a = 1$, $M = 4$, $R = \sqrt{2}$ and the single parity check $[2, 1, 2]_q$ code C_1, we get successfully the T-lattices D_4, E_8, Λ_{16}, $\bar{\Lambda}_{32}$ in the corresponding dimensions; one can take this description as a definition for those lattices. Moreover, applying Construction E to D_4 and the single parity check $[m, m-1, 2]_4$ code for any $m \geq 2$ we get a T-lattice $\tilde{\Lambda}_{4m}$ in $4m$ dimensions. The Leech lattice Λ_{24} is also a T-lattice [Bos et al. 1982, p. 177]; note, however that $\Lambda_{24} \neq \tilde{\Lambda}_{24}$.

4. Codes with many light vectors

Recall the following principal result of [Ashikhmin et al. 2001].

Denote by A_d is the number of minimum weight vectors in an $[n, k, d]_q$-code C_n, and let E_s for $s \in \mathbb{N}$, $s \geq 3$ be the function

$$E_s(\delta) = H(\delta) - \frac{2s}{2^s - 1} - \log \frac{2^{2s}}{2^{2s} - 1}, \tag{4-1}$$

which has two zeros $0 < \delta_1 < \delta_2 < 1 - 2^{-2s}$ and is positive for $\delta_1 < \delta < \delta_2$. In particular, for $s = 3$, $q = 64$, $\delta = \frac{1}{2}$ we have

$$E_3(0.5) = \tfrac{1}{7} - \log \tfrac{64}{63} \simeq 0.1201\ldots, \qquad \tfrac{1}{64} E_3(0.5) \simeq 0.001877\ldots.$$

Theorem 4.1. *Let $q = 2^{2s}$, $s = 3, 4, \ldots$ be fixed. Then for any $\delta_1 < \delta < \delta_2$ there exists a sequence of binary linear codes $\{C_n\}$ of length $n = qN$, $N \to \infty$ and distance $d_n = n\delta/2$ such that*

$$\frac{\log A_{d_n}}{n} \geq \frac{E_s(\delta)}{2^s} - o(1). \tag{4-2}$$

Theorem 4.1 is a simple consequence of the following result concerning AG codes. Consider a curve X of genus g over $\mathbb{F}_q$, where $q = 2^{2s}$, $s \geq 3$. Suppose that $N \geq (2^s - 1)g$, where $N = |X(\mathbb{F}_q)|$ is the number of $\mathbb{F}_q$-rational points of X (e.g., X is a curve from Subsections 5A, 5B below). Let D be an $\mathbb{F}_q$-rational positive divisor of degree $a > 0$, and let $C = C(X, D, X(\mathbb{F}_q))$ be the corresponding AG code of length N, dimension $k(C) \geq a - g + 1$, and distance $d(C) \geq N - a$.

Proposition 4.2. *Let $\delta = (N - a)/N$ satisfy the inequality $\delta_1 < \delta < \delta_2$. Then there exists an $\mathbb{F}_q$-rational positive divisor with $\deg(D) = a$ such that the corresponding AG code C has the minimum distance $d = N - a = \delta N$ and for the number A_d of vectors of weight d we have*

$$\log A_d \geq N E_s(d) - o(N).$$

Recall that this is proved using an averaging procedure applied to the set of linearly equivalent classes of $\mathbb{F}_q$-rational positive divisors D with $\deg(D) = a$ which form the set $J_X(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on the Jacobian J_X of X. This result is based on the estimate

$$\frac{\log |J_X(\mathbb{F}_q)|}{g} = q + (\sqrt{q} - 1) \log \frac{q}{q-1} + o(1). \tag{4-3}$$

In order to deduce Theorem 4.1 from Proposition 4.2 we take the binary simplex code, that is, the linear code dual to the $[n = q - 1, n - 2s, 3]$ Hamming code and lengthen each vector of this simplex code by a zero coordinate. This gives a binary linear $[q, 2s, q/2]$-code C_0 in which every nonzero vector has Hamming weight $q/2$. Using then a linear bijection $\varphi : \mathbb{F}_q \to C_0$ and replacing every coordinate by its image, we obtain from $C(D)$ a linear binary code C_n in Theorem 4.1.

