ANNALES

DE

L'INSTITUT FOURIER

Philippe GABORIT & Gilles ZÉMOR

On the construction of dense lattices with a given automorphisms group

Tome 57, nº 4 (2007), p. 1051-1062.

<http://aif.cedram.org/item?id=AIF_2007__57_4_1051_0>

Ann. Inst. Fourier, Grenoble
57, 4 (2007) 1051-1062

ON THE CONSTRUCTION OF DENSE LATTICES WITH A GIVEN AUTOMORPHISMS GROUP

by Philippe GABORIT & Gilles ZÉMOR

Abstract. — We consider the problem of constructing dense lattices in $\mathbb{R}^n$ with a given non trivial automorphisms group. We exhibit a family of such lattices of density at least $cn2^{-n}$, which matches, up to a multiplicative constant, the best known density of a lattice packing. For an infinite sequence of dimensions n, we exhibit a finite set of lattices that come with an automorphisms group of size n, and a constant proportion of which achieves the aforementioned lower bound on the largest packing density. The algorithmic complexity for exhibiting a basis of such a lattice is of order $\exp(n \log n)$, which improves upon previous theorems that yield an equivalent lattice packing density. The method developed here involves applying Leech and Sloane's Construction A to a special class of codes with a given automorphisms group, namely the class of double circulant codes.

Résumé. — On s'intéresse à la construction de réseaux denses de $\mathbb{R}^n$ contenant un groupe d'automorphismes donné non trivial. On obtient une telle construction de réseaux, dont la densité est au moins $cn2^{-n}$, ce qui, à une constante multiplicative près, atteint la meilleure densité asymptotique connue d'un empilement de sphères. Plus précisément, on exhibe, pour une suite infinie de dimensions n, un ensemble de réseaux de groupe d'automorphismes fixé et de taille n, et dont une proportion constante atteint la borne inférieure précitée sur la densité. La complexité algorithmique de la construction d'une base d'un tel réseau dense est d'ordre $\exp(n \log n)$, ce qui améliore la complexité des constructions déjà connues de réseaux d'une densité équivalente. La méthode que nous proposons utilise la construction A de Leech et Sloane appliquée à une classe particulière de codes : la classe des codes doublement circulants.

1. Introduction

A lattice packing of Euclidean balls in $\mathbb{R}^n$ is a family of disjoint Euclidean balls of maximum equal radius centered on the points of some non degenerate lattice. The proportion of the space covered by these Euclidean balls is

Keywords: Lattice packings, Minkowski-Hlawka lower bound, probability, automorphism group, double circulant codes.
Math. classification: 06B20, 03G10.

called the density of the packing. When balls of volume V are packed by a lattice Λ, the corresponding density is $V.(\det\Lambda)^{-1/2}$, where $\det\Lambda$ denotes the determinant of a Gram matrix associated to the lattice. *i.e.* $(\det\Lambda)^{1/2}$ is the volume of a fundamental region of Λ.

The classical Minkowski-Hlawka Theorem states that for n greater than 1 there exist lattice packings with density at least $2^{1-n}\zeta(n)$. This lower bound on the lattice packing density was later improved by a linear factor to a quantity of the form $cn2^{-n}$ for constant c. This improvement is originally due to Rogers [8] with $c = 2e^{-1}$. The constant c was successively improved by Davenport and Rogers [4] to $c = 1.68$ and eventually by Ball [2] to $c = 2$.

In the meantime, Rush [9], building upon a technique of Rush and Sloane [10], essentially recovered the original Minkowski-Hlawka lower bound on the largest density of a sphere packing using coding theory arguments together with the Leech-Sloane Construction A for lattices. While this did not achieve the improved density of the form $cn2^{-n}$, it had the alternative advantage of being more effective than the proofs of the above results. Rush's construction exhibits in a natural way a finite number of lattices among which dense ones exist. This number, though still too large to be in any way practical, is much smaller than what can be derived by applying the original proofs of the results highlighted above: Consequently, the algorithmic complexity of Rush's construction is of the form $\exp(n\log n)$ which is a substantial improvement over the preceding ones (see [3], p.18). A different approach with smaller complexity than the original proofs is also presented by Bacher in [1].

