JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Hao CHEN

On a generalization of Craig lattices

Tome 25, n° 1 (2013), p. 59-70.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_1_59_0>

Journal de Théorie des Nombres
de Bordeaux **25** (2013), 59-70

On a generalization of Craig lattices

par Hao CHEN

Résumé. Dans cet article nous introduisons une généralisation des réseaux de Craig, qui nous permet de construire dans de nombreuses dimensions entre 3332 et 4096 des réseaux euclidiens plus denses que les réseaux de Mordell-Weil les plus denses connus. De plus, nous montrons que,sous réserve de l'existence de certains codes linéaires binaires, nous pouvons encore améliorer ces constructions dans l'intervalle $128-3272$. Nous construisons aussi quelques réseaux denses dans les dimensions $4098-8232$. Finalement nous obtenons également de nouveaux réseaux dans des dimension modérées, comme $68, 84, 85, 86$, qui sons plus denses que les réseaux connus jusqu'à présent.

Abstract. In this paper we introduce generalized Craig lattices, which allows us to construct lattices in Euclidean spaces of many dimensions in the range $3332-4096$ which are denser than the densest known Mordell-Weil lattices. Moreover we prove that if there were some nice linear binary codes we could construct lattices even denser in the range $128-3272$. We also construct some dense lattices of dimensions in the range $4098-8232$. Finally we also obtain some new lattices of moderate dimensions such as $68, 84, 85, 86$, which are denser than the previously known densest lattices.

1. Introduction

The problem of finding dense packings of infinite equal non-overlapping spheres in the Euclidean space $\mathbf{R}^n$ is a classical mathematical problem ([19, 16, 6, 29]). Low-dimensional sphere packing problems seem to be understood better than the problems in higher dimensions. The $1, 2, 3, 4, 5, 6, 7, 8$-dimensional root lattices had been proved to be the unique densest lattice sphere packings in these dimensions (see [6]). The Kepler conjecture about the 3-dimensional sphere packing problem was proved in [18]. Many known densest sphere packings are lattice packings or packings consisting of finitely many translates of lattices (see [6, 7, 23]). Constructing lattices

Manuscrit reçu le 7 septembre 2012, révisé le 11 février 2013.
The work was supported by National Science Foundation of China Grants 11061130539 and 61021004.
Classification math. 52C17, 52C07, 11H31, 11H71.

from error-correcting codes, algebraic number fields and algebraic varieties have been proposed by many authors and stimulated many further works ([22, 23, 6, 10, 11, 25, 12, 13, 14, 3, 15, 28]). Recently the Leech lattice, which was found in 1965 in [22], has been proved to be the unique densest lattice packing of dimension 24 (see [4, 5]). We refer to [6], pages 19–20 for Rogers and Kabatiansky-Levenshtein upper bounds of the densities of sphere packings; better upper bounds in low-dimensions are proved in the recent work [4]. From Voronoi's theory ([26]), there are algorithms to determine the densest lattice sphere packings in each dimension. However the computational task looks infeasible beyond dimension 9.

We refer to [24] for the known densest sphere packings in low dimensions; see also [1]. Our knowledge on high-dimensional sphere packings is quite different. In high dimensions n, in the range $80 \leq n \leq 4096$, $n = 2p - 2$ where p is a prime number satisfying $p \equiv 5 \mod 6$, or $n = 2^t$, where $7 \leq t \leq 12$, the known densest sphere packings are the lattices from algebraic curves over function fields. These are the Mordell-Weil lattices which were discovered by N. Elkies and T. Shioda in 1990's (see [12, 13, 28], and [6], preface to the third edition, page xviii). For example, the densest known 4096-dimensional sphere packing is a Mordell-Weil lattice with center density 2^{11527}. For dimensions in the range $149 \leq n = p - 1 \leq 3001$ (where p is a prime number, $149 \leq n \leq 3001$ except $p = 509, 513$ and 521), many of the known $n = (p - 1)$-dimensional densest sphere packings are Craig's lattices and their recent refinement (see [10, 11, 15, 6]). In the range $4100 \leq n \leq 12754608$ or $n \leq 8 \cdot 10^8$, the best known sphere packings are the lattices given by the Bos-Conway-Sloane construction ([2], [6], page 17, Table 1.3 and Chapter 8, Section 10).