Remark. Proposition 4.2 is valid for any even prime power $q \geq 49$, but we do not use this below. Note also that its proof guarantees in general only the existence of *one* divisor class D satisfying the conclusion (and not of exponentially many such divisor classes); however, when the bound is strictly bigger than $k(C)$, we get exponentially many such divisor classes in $J_X(\mathbb{F}_q)$.

Effective version. Note that at the expense of a small decline in parameters the above estimate can be made completely explicit, namely, we have:

Theorem 4.3. *Let $q = p^h$ be a prime power, let X be a curve of genus g over $\mathbb{F}_q$, let $S \subseteq X(\mathbb{F}_q)$, $|S| = N$, and let $a \in \mathbb{N}$ with $1 \leq a \leq N - 1$. Then there exists an $\mathbb{F}_q$-rational positive divisor $D \geq 0$, $\deg(D) = a$, such that the corresponding AG code $C = C(X, D, S)$ has the minimum distance $d = N - a = \delta N$ and we have*

$$A_d \geq \frac{\binom{N}{a}}{(\sqrt{q} + 1)^{2g}}.$$

The proof simply replaces the asymptotic inequality (4-3) by a simpler effective inequality

$$|J_X(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g}.$$

Applying Stirling's formula, we get:

Corollary 4.4. *We have*

$$\frac{\log A_d}{N} \geq H(\delta) - \frac{2g}{N} \log(\sqrt{q} + 1) - \frac{\log(2\pi ad)}{2N} - \frac{1}{12ad}.$$

In particular, if $N = 2a = 2d \geq (\sqrt{q} - 1)g$, then

$$\frac{\log A_d}{N} > 1 - \frac{2 \log(\sqrt{q} + 1)}{\sqrt{q} - 1} - \frac{2 + 2 \log N}{N}.$$

Note, that Theorem 4.3 and Corollary 4.4 are applicable, e.g., for $g = 0$, where we get an estimate for the Reed–Solomon codes.

5. Some good families of curves

We recall now some constructions of curves over $\mathbb{F}_q$ with many rational points. Let q be a prime power (we will be interested only by the case $q = p^{2h}$), and let

$$N_q(g) := \max\{|C(\mathbb{F}_q)| : C \text{ is a curve of genus } g \text{ over } \mathbb{F}_q\}.$$

Define then

$$A(q) := \lim_{g\to\infty} \sup \frac{N_q(g)}{g} \le \sqrt{q} - 1, \quad A^-(q) := \lim_{g\to\infty} \inf \frac{N_q(g)}{g}$$

as the corresponding upper and lower asymptotic quantities. We begin with some families attaining the bound for $A(q)$ (the Drinfeld–Vlăduț bound).

5A. ***Garcia–Stichtenoth tower.*** The tower X_n, $n = 1, 2, \ldots$, from [Garcia and Stichtenoth 1996] is defined recursively by the equations

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1} \quad \text{for } i = 1, \ldots, n-1. \tag{5-1}$$

Therefore, the function field $T_n := \mathbb{F}_{q^2}(X_n)$ of the curve X_n is given by $T_n = \mathbb{F}_{q^2}(x_1, \ldots, x_n)$, where x_i, $i = 1, \ldots, n$, are related by (5-1). The main result of [Garcia and Stichtenoth 1996] gives the parameters of that tower.

Theorem 5.1. *We have for the genus* $g_n = g(X_n)$

$$g_n = (q^m - 1)^2 \qquad \text{for } n = 2m,$$
$$g_n = (q^m - 1)(q^{m-1} - 1) \quad \text{for } k = 2m - 1,$$

and the number $N(n) = |X_n(\mathbb{F}_{q^2})|$ *of* $\mathbb{F}_{q^2}$*-rational points of* X_n *satisfies*

$$N(n) \ge (q-1)q^n.$$

Let us then describe an optimal tower of Drinfeld curves closely related to the tower X_n.