Recently, the $cn2^n$ improved lower bound on the minimum density was made as effective as Rush's lattice construction, with $c = 0.01$, for (non-lattice) sphere packings by Krivelevich, Litsyn and Vardy in [7]. They use an elegant graph theory method that enables them to find dense packings with a time (and space) complexity $\exp(n\log n)$.

In this paper, we again make the $cn2^n$ lower bound as effective, with $c \approx 0.06$, without paying the price of losing lattice structure. In fact, the dense lattice packings that we exhibit have *additional* algebraic structure, namely they come together with an automorphism group of size n. This additional structure is not a by-product of our method but is an essential reason for the improved density. This is a small step towards showing that, in the asymptotic setting, algebraic constructions can compete with unstructuredness, and maybe even stand out.

The starting point of our approach is similar to that of [10] and [9], namely relies upon construction A to transform codes in $\mathbb{F}_p^n$ into lattices of $\mathbb{R}^n$. The specificity of the Rush-Sloane method is to consider codes designed for a metric which is unconventional in $\mathbb{F}_p^n$ but specially adapted to the Euclidean metric in $\mathbb{R}^n$. However, instead of indiscriminately looking for the best codes for this metric in the whole space $\mathbb{F}_p^n$, we depart from [10, 9] by restricting our attention to an exponentially smaller set of codes, namely a class that has a given automorphism group (double circulant codes), and prove that a constant fraction of them yield lattices with improved density. Similar codes were also used in a coding theory context to improve the classical Gilbert-Varshamov bound for linear codes by a linear factor [5]. Exhibiting a lattice basis has algorithmic (time) complexity $\exp(n \log n)$.

The paper is organized as follows: In Section 2, we show how dense lattices are constructed from "dense" codes and we formulate our main results, Theorem 1 and Corollary 2. In Section 3 we show how to obtain good double circulant codes.

2. From dense codes to dense lattices

Let S_n denote the Euclidean ball of radius 1 in $\mathbb{R}^n$, we have:

$$\mathrm{Vol}\,(S_n) = \frac{\pi^{(n/2)}}{(n/2)!}. \tag{1}$$

Let $S_n(d)$ denote the Euclidean ball of radius d in $\mathbb{R}^n$, so that we have

$$\mathrm{Vol}\,(S_n(d)) = d^n\,\mathrm{Vol}\,(S_n)\,.$$

Let $\rho \in \mathbb{R}$ be the radius of a Euclidean ball of volume $p^{n/2}$ for p any positive number, *i.e.* $\mathrm{Vol}\,(S_n(\rho)) = p^{n/2}$. By (1) and Stirling's formula we have:

$$\rho = \sqrt{\frac{pn}{2e\pi}}(1+o(1)) \tag{2}$$

where $o(1)$ will always be understood to mean a quantity that vanishes as n goes to infinity.

For Λ a lattice of dimension n it is customary to define its minimum norm by

$$\mu(\Lambda) = \min\left\{\sum_{i=1}^{n} x_i^2, \quad (x_1,\ldots,x_n) \in \Lambda \smallsetminus \{0\}\right\}.$$

The lattice Λ defines a packing of $\mathbb{R}^n$ by spheres of Euclidean radius $\sqrt{\mu}/2$ and the density of this packing is given by:

$$\Delta = \frac{\mathrm{Vol}\left(S_n(\sqrt{\mu}/2)\right)}{(\det\Lambda)^{1/2}} = \frac{\mathrm{Vol}\left(S_n\right)\mu^{n/2}}{2^n(\det\Lambda)^{1/2}}, \tag{3}$$

where $\det\Lambda$ stands for the determinant of Λ.

From now on let p be an odd prime. We identify elements z of $\mathbb{F}_p$ with elements z of $\mathbb{Z}$ such that

$$-\frac{p-1}{2} \leqslant z \leqslant \frac{p-1}{2}.$$

With this convention, following [10, 9], we introduce the *norm* of a vector $\mathbf{x} = (x_1, \dots, x_n)$ in $\mathbb{F}_p^n$ as the non-negative real number

$$\|\mathbf{x}\|_2 = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Let $B_{n,p}(d)$ denote the set of vectors $\mathbf{x} \in \mathbb{F}_p^n$ such that $\|\mathbf{x}\|_2 \leqslant d$. We shall only be dealing with values of d such that $d < p/2$ so that we shall always have:

$$|B_{n,p}(d)| = |\mathbb{Z}^n \cap S_n(d)| \tag{4}$$

hence, by fitting the sphere $S_n(d)$ inside a union of n-cubes of volume 1,

$$\mathrm{Vol}\left(S_n\left(d - \frac{\sqrt{n}}{2}\right)\right) \leqslant |B_{n,p}(d)| \leqslant \mathrm{Vol}\left(S_n\left(d + \frac{\sqrt{n}}{2}\right)\right). \tag{5}$$