In this paper we propose a generalization of Craig's lattices, which is a far-reaching extension of the Craig lattices described in [10, 11, 6], section 6, Chapter 8. These lattices are polynomial lattices and can be constructed for all dimensions. This generalization of Craig's lattices leads to many lattice sphere packings of moderate dimensions which are denser than the random lattices from Minkowski-Hlawka theorem (see section 3). Our construction establishes a close relation between nice lattices and linear error-correcting codes. If there were some "good enough" linear binary codes (see [17]), then our construction would lead to new lattices denser than the known densest Mordell-Weil lattices in many dimensions in the range $128 - 3272$. In the range $3332 - 4096$, it is easy to prove that some wanted codes in the above description exist. Thus we present some lattices which are denser than the Mordell-Weil lattices. New lattices denser than Shimada lattices of dimensions $84, 85$ and 86 ([24, 27]) are constructed in section 3. New denser lattices of many high dimensions in the range $4098 - 8323$ which are denser

than the known densest lattices from Bos-Conway-Sloane construction are also presented in section 5.

Definition 1.1. *For a packing of infinite equal non-overlapping spheres in* $\mathbf{R}^n$ *with centers* $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_m, ...,$ *the* packing radius *is*

$$\rho = \frac{1}{2} \min_{i \neq j} \{||\mathbf{x}_i - \mathbf{x}_j||\} .$$

The density *is* $\Delta = lim_{t \to 0} \frac{\text{Vol}\{\mathbf{x} \in \mathbf{R}^n : ||\mathbf{x}|| < t, \exists \mathbf{x}_i, ||\mathbf{x} - \mathbf{x}_i|| < \rho\}}{\text{Vol}\{\mathbf{x} \in \mathbf{R}^n : ||\mathbf{x}|| < t\}}$, *and the* center density *is* $\delta = \frac{\Delta}{V_n}$, *where* V_n *is the volume of the ball of radius* 1 *in* $\mathbf{R^n}$.

Let $\mathbf{b}_1, ..., \mathbf{b}_m$ be m linearly independent vectors in the n-dimensional Euclidean space $\mathbf{R}^n$. The discrete point set

$$\mathbf{L} = \{x_1 \mathbf{b}_1 + \cdots + x_n \mathbf{b}_m : x_1, ..., x_m \in \mathbf{Z}\}$$

is an m-dimensional lattice in $\mathbf{R}^n$, of determinant $\det(\mathbf{L}) = \det(\langle \mathbf{b}_i, \mathbf{b}_j \rangle)$. The volume of the lattice is $\text{Vol}(\mathbf{L}) = (\det(\mathbf{L}))^{\frac{1}{2}}$. The minimum norm of the lattice is $\mu(\mathbf{L}) = \min\{\langle \mathbf{x}, \mathbf{x} \rangle : \mathbf{x} \in \mathbf{L}\}$. Spheres with centers at these lattice vectors in $\mathbf{L}$ make a lattice sphere packing with packing radius $\rho = \frac{1}{2}\sqrt{\mu(\mathbf{L})}$ and center density $\delta(\mathbf{L}) = \frac{\rho^n}{\text{Vol}(\mathbf{L})}$. The lattice $\mathbf{L}^* = \{\mathbf{y} \in \mathbf{R}^m : \langle \mathbf{y}, \mathbf{x} \rangle \in \mathbf{Z}\}$ is the *dual lattice of* $\mathbf{L}$. A lattice is *integral* if the inner products between lattice vectors are integers. All lattices constructed in this paper are integral.

Let r be a prime power and $\mathbf{F}_r$ be the finite field with r elements. A linear (non-linear) error-correcting code $\mathbf{C} \subset \mathbf{F}_r^n$ is a k-dimensional subspace (or a subset of M vectors). For a codeword $\mathbf{x} \in \mathbf{C}$, $\text{wt}(\mathbf{x})$ is the number of nonzero coordinates of $\mathbf{x}$. The minimum Hamming weight (or distance) of a code C is $d(\mathbf{C}) = \min_{\mathbf{x} \neq \mathbf{y} \in \mathbf{C}} \{\text{wt}(\mathbf{x} - \mathbf{y})\}$. A linear (resp. non-linear) code of length n, distance d and dimension k (resp. with M codewords) is denoted as an $[n, k, d]$ (or an (n, M, d))-code . Given a binary $[n, k, d]$-code $\mathbf{C} \subset \mathbf{F}_2^n$ construction A ([6, 23]) leads to the lattice $\mathbf{L}(\mathbf{C})$ in $\mathbf{R}^n$ defined as the set of all integral vectors $\mathbf{x} = (x_1, ..., x_n) \in \mathbf{Z}^n$ satisfying $x_i \equiv c_i \mod 2$, $i = 1, ..., n$, for some codeword $\mathbf{c} = (c_1, ..., c_n) \in \mathbf{C}$. It is easy to check that $\rho = \frac{1}{2} \min\{\sqrt{d}, 2\}$ and $\text{Vol}(\mathbf{L}(\mathbf{C})) = 2^{n-k}$. This gives a lattice sphere packing with center density $\delta = \frac{\min\{\sqrt{d}, 2\}^n}{2^{2n-k}}$. Construction A leads to some of the densest known lattice packings in low dimensions (see [6]). For a non-linear binary (n, M, d)-code, the same construction gives a non-lattice packing with center density $\frac{M \cdot \min\{\sqrt{d}, 2\}^n}{2^{2n}}$. For example, the non-linear $(10, 40, 4)$-code gives us a non-lattice packing of dimension 10 with center density $\delta = \frac{5}{128} = 0.03906$, which is the densest known 10-dimensional sphere packing ([6]).