5B. ***Drinfeld modular curves.*** The general reference for Drinfeld modular curves is [Gekeler 1986], but we use a particular case from [Elkies 2001]; see also [Gekeler 2001].

A tower of Drinfeld curves. For any field $L \supseteq \mathbb{F}_q$, we denote by $L\{\tau\}$ the noncommutative L-algebra generated by τ and satisfying the relation $\tau a = a^q \tau$ for all $a \in L$. Let $A = \mathbb{F}_q[T]$; then a rank-2 Drinfeld module φ over A is an $\mathbb{F}_q$-algebra homomorphism from A to $L\{\tau\}$ such that

$$\varphi(T) = l_0 + l_1\tau + l_2\tau^2 = l_0 + g\tau + \Delta\tau^2 \in L\{\tau\}, \tag{5-2}$$

with nonzero *discriminant* $\Delta = \Delta(\varphi)$. The map $\gamma : A \to L$ taking any $a \in A$ to the constant term of a is a ring homomorphism; thus, $\gamma(T) = l_0$ in (5-2).

If φ, ψ are two Drinfeld modules, an isogeny from φ to ψ is an element $u \in \bar{L}\{\tau\}$ such that

$$u \circ \varphi_a = \psi_a \circ u$$

for all $a \in A$, and its kernel is the A-submodule of $\bar{L}$ given by

$$\ker(u) := \{x \in \bar{L} : u(x) = 0\},$$

which is of finite dimension over $\mathbb{F}_q$ unless $u = 0$. In particular, if $u = \varphi_a$ then u is an isogeny from φ to itself, called multiplication by a, and its kernel is isomorphic with $(A/aA)^2$ as an A-module for $\gamma(a) \neq 0$; elements of $\ker(a)$ are called a-torsion points of φ. If γ is not injective then $\ker \gamma = Ab$ for

some irreducible $b \in A$; φ is then said to be supersingular if $\ker(b) = \{0\}$, and for $\deg(b) = 1$ we have $\varphi_b = g\tau + \Delta\tau^2$ and φ_b is supersingular if and only if $g = 0$. An isomorphism between Drinfeld modules is simply an element $u \in \bar{L}^*$, and it multiplies each coefficient l_i in (5-2) by u^{1-q^i}. Let

$$J(\varphi) = \frac{g^{q+1}}{\Delta}.$$

Then φ and ψ with the same γ are isomorphic over $\bar{L}$ if and only if $J(\varphi) = J(\psi)$. Thus, we can refer to the J-line as the Drinfeld modular curve $X(1)$ for a given γ. Moreover, for $N \in A$ with $\gamma(N) \neq 0$, we have Drinfeld modular curves $X_0(N)$ parametrizing Drinfeld modules with a choice of torsion subgroup $G \simeq A/NA$ (and fixed γ). If $\gamma(T) \in \mathbb{F}_q$, we may regard the curves $X(1)$ and $X_0(N)$ as the "reduction mod $(T - \gamma(T))$" of the corresponding modular curves for $\gamma(T) = T$. Below we suppose that $\gamma(T) = 1$ and we say that a point on $X_0(N)$ is supersingular if the corresponding Drinfeld module is supersingular; such points are $\mathbb{F}_{q^2}$-rational.

Let us consider the case $N = T^{k+1}$; for the curve $\widetilde{X}_k := X_0(T^{k+1})$ of genus $\tilde{g}_k = g(\widetilde{X}_k)$ we have [Gekeler 2001, Example 10.2]

$$\begin{aligned}
\tilde{g}_k &= \frac{(q^m-1)^2}{q-1} && \text{for } k = 2m,\\
\tilde{g}_k &= \frac{(q^{m+1}-1)(q^m-1)}{q-1} && \text{for } k = 2m+1,\\
\widetilde{N}(k) &= \left|\widetilde{X}_k(\mathbb{F}_{q^2})\right| \geq q^k + 4 && \text{for } k \geq 2;
\end{aligned}$$

thus,

$$\widetilde{N}(k) \geq (q-1)\tilde{g}_k \quad \text{for } k \geq 2$$

and the number of supersingular points on $\widetilde{X}_k$ equals q^k.