Define a $[n,k,d,p]$ code as a k-dimensional subspace C of $\mathbb{F}_p^n$ such that d equals the minimum of the norm $\|\mathbf{x}\|_2$ of a nonzero codevector $\mathbf{x} \in C$. We will refer to d as the minimum norm of the code C.

Recall that Construction A associates to a code C the lattice:

$$A_p(C) = \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid (x_1 \bmod p, \dots, x_n \bmod p) \in C\}.$$

It is readily seen that this lattice has minimum norm $\mu = \min(d^2, p^2)$ and determinant $p^{2(n-k)}$. In the following, we will always ensure that $d \leqslant p$ so that the $[n,k,d,p]$ code C yields by construction A a lattice of $\mathbb{R}^n$ of norm d^2 with density (3):

$$\Delta = \frac{1}{2^n}\frac{\mathrm{Vol}\left(S_n(d)\right)}{p^{n-k}}. \tag{6}$$

By (5) this gives a density

$$\Delta \geqslant \frac{1}{2^n}\frac{|B_{n,p}(d)|}{p^{n-k}}\left(1 + \frac{\sqrt{n}}{2d}\right)^{-n}. \tag{7}$$

We shall prove

Theorem 1. — *There exists a constant c, such that for any $n = 2q$, q a large enough prime, there exists a prime p, $n^2 \log n < p \leqslant (n^2 \log^2 n)^{5.5}$, and an $[n, n/2, d, p]$ code C such that*

$$|B_{n,p}(d)| \geqslant cnp^{n/2}.$$

Furthermore, the automorphism group of C contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Since $p \sim \sqrt{\frac{pn}{2e\pi}}$ by (5) and (2), the condition $n^2 \log n < p$ in Theorem 1 will ensure that the term $(1 + \sqrt{n}/2d)^{-n}$ in (7) tends to 1 when n tends to infinity. This will enable us to obtain:

Corollary 2. — *There exists a constant c, such that for any $n = 2q$, q a large enough prime, there exists a lattice of $\mathbb{R}^n$ with density at least $cn/2^n$ and whose automorphism group contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Such a lattice can be constructed with time complexity* $\exp(n \log n)$).

The numerical value of the constant c in Theorem 1 and Corollary 2 can be estimated to be at least $(2 - 1/e)(2 + e^2\pi)^{-1} \approx 0.064$.

3. Double circulant codes and random choice

A p-ary *double circulant code* is a $[2q, q, d, p]$ linear code C with a parity-check matrix of the form $\mathbf{H} = [\mathbf{I}_q \mid \mathbf{A}]$ where $\mathbf{I}_q$ is the $q \times q$ identity matrix and

$$\mathbf{A} = \begin{bmatrix} a_1 & a_2 & \dots & a_q \\ a_q & a_1 & \dots & a_{q-1} \\ a_{q-1} & a_q & \dots & a_{q-2} \\ \dots & \dots & \dots & \dots \\ a_2 & a_3 & \dots & a_1 \end{bmatrix}.$$

This simply means that C is the kernel generated by the row-vectors of $[A^t, -I_q]$ of the mapping $\mathbf{x} \mapsto \mathbf{x}\,{}^t\mathbf{H}$ from $\mathbb{F}_p^{2q}$ to $\mathbb{F}_p^q$.