2. A generalization of the Craig lattices

Let ζ be a primitive p-th root of unity, where p is an odd prime. The ring of integers in $\mathbf{Q}[\zeta]$ is $\mathbf{Z}[\zeta]$ ([10, 11]). The $(p-1)$-dimensional Craig

lattice $\mathbf{A}_{p-1}^{(i)}$ introduced in [10] is the ideal in the ring $\mathbf{Z}[\zeta]$ (a free $\mathbf{Z}$ module) generated by $(1-\zeta)^i$, where i is a positive integer. A cyclotomic construction of the Leech lattice was given by Craig in [11]. In [15] a refinement of Craig lattices was proposed by adding some fractional numbers. The center densities of the refined Craig lattices are at least three times that of the original Craig lattices. These provided some new records; see [15].

Another kind of Craig lattices was given in [6], Section 6 of Chapter 8, namely lattices $\mathbf{A}_n^{(m)}$ of dimension n in the ring $\mathbf{Z}[x]/(x^{n+1}-1)$, the ideals generated by $(x-1)^m$ in the ring $\mathbf{Z}[x]/(x^{n+1}-1)$. The volume of $\mathbf{A}_n^{(m)}$ is $(n+1)^{m-\frac{1}{2}}$. When $n+1=p$ is an odd prime and $m<\frac{p}{2}$, they have minimum norm $\mu(\mathbf{A}_n^{(m)}) \geq 2m$; see Theorem 7, page 223 of [6]. These are the original lattices introduced by Craig in [10].

Our generalization of the Craig lattices are the $\mathbf{Z}$-sub-modules of the $\mathbf{Z}$-modules $R=\mathbf{Z}\langle 1,x,...,x^n\rangle$ spanned by $1,x,x^2,...,x^n$.

Given positive integers n,m,ℓ such that $m<\frac{n}{2}$ and $\ell \geq n+1$, consider the sub-module $\mathbf{A}_n^{(m,\ell)} = \mathbf{Z}(x-1)^n + \mathbf{Z}(x-1)^{n-1} + \cdots + \mathbf{Z}(x-1)^m + \ell\mathbf{Z}(x-1)^{m-1} + \ell\mathbf{Z}(x-1)^{m-2} + \cdots + \ell\mathbf{Z}(x-1)$ in $\mathbf{Z}\langle 1,x,...,x^n\rangle$. Any element v in $\mathbf{A}_n^{(m,\ell)}$ can be written as $v_0 1 + v_1 x + \cdots + v_n x^n$. The set of all coordinates $(v_0,v_1,...,v_n)$ of these vectors v in $\mathbf{A}_n^{(m,\ell)}$ is a sub-lattice of $\mathbf{Z}^{n+1}$. Equivalently we take the basis $\{1,x,...,x^n\}$ as an orthogonal basis for the $\mathbf{Z}$-module R and the $\mathbf{Z}$ sub-module described above is our generalized Craig lattice. For any polynomial $f(x)=a_0+a_1x+\cdots+a_nx^n \in R$ with integral coefficients satisfying $f(1)=0$, $f(x)$ is a linear combination of $(x-1),...,(x-1)^n$ with integral coefficients. If ℓ has no prime factor smaller than m, a polynomial $f(x)=a_nx^n+\cdots+a_1x+a_0$ with integral coefficients is in the lattice $\mathbf{A}_n^{(m,\ell)}$ if and only if $f(1)=0$ and $f^{(i)}(1)\equiv 0 \mod \ell$ for $i=1,...,m-1$.

Theorem 2.1. (1) *When $n+1$ is a prime or $m=1$, $\mathbf{A}_n^{(m,n+1)}$ is just the original Craig lattice;*

(2) *Given positive integers n,m,ℓ satisfying $m<\frac{n}{2}$ and $\ell \geq n+1$, $\mathbf{A}_n^{(m,\ell)}$ is a lattice of rank n and volume $\ell^{m-1}(n+1)^{\frac{1}{2}}$. When ℓ is a prime number, its minimum norm satisfies $\mu(\mathbf{A}_n^{(m,\ell)}) \geq 2m$.*

Proof. 1) When $m=1$, $\mathbf{A}_n^{(1,\ell)}$ has an integral base $\{(x-1),(x-1)x,...,(x-1)x^{n-1}\}$. Thus $\mathbf{A}_n^{(1,\ell)}=\mathbf{A}_n^{(1)}$.