Elkies [2001] proved that the function field $\widetilde{K}_k = \mathbb{F}_q(\widetilde{X}_k)$, $k \geq 2$, is given by

$$\widetilde{K}_k = \mathbb{F}_q(x_1, \ldots, x_k) \quad \text{with } x_{j+1}(x_{j+1}+1)^{q-1}(x_j+1)^{q-1} = x_j^q,\ j = 1, \ldots, k-1,$$

and the set of q^k supersingular points of $\widetilde{X}_k(\mathbb{F}_{q^2})$ is determined by the conditions $\Phi_{q+1}(x_j) = 0$ for $j = 1, \ldots, k$, where $\Phi_{q+1}(t) = (t^{q+1}-1)/(t-1)$.

Note also that the Garcia–Stichtenoth curve X_n is a cyclic covering of $\widetilde{X}_n$ of degree $q+1$, but we do not need this fact.

More general Drinfeld curves. We will need also more general Drinfeld modular curves which do not form a tower and as yet have no explicit equations. However, the family of those curves is optimal and their genera are explicitly known [Gekeler 2001]. Let M be a monic element of A with $M(1) \neq 0$, $\deg M \geq 3$, and let $M = \prod_{i=1}^s P_i^{r_i}$ be its prime factorization; thus each $P_i \in A$ is a monic irreducible polynomial of degree l_i and $r_i \geq 1$ for $1 \leq i \leq s$. We put $q_i := q^{l_i}$ and define the arithmetic functions

$$\varepsilon = \varepsilon(M) = \prod_{i=1}^s q_i^{r_i-1}(q_i+1), \quad \kappa = \kappa(M) = \prod_{i=1}^s (q_i^{[r_i/2]} + q_i^{[(r_i-1)/2]}).$$

Consider the curve $\widetilde{X}_0(M)$ over $\mathbb{F}_q$ which is the Drinfeld modular curve $X_0(M)$ with $\gamma(T)=1$. We have then [Gekeler 1986, Sections 8–10]:

Proposition 5.2. *Suppose that at least one degree l_i is odd. Then*:

(i) *The curve $\widetilde{X}_0(M)$ is smooth of genus $g_0(M)$ given by*

$$g_0(M) = 1 + \frac{\varepsilon - (q+1)\kappa - 2^{s-1}(q+1)(q-2)}{q^2-1} \le \frac{\varepsilon}{q^2-1}.$$

(ii) $$|\widetilde{X}_0(M)(\mathbb{F}_{q^2})| \ge \frac{\varepsilon}{q+1} \ge (q-1)g_0(M).$$

Therefore, for any sequence M_i with $\deg(M_i)\to\infty$ the family $\widetilde{X}_0(M_i)$ is asymptotically optimal over $\mathbb{F}_{q^2}$.

5C. ***Curves of every genus with many points.*** Note the genera of curves in Subsections 5A–5B are of a special form and thus they give no estimate for the quantity $A^-(q)$ measuring the maximal number of points on curves of every genus. However, in [Elkies et al. 2004] it was shown that $A^-(q)\ge c\log q$ for any prime power q and a positive constant c. Moreover, for an even square q the result gets much better:

Theorem 5.3. *For $q=2^{2h}$ we have*

$$A^-(q) \ge \frac{\sqrt{q}-1}{2+1/\log q} = \frac{2^h-1}{2+1/(2h)}.$$

Thus $A^-(q)$ is, roughly speaking, only half as small as $A(q)$; a similar result holds also for the odd squares.