We will only consider the case where q is an odd prime. Let $n = 2q$. There is a natural action of the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ on the space $\mathbb{F}_p^n$ of vectors $\mathbf{x} = (x_1 \dots x_q, x_{q+1} \dots x_{2q})$

$$\begin{array}{rcl} G \times \mathbb{F}_p^n & \to & \mathbb{F}_p^n \\ (g, \mathbf{x}) & \mapsto & g \cdot \mathbf{x} \end{array}$$

where $(0,1) \cdot \mathbf{x} = (x_q, x_1 \dots x_{q-1}, x_{2q}, x_{q+1}, \dots x_{2q-1})$ and $(1,0) \cdot \mathbf{x} = -\mathbf{x}$. The double circulant code C is invariant under this group action and so is the norm of any vector $\mathbf{x}$. Note that construction A applied to the code C will clearly yield a lattice whose automorphism group contains G.

To show that double circulant codes with a large minimum norm d exist, we shall study the typical behaviour of d when a double circulant code is chosen at random. We now formalize this:

Consider the random double circulant code C_{rand} obtained by choosing the first row vector $(a_1, \dots, a_q)$ of $\mathbf{A}$ with a uniform distribution in $\mathbb{F}_p^q$. We are interested in the random variable $X(w)$ equal to the number of nonzero codevectors of C_{rand} of norm not more than w. In other words we define

$$X(w) = \sum_{\mathbf{x} \in B_{n,p}(w) \smallsetminus \{0\}} X_{\mathbf{x}}$$

where $X_{\mathbf{x}}$ is the Bernoulli random variable equal to 1 if $\mathbf{x} \in C_{\mathrm{rand}}$ and equal to zero otherwise. Our strategy is to construct a number w such that $\mathrm{P}\left(X(w) > 0\right) < 1$, this will prove the existence of codes of parameters $[n, n/2, d > w, p]$.

The core remark is now that, if $\mathbf{y} = g \cdot \mathbf{x}$, then

$$X_{\mathbf{y}} = X_{\mathbf{x}}.$$

Let now $B'_{n,p}(w)$ be a set of representatives of the orbits of the elements of $B_{n,p}(w)$, *i.e.* for any $\mathbf{x} \in B_{n,p}(w)$, $|\{g \cdot \mathbf{x}, g \in G\} \cap B'_{n,p}(w)| = 1$. We clearly have $X(w) > 0$ if and only if $X'(w) > 0$ where

$$X'(w) = \sum_{\mathbf{x} \in B'_{n,p}(w) \smallsetminus \{0\}} X_{\mathbf{x}}.$$

Denote by $\ell(\mathbf{x})$ the length (size) of the orbit of $\mathbf{x}$, *i.e.* $\ell(\mathbf{x}) = \#\{g \cdot \mathbf{x}, g \in G\}$. We have

$$X'(w) = \sum_{\mathbf{x} \in B_{n,p}(w) \smallsetminus \{0\}} \frac{X_{\mathbf{x}}}{\ell(\mathbf{x})} \tag{8}$$

By writing $\mathrm{P}\left(X(w) > 0\right) = \mathrm{P}\left(X'(w) > 0\right) \leqslant \mathrm{E}\left[X'(w)\right]$ (remark that $X'(w) \in \mathbb{N}$), together with (8) we obtain

$$\mathrm{P}\left(X(w) > 0\right) \leqslant \sum_{\lambda | n} \sum_{\substack{\|\mathbf{x}\|_2 \leqslant w \\ \ell(\mathbf{x}) = \lambda}} \frac{\mathrm{E}\left[X_{\mathbf{x}}\right]}{\lambda}. \tag{9}$$

Since $n = 2q = |G|$ and q is a prime, possible values of λ in (9) are $1, 2, q, n$. Note that $\ell(0) = 1$, $\ell(\mathbf{x}) = 2$ for $\mathbf{x}$ of the form $\mathbf{x} = (\alpha(1, 1, \dots 1), \beta(1, 1, \dots 1))$ and $\ell(\mathbf{x}) \geqslant q$ for all other vectors. In fact a closer look shows that $\ell(\mathbf{x}) = q$ is not possible. For this to happen, one of the two halves of $\mathbf{x}$, call it $\mathbf{y}$, would have all its q cyclic shifts distinct, and the property that

$-\mathbf{y}$ equals some cyclic shift of $\mathbf{y}$. But then it would be possible to partition the set of cyclic shifts of $\mathbf{y}$ into pairs of opposite vectors, but q is an odd prime, a contradiction. Therefore Inequality (9) gets rewritten as

$$\text{(10)}\quad \mathrm{P}\left(X(w)>0\right) \leqslant \sum_{\substack{\mathbf{x}=(\alpha(1,1,\ldots 1),\ \beta(1,1,\ldots 1))\\ 0<\|\mathbf{x}\|_2\leqslant w}} \frac{\mathrm{E}\left[X_{\mathbf{x}}\right]}{2} + \sum_{\substack{\ell(\mathbf{x})=n\\ 0<\|\mathbf{x}\|_2\leqslant w}} \frac{\mathrm{E}\left[X_{\mathbf{x}}\right]}{n}.$$

We now switch to evaluating the right hand side of (10).