We now prove that the lattice $\mathbf{A}_n^{(m,\ell)}$ is a cyclic lattice when $\ell=n+1$ is a prime number. It is clear that $(x-1)^jx=(x-1)^{j+1}+(x-1)^j$ lies in $\mathbf{A}_n^{(m,\ell)}$ for $m\leq j\leq n-1$ and that so is $\ell(x-1)^rjx=\ell(x-1)^{j+1}+\ell(x-1)^j$ for any j satisfying $1\leq j\leq m-1$. We only need to check that the element

$(x-1)^n x-(x^{n+1}-1)$, which is a shift of $(x-1)^n$, also lies in $\mathbf{A}_n^{(m,\ell)}$. Since $(x-1)^n x-(x^{n+1}-1)=(x-1)^{n+1}-x^{n+1}+1+(x-1)^n$, the coefficients of $(x-1)^j$, where $1\le j\le n-1$, are divisible by $n+1$ when $n+1$ is a prime number. Thus $(x-1)^n x-(x^{n+1}-1)$ is also in $\mathbf{A}_n^{(m,\ell)}$ when $n+1$ is a prime. Then the lattice $\mathbf{A}_n^{(m,n+1)}$ contains the Craig lattice $\mathbf{A}_n^{(m)}$ as a sub-lattice, and has the same index in $\mathbf{A}_n^{(1)}$. This proves (1).

2) It is obvious that $\mathbf{A}_n^{(m,\ell)}$ is a sub-lattice of the n-dimensional Craig lattice $\mathbf{A}_n^{(1)}=\{(v_0,v_1,...,v_n)\in\mathbf{Z}^{n+1}: v_0+v_1+\cdots+v_n=0\}$. On the other hand $\mathbf{A}_n^{(m,\ell)}$ has index ℓ^{-1} in $\mathbf{A}_n^{(1)}$. Thus it has dimension n and volume $\ell^{m-1}\,\mathrm{Vol}(\mathbf{A}_n^{(1)})=\ell^{m-1}(n+1)^{\frac{1}{2}}$. The proof of the second assertion is the same as the proof of Theorem 7 in the page 223 of [6]. If $\mu(\mathbf{A}_n^{(m,\ell)})<2m$, there is an element $f(x)=\Sigma_{i\in S}x^i-\Sigma_{j\in T}x^j\in\mathbf{A}_n^{(m,\ell)}$, where S and T are two subsets in $\{0,1,...,n\}$ satisfying $h=|S|=|T|<m$. Here $S=\{s_1,...,s_h\}$ and $T=\{t_1,...,t_h\}$ may contain repeated elements. Then from the condition $f(x)\in\mathbf{A}_n^{(m,\ell)}$ we have $f^{(i)}(1)\equiv 0\ mod\ \ell$, for $i=0,1,...,m-1$. Thus $\Sigma_{j=1}^h s_j^i\equiv\Sigma_{j=1}^h t_j^i\ mod\ \ell$, for all indices i's $i=0,1,...,m-1$. Since ℓ is a prime number, from the Newton's identities over the finite field $\mathbf{Z}/\ell\mathbf{Z}$, the elementary symmetric functions of S and T of degree $<m$ must be the same. Thus $S=T$ and $f(x)=0$ since $\ell\ge n+1$. □

The following result can be compared with the construction of the Craig-like lattices in [3]. Our lattices are obviously denser, since in their construction the prime number q is required to be the smallest prime q satisfying $q\equiv 1\ mod\ n$. When $\ell(>n)$ is a prime number, the generalized Craig lattice $\mathbf{A}_n^{(m,\ell)}$ is just the section of the Craig lattice $\mathbf{A}_{\ell-1}^{(m,\ell)}$ by imposing the condition that the last $\ell-n-1$ coordinates are zero.

Theorem 2.2. *For every dimension n and every positive integer $m<\frac{n}{2}$ the generalized Craig lattice with density $\Delta_n\ge\frac{m^{\frac{n}{2}}}{2^{m-1+\frac{n}{2}}\cdot n^{m-1}(n+1)^{\frac{1}{2}}}$. For suitable m we have $\frac{1}{n}\log_2\Delta_n\ge-\frac{1}{2}\log_2\log_2 n+o(1)$.*

Proof. By the Bertrand postulate there exists for any positive integer n a prime number ℓ between n and $2n$. Set m to be the nearest integer to $\frac{n}{2log_e n}$ as in the page 224 of [6]. We consider the generalized Craig lattice $\mathbf{A}_n^{(m,\ell)}$. A direct calculation gives us the result. □