6. Proofs

We begin with an easy construction which gives a small positive constant lower bound for the ratio $\log(\tau_n^l)/n$, ensuring thus the existence of τ-asymptotically good lattice families. Indeed, let us take $N=2^{K+1}$, $d=a=N/2=2^K$ for some $K\ge 2$, and let us apply Theorem 4.1 with $s=3$, $q=64$ and the Drinfeld curves $\widetilde{X}_k$ over $\mathbb{F}_8$ having at least $8^k=2^{K+1}$, $K=3k-1$, points rational over the field $\mathbb{F}_{64}$. We get then a binary $[N,k,d]$-code C_K with

$$\log A_d \ge \tfrac{1}{64}E_3(0.5)N - o(N) = \tfrac{1}{64}\big(\tfrac{1}{7}-\log\tfrac{64}{63}\big)N - o(N).$$

We can construct then a decreasing family $C_0=\mathbb{F}_2^N\supset C_1\supset\cdots\supset C_K$ defining inductively C_{K-i} for $i=1,\dots,K-1$ as generated by C_{K-i+1} and c_i for some binary vector $c_i\in\mathbb{F}_2^N$ with $\mathrm{wt}(c_i)=2^{K-i}$. Applying then Construction D we get a lattice $L_N\subset\mathbb{R}^N$ with $d_L=2$, and each minimum weight vector of C_K produces a minimum norm vector in L. Therefore we have

$$\frac{\log\tau(L_N)}{N} \ge \frac{\log A_d}{N} \ge \tfrac{1}{64}\big(\tfrac{1}{7}-\log\tfrac{64}{63}\big) - o(1) > 0.00187 - o(1).$$

This formula implies Corollary 1.2, albeit with a very small c_0.

Remark. We do not care here about the density of L, but the constructed family is still asymptotically good, albeit very poor for its density; however, it is easy to modify the construction to get a better (yet rather poor) family while conserving the ratio $\log\tau(L_N)/N$.

Remark. If we replace in the above construction the Drinfeld curve $\widetilde{X}_k$ by the Garcia–Stichtenoth curve X_k over $\mathbb{F}_{64}$ which has $63\cdot 64^k + O(1)$ points rational over $\mathbb{F}_{64}$, we can use $\delta = \frac{32}{63}$, since the minimum distance should be a power of 2. This leads to the bound $\frac{1}{64}\big(H\big(\frac{32}{63}\big) - \frac{6}{7} - \log\frac{64}{63}\big) \simeq 0.001874\ldots$ instead of $\frac{1}{64}\big(\frac{1}{7} - \log\frac{64}{63}\big) \simeq 0.001877\ldots$, and in that sense the Garcia–Stichtenoth tower is not optimal for our construction. The same remark applies to the constructions below, but the deterioration of the parameters is always very small.

It is then clear how to proceed: we can replace Construction D by Construction E applied to suitable T-lattices and codes from Theorem 4.3, which we complete in an appropriate manner. The best results are obtained using the T-lattices $\tilde{\Lambda}_{20}$, Λ_{24} (or $\tilde{\Lambda}_{24}$), and $\tilde{\Lambda}_{28}$, which give the lattice families in Theorem 4.1.

More precisely, in the case of Λ_{24} we take $q = 2^{12} = 4096$, the curve $\widetilde{X}_k$ over $\mathbb{F}_{64}$ having $N = 2^{12k} = 4^{6k}$ points rational over $\mathbb{F}_{2^{12}}$, put $d = a = N/2$ and apply Construction E to Λ_{24} and the family $C_0 = \mathbb{F}_2^N \supset C_1 \supset \cdots \supset C_{6k}$ of $[N, k_i, 4^i]$-codes over $\mathbb{F}_{2^{12}}$ for $i = 0, \ldots, 6k$, where $d_i = 4^i$, $d_{6k} = d = N/2$ and C_{6k-i} is defined inductively for $i = 1, \ldots, 6k-1$ as generated by C_{6k-i+1} and c_i for some vector $c_i \in \mathbb{F}_{4096}^N$ with $\mathrm{wt}(c_i) = 4^{6k-i}$. Exactly as above, each minimum-weight vector of C_{6k} gives rise to a minimum-norm vector of the resulting lattice L_{24N} and applying Corollary 4.4 we get (1-2). If we apply the same construction to $\tilde{\Lambda}_{4m}$, $q = 2^{2m}$ and the curve $\widetilde{X}_k$ over $\mathbb{F}_q$ having $N = 2^{2mk} = 4^{mk}$ points rational over $\mathbb{F}_q$, we get a lattice with

$$\frac{\log(\tau_N^l)}{N} \geq \frac{1}{4m}\left(1 - \frac{2\log(2^m+1)}{2^m-1}\right) - \frac{2+2\log N}{N}, \tag{6-1}$$

which gives (1-1)–(1-3) for $m = 5$, 6 and 7, respectively (the result is < 0.03 for any other value of m).