3.1. Syndrome distribution

We need to study carefully the quantities $\mathrm{E}\left[X_{\mathbf{x}}\right] = \mathrm{P}\left(\mathbf{x}\in C_{\mathrm{rand}}\right)$, for $\mathbf{x}\in B_{n,p}(w)$. For $\mathbf{x}\in\mathbb{F}_p^n$, let us write $\mathbf{x}=(\mathbf{x}_L,\mathbf{x}_R)$ with $\mathbf{x}_L,\mathbf{x}_R\in\mathbb{F}_p^q$. Consider the syndrome function σ

$$\begin{aligned}\sigma : \mathbb{F}_p^n &\to \mathbb{F}_p^q\\ \mathbf{x} &\mapsto \sigma(\mathbf{x}) = \mathbf{x}\,{}^t\mathbf{H} = \sigma_L(\mathbf{x})+\sigma_R(\mathbf{x})\end{aligned}$$

where $\sigma_L(\mathbf{x})=\mathbf{x}_L$ and $\sigma_R(\mathbf{x})=\mathbf{x}_R\,{}^t\mathbf{A}$.

For any vector $\mathbf{u}=(u_0,\ldots,u_{q-1})$ of $\mathbb{F}_p^q$, denote by $\mathbf{u}(Z)=u_0+u_1Z+\cdots+u_{q-1}Z^{q-1}$ its polynomial representation in the ring $\mathbf{R}=\mathbb{F}_p[Z]/(Z^q-1)$. For any $\mathbf{u}\in\mathbb{F}_p^q$, let $C(\mathbf{u})$ denote the cyclic code of length q generated by the polynomial representation of $\mathbf{u}$ (*i.e.* $C(\mathbf{u})$ is the ideal generated by $\mathbf{u}(Z)$ in the ring $\mathbf{R}$). We have:

Lemma 3. — *The right syndrome $\sigma_R(\mathbf{x})$ of any given $\mathbf{x}\in\mathbb{F}_p^n$ is uniformly distributed in the cyclic code $C(\mathbf{x}_R)$. Therefore, the probability $\mathrm{P}\left(\mathbf{x}\in C_{\mathrm{rand}}\right)$ that $\mathbf{x}$ is a codevector of the random code C_{rand} is*

- $\mathrm{P}\left(\mathbf{x}\in C_{\mathrm{rand}}\right) = 1/|C(\mathbf{x}_R)|$ *if* $\mathbf{x}_L\in C(\mathbf{x}_R)$,
- $\mathrm{P}\left(\mathbf{x}\in C_{\mathrm{rand}}\right) = 0$ *if* $\mathbf{x}_L\notin C(\mathbf{x}_R)$.

Proof. — A little thought shows that $\sigma_R(\mathbf{x})$ has polynomial representation equal to $\mathbf{x}_R(Z)\mathbf{a}(Z)$, where $\mathbf{a}=(a_1,a_q,a_{q-1},\ldots,a_2)$ is the transpose of the first column of $\mathbf{A}$. Therefore, the image of the mapping

$$\begin{array}{rcl}\psi\ :\mathbb{F}_p^q & \to & \mathbb{F}_p^q\\ \mathbf{a} & \mapsto & \sigma_R(\mathbf{x})\end{array}$$

for fixed $\mathbf{x}$, is the cyclic code $C(\mathbf{x}_R)$. Since this mapping is linear, every element of $C(\mathbf{x}_R)$ has the same number of preimages (namely $\operatorname{Ker}\psi$), therefore when the distribution of $\mathbf{a}$ is uniform in $\mathbb{F}_p^q$, the distribution of $\sigma_R(\mathbf{x})$ is uniform in the code $C(\mathbf{x}_R)$. □

3.2. The choice of p and the cyclic codes $C(\mathbf{x}_R)$

The right hand side of (10) will be easiest to study if there are as few as possible cyclic codes in $\mathbb{F}_p^q$, *i.e.* if the ring $\mathbf{R}$ has as few as possible invertible elements, equivalently if Z^q-1 has as few as possible divisors in $\mathbb{F}_p[Z]$. The next lemma tells us how to ensure this, while simultaneously bounding from above the size of p, so as to retain some control over the overall construction complexity.