Let ℓ be an odd number. We define a mapping

$$\pi:\mathbf{A}_n^{(m,\ell)}/2(\mathbf{A}_n^{(m,\ell)})\to\mathbf{Z}^{n+1}/2(\mathbf{Z}^{n+1})$$

by $\pi(a_0 + a_1 x + \cdots + a_n x^n) \equiv (a_0, ..., a_n) \mod 2$. This is an injective $\mathbf{Z}$-linear map. Since $2\frac{f^{(i)}(1)}{i!}$ is divisible by ℓ, $\frac{f^{(i)}(1)}{i!}$ also is (ℓ is odd). Clearly the image of π is a linear binary $[n+1, n, 2]$-code.

Theorem 2.3. *Suppose the positive integers n, m, ℓ satisfy $m < \frac{n}{2}$, $\ell \geq n+1$ and ℓ is a odd prime. If there exists a linear binary sub-code of the $[n+1, n, 2]$-code with parameters $[n+1, k, \geq 8m]$, then there exists a lattice with center density at least $\frac{2^{k-\frac{n}{2}} \cdot m^{\frac{n}{2}}}{\ell^{m-1}(n+1)^{\frac{1}{2}}}$.*

Proof. The binary linear $[n+1, k, \geq 8m]$-sub-code V is in $\pi(\mathbf{A}_n^{(m,\ell)})$ as a binary linear $[n+1, n, 2]$-code. From the linearity of π, the inverse image $\pi^{-1}(V)$ is a lattice with volume $2^{n-k}\operatorname{Vol}(\mathbf{A}_n^{(m,\ell)})$. Let $\mathbf{v}$ be a vector in $\pi^{-1}(V)$. If $\pi(\mathbf{v}) = 0$, $\mathbf{v} \in 2\mathbf{A}_n^{(m,\ell)}$, then the Euclidean norm of $\mathbf{v}$ is at least $8m$. If $\pi(\mathbf{v}) \neq 0$, then at least $8m$ coordinates of the vector $\mathbf{v}$ are odd numbers and the norm of $\mathbf{v}$ is at least $8m$. This completes the proof of the theorem. □

Theorem 2.4. *Suppose the positive integers n, m, ℓ satisfy $m \leq \frac{n+1}{2}$, ell $\geq n+1$ and ℓ is a odd prime. If there exists a linear binary $[n, k, 8m]$-code then there exists a lattice having center density at least $\frac{2^{k-\frac{n}{2}} \cdot m^{\frac{n}{2}}}{\ell^{m-1}(n+1)^{\frac{1}{2}}}$.*

Proof. We may apply Theorem 2.3 to the extended code of the $[n, k, 8m]$-code by adding a parity check digit. □

In dimension $n = 160$, since $n + 1 = 161 = 23 \cdot 7$ is not a prime, there exists no convenient Craig lattice. However the generalized Craig lattice $\mathbf{A}_{160}^{(16,163)}$ has center density $\delta_{160} = \frac{8^{80}}{163^{15.5}} \approx 2^{126.4051}$. Using the trivial linear binary $[160, 1, 160]$-code together with Theorem 2.4 we obtain a dense lattice of the dimension 160 with center density at least $2^{127.4051}$. On the other hand, there is no 160-dimensional Mordell-Weil lattice . The nearest (by the dimension) known Mordell-Weil lattice (Theorem 1.1 of [28]) having a smaller dimension (by Theorem 1.1 of [28]) has dimension 140 and center density $2^{113.31}$. There is no child lattice $\eta(\mathbf{E}_8)$ of dimension 160 ([6], page 241). A 160-dimensional lattice satisfying the Minkowski-Hlawka bound has the center density approximately 111.2378. Thus our construction provides a new dense lattice in this dimension.

3. Some new dense lattices

Theorem 3.1. *Let p be a prime number larger than or equal to 1223. Suppose $\mathbf{A}_{p-1}^{(m)}$ is the densest Craig lattice of dimension $p-1$. Then the construction of Theorem 2.4 yields a lattice having center density at least $8\,\delta(\mathbf{A}_{p-1}^{(m)})$.*

Proof. It is known that the Craig lattice $\mathbf{A}_n^{(m)}$, where m is nearest integer to $\frac{n}{2log_e(n+1)}$, is the densest Craig lattice in the dimension $n = p-1$, p a prime. Since $n \geq 1222$, we have $\frac{8(\frac{n}{2log_e(n+1)}+1)}{n} \leq \frac{4}{7}$. Using a suitable trivial extension of the concatenation of a $[[\frac{n}{7}], 1, [\frac{n}{7}]]$-code over $\mathbf{F}_8$ with a $[7, 3, 4]$-code we get an $[n, 3, 8(\frac{n}{2log_e(n+1)} + 1)]$ code, to which we may apply Theorem 2.4. □

In [15] the Craig lattices are refined to new lattices with center densities at most $6\delta(\mathbf{A}_n^{(m)})$ in the range $1298 \leq n \leq 3482$. Thus the lattices above are denser than those in [15]. Some of them are even denser than any previously known lattice.