Applying in the same way Proposition 4.2 instead of Corollary 4.4 we get the lattices with

$$\frac{\log(\tau_N^l)}{N} \geq \frac{1}{4m}\left(1 - \frac{2m}{2^m-1} - \log\frac{2^{2m}}{2^{2m}-1}\right) - o(1) \tag{6-2}$$

and thus Theorem 1.3 for $m = 5$, 6 and 7.

We begin the proof of Theorem 1.5 with the following:

Proposition 6.1. *For any $q = p^h$ there exist monic polynomials $M_i \in \mathbb{F}_q[T]$ for $i = 1, 2, \ldots,$ with* $\deg M_{i+1} \geq \deg M_i$, *satisfying*

$$\lim_{i\to\infty} \frac{\tilde{g}_{i+1}}{\tilde{g}_i} = 1, \quad \tilde{g}_i < \tilde{g}_{i+1},$$

for $\tilde{g}_i := g(\widetilde{X}_0(M_i)) > 0$.

To prove this we "densify" the tower $\{\widetilde{X}_k\}$, inserting between its consecutive levels some curves from the family $\{\widetilde{X}_0(M)\}$. Indeed, let us consider two consecutive curves $\widetilde{X}_{2m}$ of genus $\tilde{g}_{2m} = (q^m-1)^2/(q-1)$ and $\widetilde{X}_{2m+1}$ of genus

$$\tilde{g}_{2m+1} = \frac{(q^{m+1}-1)(q^m-1)}{q-1} = q\,\tilde{g}_{2m} + O(\sqrt{\tilde{g}_{2m}}),$$

say, for $k = 2m \geq 100$. Set $s = s(k)$ for a suitable nondecreasing unbounded function $s : \mathbb{N} \to \mathbb{N}$ (to be chosen afterwards); then the number $P(s)$ of monic irreducible polynomials in A of degree s satisfies

$$\frac{q^s - q^{s/2}}{s} \leq P(s) \leq \frac{q^s}{s}.$$

We consider then the curves $\widetilde{X}_{k,j},\ j=1,\dots,l_k$ for $l_k=\min\{P(s),\lfloor k/s\rfloor\}$, defined by

$$\widetilde{X}_{k,j}=\overline{X}_0(T^{k+1-js}M_{s,j})\quad\text{for } M_{s,j}=\prod_{i=1}^{j}M_i^{(s)},$$

where $\{M_1^{(s)},\dots,M_{P(s)}^{(s)}\}$ is the list of all monic degree-s irreducible polynomials in A. The genus of $\widetilde{X}_{k,j}$ equals

$$\tilde{g}_{k,j}=\frac{q^{2m-sj}(q^s+1)^j}{q-1}+O(\sqrt{\tilde{g}_{2m}}),$$

which is increasing with j and $\tilde{g}_{k,j+1}/\tilde{g}_{k,j}$ tends to 1 for growing k. If $\tilde{g}_{k,l_k}$ is still less than $q^{2m+1}/(q-1)$, we can increase further the genus, taking $s+1$ instead of s and continuing to replace the factors T^{s+1} consecutively by irreducible polynomials of degree $s+1$, until we run out of such polynomials. If $k-sP(s)-(s+1)P(s+1)>0$ we can continue with the polynomials of degree $s+2$ and so on. The procedure stops when either we reach the genus $\tilde{g}_{2m+1}$ and we have densified our level, or there are no factors T^l to replace by the next polynomial of degree, say, $s+h,\ h\ge 1$. We want to show that choosing $s(k)$ appropriately, we can always reach $\tilde{g}_{2m+1}$ and thus densify our initial tower, which will end the proof. Indeed, for a given s, using all $P(s)$ degree-s irreducible polynomials, we multiply the genus by the factor $(1+q^{-s})^{P(s)}\simeq\exp(1/s)$. Therefore, using all irreducible polynomials of degrees from s to, say $s+t$, we can multiply the genus by

$$\exp\left(\frac{1}{s}+\cdots+\frac{1}{s+t}\right)\simeq 1+\frac{t}{s},$$

where this is possible whenever $sP(s)+\cdots+(s+t)P(s+t)\simeq q^s+\cdots+q^{s+t}\le k$. It is then sufficient to take $t/s>q,\ (s+t)q^{s+t}\le k$; for example, we can choose $t=(q+1)s,\ s=\log k/(2q\log q)$ to guarantee those inequalities for sufficiently large k, and the proof is finished (the case of an odd k is similar).

Remark. This proof can replace the sketchy proof of Claim (3.2)–(3.3) in [Shparlinski et al. 1992], equivalent to Proposition 6.1.

Let us deduce Theorem 1.5 from Proposition 6.1. Let $q=2^{12}=4096$, and let $k\in\mathbb{N}$ satisfy $\tilde{g}_k<n/24\le\tilde{g}_{k+1}$ for a given large dimension n; moreover, let $2^a\tilde{g}_k<n/24\le 2^{a+1}\tilde{g}_k$ for some $0\le a\le 11$ (recall that $\tilde{g}_{k+1}/\tilde{g}_k\simeq q$). Let us take the curve $X_0(M_i)$ from Proposition 6.1 of genus closest to $2^a\tilde{g}_k$ and the curve $X_0(M_j)$ of genus closest to $2^{a+1}\tilde{g}_k$. Then we construct, by Proposition 4.2, an $[N_i,k_i,2^{a+12k}=d_i]$-code C_i on $X_0(M_i)$ with exponentially many light vectors and the same with an $[N_j,k_j,2^{a+1+12k}=d_j]$-code C_j on $X_0(M_j)$; note that relative distances of both codes are asymptotic to $\frac{1}{2}$ and the ratio N_j/N_i is asymptotic to 2. We can then construct the lattices L_{24N_i} and L_{24N_j} in dimensions $24N_i$ and $24N_j$ using Construction E for the Leech lattice Λ_{24} (or $\tilde{\Lambda}_{24}$) and nested families of codes beginning, respectively, by C_i and C_j. The lattices L_{24N_i} and L_{24N_j} have then kissing numbers satisfying (1-6). Since $24N_i\le n\le 24N_j\simeq 48N_i$, the kissing number of the lattice L_{24N_i} gives the estimate

$$\frac{\log(\tau_n^l)}{n}\ge\tfrac{1}{24}\left(\tfrac{17}{21}-\log\tfrac{4096}{4095}\right)\delta \tag{6-3}$$

for $\delta=24N_i/n\in[0.5,1]$, and thus we can shorten the code C_j by deleting some $\mathbb{F}_q$-rational points from the corresponding curve to get a code of length $n/24$ and then apply Construction E with Λ_{24}. This gives

the estimate

$$\frac{\log(\tau_n^l)}{n} \geq \tfrac{1}{24}\Big(\lambda H\Big(\frac{1}{2\lambda}\Big) - \tfrac{4}{21} - \log\tfrac{4096}{4095}\Big), \tag{6-4}$$

with $\lambda \simeq 1/(2\delta) = n/(24N_j) \in [0.5, 1]$, and taking the minimax we get (1-8).

Remark. Using the lattices $\tilde{\Lambda}_{4m}$ together with the codes over $\mathbb{F}_{2^{2m}}$ with similar properties constructed on the curves from Theorem 5.3, instead of the above "densified" curves, we get the lattices with somewhat worse parameters, which are optimal for $m = 7$ and give the estimate

$$\liminf_{n\to\infty} \frac{\log(\tau_N^l)}{N} \geq 0.020715\ldots.$$

Acknowledgement

I thank G. Kabatiansky for drawing my attention to the problem of asymptotics for lattice kissing numbers.