The 68-dimensional extremal unimodular lattices (of minimum norm 6) have center density $(\frac{3}{2})^{34} \approx 2^{19.89}$ ([24]). Applying Theorem 2.4 to the generalized Craig lattice $\mathbf{A}_{68}^{(4,71)}$ and binary $[68, 8, 32]$- code (see [17]) we get a new lattice with center density at least $2^{20.4757}$. The volume of this new lattice is $2^{60} \cdot 71^3 \cdot 69^{\frac{1}{2}}$. In [27] a long computation of algebraic geometry over finite fields was used to construct dense lattices in dimensions 84, 85 and 86 with center densities $\delta_{84}^{Shimada} \approx 2^{30.795}, \delta_{85}^{Shimada} \approx 2^{32.5}$ and $\delta_{86}^{Shimada} \approx 2^{34.2075}$. The generalized Craig lattice $\mathbf{A}_{86}^{(10,89)}$ has center density $2^{38.3225}$, the generalized Craig lattice $\mathbf{A}_{85}^{(10,89)}$ has center density $2^{37.1616}$ and the generalized Craig lattice $\mathbf{A}_{84}^{(10,89)}$ has center density $2^{36.006}$. Applying Theorem 2.4 to the trivial linear binary $[84, 1, 84]$-, $[85, 1, 84]$- and $[86, 1, 86]$-codes we obtain new lattices in dimensions $84, 85$ and 86 with center densities $2^{37.006}$, $2^{38.1616}$ and $2^{39.3225}$ respectively.

Note that many constructions of dense lattices are valid only in even dimensions. Our constructions in Theorems 2.2 and 2.4 can be used in all dimension and the center density of our lattices depends "continuously" on the dimension. This allows us to obtain high densities in some odd dimensions.

In Table 3.1 below we list some new denser lattices from Theorem 2.4.

4. Some possible new dense lattices

In this short section we briefly describe some putative lattices which might exist, depending on the existence of some convenient codes.

Proposition 4.1. *Let $p \equiv 5 \bmod 6$ be a prime. If there exists a $[2p-2, \frac{7p-5}{6} - \lceil \frac{p-11}{12} \cdot log_2 p \rceil, \geq \frac{2(p+1)}{3}]$-code, then there exists a lattice of dimension $2p-2$ with center density (equal to $\frac{((p+1)/12)^{p-1}}{p^{(p-5)/6}}$) larger than that of any $(2p-2)$-dimensional Mordell-Weil lattice.*

Table 3.1

$dimension$	$new - log_2\delta$	$previously - known$
68	20.6757	$19.89(Gaborit + Harada - Kitazume)$
84	37.006	$30.795(Shimada)$
85	38.1616	$32.5(Shimada)$
86	39.3225	$34.2075(Shimada)$
144	105.6736	$96(\eta(\mathbf{\Lambda}_{24}))$
149	112.3048	no
151	113.7424	no
152	115.2811	no
153	116.8248	no
154	118.3685	no
155	119.9122	no
157	122.1067	no
158	123.6504	no
160	127.4051	$111(Minkowski - Hlawka)$
168	135.9011	$120(\eta(\mathbf{\Lambda}_{24}))$
246	249.2827	$234.33039(Minkowski - Hlawka)$
248	227.0997	$196.54(Thompson - Smith)$
288	318.3031	$300(\eta(\mathbf{\Lambda}_{24}))$
360	443	$408(\eta(\mathbf{\Lambda}_{24}))$

Proof. Set $m = \lceil \frac{p+1}{12} \rceil$. By Bertrand 's postulate there exists a prime ℓ between $2p-1$ and $4p-2$. Applying Theorem 2.4 to the generalized Craig lattice $\mathbf{A}_{2p-2}^{(m,\ell)}$ and the code in the statement, we obtain a lattice as required. □

For example, applying Theorem 2.4 to $\mathbf{A}_{128}^{(4,131)}$ and a putative binary linear $[128, 59, 32]$ code, we could get a new lattice of rank 128 with center density $2^{98.3831}$. That of the 128-dimensional Mordell-Weil lattice is

$2^{97.40}$ (see [6] page xviii). From the table in [17] there exists a binary linear $[128, 43, 32]$-code and we may thus construct a 128-dimensional lattice with center density $2^{82.3831}$. The upper bound for the minimum distance of linear binary $[128, 59]$ code is 32, but we do not know whether such a code exists. Similarly if a code with one of the following parameters $[256, 99, 64]$, $[256, 74, 80]$, $[256, 136, 48]$ and $[256, 56, 96]$ exists, then a 256-dimensional lattice with center density larger than the center density $2^{294.8}$ of the 256-dimensional Mordell-Weil lattice (see [6] page xviii) could be constructed from Theorem 2.4.

5. Denser lattices in dimensions $3332 - 8640$

From the Gilbert-Varshamov bound ([30]), if

$$V(4096, 1023) = \Sigma_{i=0}^{1023}\tbinom{4096}{i} < 2^{4097-k},$$

there exists a linear binary $[4096, k, 1024]$ code. From the inequality

$$\Sigma_{i=0}^{r}\tbinom{n}{i} < 2^{nH(r/n)} < 2^{H(\frac{1}{4})n},$$

where $H(x)$ is the binary entropy function ([30] page 21), we have $V(4096, 1023) < 2^{3324}$. Thus a binary, linear $[4096, 772, 1024]$-code exists, and we can construct a 4096-dimensional lattice with center density at least 2^{11529}, hence denser than Mordell-Weil lattices of this dimension.

Lemma 5.1. *There exist linear binary codes of length* $8n$*, dimension* $[(6log_2 3 - 8)n]$ *and minimum distance* $2n$*.*

Proof. Set $V(n, r) = \Sigma_{i=0}^{r}\binom{n}{i}$. From the Gilbert-Varshamov bound ([30]), if $V(n, d-1) < 2^{n-k+1}$, then a linear binary code with parameter $[n, k, d]$ exists. From Theorem 1.4.5 of [30], page 21, $V(8n, 2n-1) < 2^{8H(\frac{1}{4})n}$. The conclusion follows directly. □

Theorem 5.2. *Let* $p \equiv 5 \mod 6$ *be a prime such that* $1667 \leq p \leq 2039$*. Then there exists a lattice of dimension* $n = 2p-2$ *with center density higher than that (equal to* $\frac{((p+1)/12)^{p-1}}{p^{(p-5)/6}}$*) of the Mordell-Weil lattice of dimension* n *(Theorem 1.1* [28]*).*

Proof. The center density of the $(2p-2)$-dimensional Mordell-Weil lattice is $\frac{((p+1)/12)^{p-1}}{p^{(p-5)/6}}$. The generalized Craig lattice $\mathbf{A}_{2p-2}^{([\frac{p-1}{16}], 2p+t)}$, where t is a positive integer such that $2p+t$ is a prime, has center density $\frac{[\frac{p-1}{32}]^{p-1}}{(2p+t)^{[\frac{p-1}{16}]-\frac{1}{2}}}$. It can be checked that $(2p+t) < 2^{1.001}p$. The conclusion follows from the existence of a $[2p-2, [0.3776(p-1)], \frac{p-1}{2}]$-code proved in Lemma 5.1. □

We also have the following result for the high-dimensional lattices in the range $4104 - 8640$.

Theorem 5.3. *For each dimension $N = 24n \in [4104 - 8640]$, there exists an N-dimensional lattice which is denser than the N-dimensional child lattice of the Leech lattice $\eta(\mathbf{\Lambda}_{24})$.*

Proof. We consider the generalized Craig lattice $\mathbf{A}_{24n}^{([\frac{3n}{4}],\ell)}$, where ℓ is smallest prime number bigger than or equal to $24n+1$. From the Gilbert-Varshamov bound, there exists a linear binary $[24n, [4.5312n], 6n]$-code. Then we can construct a lattice with center density $2^{[4.5312n]} \cdot \frac{([\frac{3n}{8}])^{12n}}{\ell^{[3n/4]-\frac{1}{2}}}$. The conclusion follows from a direct calculation. □

Some new denser lattices constructed in this section are listed in Table 5.1 below.

Table 5.1

$dimension$	$new - log_2\delta$	$previously - known$
3332	8913	$8897.0184(MW)$
3956	11035	$10969.9654(MW)$
3992	11159	$11099.6432(MW)$
4004	11208	$11130.5560(MW)$
4052	11370	$11294.2234(MW)$
4076	11455	$11375.6625(MW)$
4096	11529	$11527(MW)$
4098	11536	$11279(Craig)$
4104	11554	$11400(\eta(\mathbf{\Lambda}_{24}))$
4124	11618	$11537.1837(MW)$
8184	26823	$26712(\eta(\mathbf{\Lambda}_{24}))$
8190	26915	$26154(Craig)$
8208	26953	$26808(\eta(\mathbf{\Lambda}_{24}))$
16380	61419	$59617(Craig)$

References

[1] R. Bacher, *Dense lattices in dimensions 27-29*. Invent. Math. **130** (1997), 153–158.
[2] A. Bos, J. H. Conway and N. J. A. Sloane, *Further lattices packings in high dimensions*. Mathematika **29** (1982), 171–180.