References

[Ashikhmin et al. 2001] A. Ashikhmin, A. Barg, and S. Vlăduț, "Linear codes with exponentially many light vectors", *J. Combin. Theory Ser. A* **96**:2 (2001), 396–399. MR Zbl

[Barnes and Sloane 1983] E. S. Barnes and N. J. A. Sloane, "New lattice packings of spheres", *Canad. J. Math.* **35**:1 (1983), 117–130. MR Zbl

[Bos et al. 1982] A. Bos, J. H. Conway, and N. J. A. Sloane, "Further lattice packings in high dimensions", *Mathematika* **29**:2 (1982), 171–180. MR Zbl

[Chabauty 1953] C. Chabauty, "Résultats sur l'empilement de calottes égales sur une périsphère de R^n et correction à un travail antérieur", *C. R. Acad. Sci. Paris* **236** (1953), 1462–1464. MR Zbl

[Conway and Sloane 1988] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der Mathematischen Wissenschaften **290**, Springer, 1988. MR Zbl

[Elkies 2001] N. D. Elkies, "Explicit towers of Drinfeld modular curves", pp. 189–198 in *European Congress of Mathematics, II* (Barcelona, 2000), edited by C. Casacuberta et al., Progr. Math. **202**, Birkhäuser, Basel, 2001. MR Zbl

[Elkies et al. 2004] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell, and M. E. Zieve, "Curves of every genus with many points, II: Asymptotically good families", *Duke Math. J.* **122**:2 (2004), 399–422. MR Zbl

[Garcia and Stichtenoth 1995] A. Garcia and H. Stichtenoth, "A tower of Artin–Schreier extensions of function fields attaining the Drinfel'd–Vlăduț bound", *Invent. Math.* **121**:1 (1995), 211–222. MR Zbl

[Garcia and Stichtenoth 1996] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields", *J. Number Theory* **61**:2 (1996), 248–273. MR Zbl

[Gekeler 1986] E.-U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Mathematics **1231**, Springer, 1986. MR Zbl

[Gekeler 2001] E.-U. Gekeler, "Invariants of some algebraic curves related to Drinfeld modular curves", *J. Number Theory* **90**:1 (2001), 166–183. MR Zbl

[Kabatiansky and Levenstein 1978] G. A. Kabatiansky and V. I. Levenstein, "Bounds for packings on the sphere and in space", *Problemy Peredači Informacii* **14**:1 (1978), 3–25. In Russian; translated in Probl. Inf. Transm. 14 (1978) 1–17. MR

[Litsyn and Tsfasman 1987] S. N. Litsyn and M. A. Tsfasman, "Constructive high-dimensional sphere packings", *Duke Math. J.* **54**:1 (1987), 147–161. MR Zbl

[MacWilliams and Sloane 1977a] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes, I*, North-Holland Mathematical Library **16**, North-Holland, Amsterdam, 1977. MR Zbl

[MacWilliams and Sloane 1977b] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes, II*, North-Holland Mathematical Library **16**, North-Holland, Amsterdam, 1977. MR Zbl

[Rosenbloom and Tsfasman 1990] M. Y. Rosenbloom and M. A. Tsfasman, "Multiplicative lattices in global fields", *Invent. Math.* **101**:3 (1990), 687–696. MR Zbl

[Shannon 1959] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel", *Bell System Tech. J.* **38** (1959), 611–656. MR

[Shparlinski et al. 1992] I. E. Shparlinski, M. A. Tsfasman, and S. G. Vladut, "Curves with many points and multiplication in finite fields", pp. 145–169 in *Coding theory and algebraic geometry* (Luminy, 1991), edited by H. Stichtenoth and M. A. Tsfasman, Lecture Notes in Math. **1518**, Springer, 1992. MR Zbl

[Tsfasman et al. 2007] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007. MR Zbl

[Wyner 1965] A. D. Wyner, "Capabilities of bounded discrepancy decoding", *Bell Systems Tech. J.* **44** (1965), 1061–1122. MR

Received 22 Aug 2018. Revised 3 Oct 2018.

SERGE VLĂDUŢ:

serge.vladuts@univ-amu.fr
Aix Marseille Université, CNRS, Centrale Marseille, I2M UMR 7373, Marseille, France

and

IITP RAS, Moscow, Russia

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 2 2019