[3] J. Carmelo Interlando, A. L. Flores and T. P. da Nóbrega Neto, *A family of asymptotically good lattices having a lattice in each dimension*. Inter. J. Number Theory **4** (2008), 147–154.
[4] H. Cohn and N. D. Elkies, *New upper bounds on sphere packings I*. Ann. of Math. **157** (2003), 689–714.
[5] H. Cohn and A. Kumar, *Optimality and uniqueness of Leech lattice among lattices*. Ann. of Math **170**(2009), 1003–1050.
[6] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. 3rd Edition, Springer, 1999.
[7] J. H. Conway and N. J. A. Sloane, *Laminated lattices*. Ann. of Math. **116** (1982), 593–620.
[8] J. H. Conway and N. J. A. Sloane, *The antipode construction for sphere packings*. Invent. Math. **123** (1996), 309–313.
[9] J. H. Conway, *Sphere packings, lattices, codes and greed*. Proc. ICM Zurich, I (1994), 45–55.
[10] M. Craig, *Extreme forms and cyclotomy*. Mathematika **25** (1978), 44–56.
[11] M. Craig, *A cyclotomic construction for Leech's lattice*. Mathematika **25** (1978), 236–241.
[12] N. D. Elkies, *Mordell-Weil lattices in characteristic 2, I: Construction and first properties*. Inter. Math. Research Notices **8** (1994), 343–361.
[13] N. D. Elkies, *Mordell-Weil lattices in characteristic 2, II: The Leech lattice as a Mordell-Weil lattice*. Invent. Math. **128** (1997),1–8.
[14] N. D. Elkies, *Mordell-Weil lattices in characteristic 2, III: A Mordell-Weil lattice of rank 128*. Experimental Math. **10** (2001), 467–473.
[15] A. L. Flores, J. Carmelo Interlando, T. P. da N. Neto and J. O. D. Lopos, *On a refinement of Craig's lattice*. J. Pure Appl. Algebra **215** (2011), 1440–1442.
[16] C. F. Gauss, *Untersuchungen über die Eigenschaften der positiven ternaren quadratischen Formen von Ludwig August Seeber*. Göttingische gelehrte Anzeigen 1831, Juli 9, = "Recension der..." in J. Reine Angew Math. **20**, 312–320, = Werke 11 (1840), 188–196.
[17] M. Grassl, http://www.codetables.de
[18] T. C. Hales, *A proof of the Kepler conjecture*. Ann. of Math. **162** (2005), 1065–1185.
[19] J. Kepler, *The six-cornered snowflake* (1611); translated by L. L. Whyte, Oxford Univ. Press, 1966.
[20] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*. Math. Ann. **11** (1877), 242–292.
[21] F. R. Kschischang and S. Pasupathy, *Some ternary and quaternary codes and associated sphere packings*. IEEE Trans. on Information Theory **38** (1992), 227–246.
[22] J. Leech, *Notes on sphere packings*. Canadian J. Math. **19** (1967), 251–267.
[23] J. Leech and N. J. A. Sloane, *New sphere packings in dimension* $9-15$. Bull. Amer. Math. Soc. **76** (1970), 1006–1010.
[24] G. Nebe and N. J. A. Sloane, *A Catalogue of Lattices*. http://www.math.rwth-aachen.de/ Gabriele.Nebe/LATTICES/
[25] H.-G. Quebbemann, *A Construction of integral lattices*. Mathematika **31** (1984), 137–140.
[26] A. Schürmann, *Computational geometry of positive quadratic forms: polyhedral reduction theory, algorithms and applications*. University Lecture Series, Amer. Math. Soc. 2008.
[27] I. Shimada, *Lattices of algebraic cycles on Fermat varieties in positive characteristics*. Proc. London Math. Soc. **82** (2001), 131–172.
[28] T. Shioda, *Mordell-Weil lattices and sphere packings*. Amer. J. Math. **113** (1991), 931–948.
[29] N. J. A. Sloane, *The sphere packing problem*. Proc. ICM III, Berlin (1998), 387–396.
[30] J. H. van Lint, *Introduction to coding theory*. 3rd Edition, Springer-Verlag, 1999.

Hao Chen
Software Engineering Institute
East China Normal University
Zhong Shan North Road 3663
Shanghai 200062, P.R. China
E-mail: haochen@sei.ecnu.edu.cn
URL: http://faculty.ecnu.edu.cn/s/127/t/767/main.jspy