Lemma 4. — *For any $n=2q$ large enough, there exists a prime p in the range $n^2\log n \leqslant p \leqslant (n^2\log^2 n)^{5.5}$ for which the the factorization of Z^q-1 into irreducible polynomials of $\mathbb{F}_p[Z]$ is*

$$Z^q-1=(Z-1)(1+Z+Z^2+\cdots+Z^{q-1}).$$

Proof. — The polynomial $(1+Z+\cdots+Z^{q-1})\in\mathbb{F}_p[z]$ is irreducible if and only if the set of its roots has exactly one orbit under the group action generated by the Frobenius automorphism $\zeta\to\zeta^p$. Since these roots are q-roots of unity different from 1, we just need to find p in the required range such that $(p \mod q)$ is a primitive element in $(\mathbb{Z}/q\mathbb{Z})^*$.

Let $Q=q^2\mathfrak{p}$ where $\mathfrak{p}$ is a prime such that $4\log n\leqslant\mathfrak{p}\leqslant 4\log^2 n$: $\mathfrak{p}$ exists for q large enough, and we have $n^2\log n\leqslant Q\leqslant n^2\log^2 n$.

Let $\alpha<q$ be a positive integer that is a primitive element in $\mathbb{Z}/q\mathbb{Z}$. Since q is prime we have $q\neq 0 \bmod \mathfrak{p}$ so that we may choose $\varepsilon_1\in\{1,2\}$ and $\varepsilon_2\in\{0,1\}$ such that $r=(1+\varepsilon_1 q)(\alpha+\varepsilon_2 q)$ is coprime to $\mathfrak{p}$ and therefore to Q. Note also that r is smaller than Q for q large enough, not prime, and equal to $\alpha \bmod q$. By Linnik's Theorem on least primes in arithmetic progressions, there exists a prime p such that $p=r \mod Q$ and $p\leqslant Q^L$ for a constant L. We have $p=r=\alpha \mod q$. Note that since r is not prime we have $Q<p$ in addition to $p\leqslant Q^L$. By a result of Heath-Brown [6] we have $L\leqslant 5.5$. □

For p as in Lemma 4 we therefore have exactly two non-trivial cyclic codes over $\mathbb{F}_p$ of length q, namely C_1, the subspace generated by the all-one vector (or the generator polynomial $1+Z+\cdots+Z^{q-1}$) and its dual, $C_1^\perp$, with generator polynomial $Z-1$.

Now Lemma 3 implies that there are exactly two types of non-zero vectors of $\mathbb{F}_p^n$ such that $\mathrm{P}(\mathbf{x}\in C_{\mathrm{rand}})$ is different from zero and from $1/p^q$, namely:

- Vectors $\mathbf{x}$ such that $\mathbf{x}_L\in C_1$ and $\mathbf{x}_R\in C_1$, we call them vectors of type 1. For these vectors we have $\mathrm{P}(\mathbf{x}\in C_{\mathrm{rand}})=1/p$.
- Vectors $\mathbf{x}$ such that $\mathbf{x}_L\in C_1^\perp$ and $\mathbf{x}_R\in C_1^\perp$, we call them vectors of type 2. For these vectors we have $\mathrm{P}(\mathbf{x}\in C_{\mathrm{rand}})=1/p^{q-1}$.

Next, we study the number of these exceptional vectors to evaluate their contribution to the upper bound (10).

3.3. Number of vectors of type 1 and type 2 in $B_{n,p}(\rho)$

Suppose $w = \rho(1+o(1))$ where ρ is defined by $S_n(\rho) = p^q$ (see (2)). Note that in Lemma 4 we have chosen p such that (2) implies $\sqrt{n}/\rho = o(1/n)$. Therefore, (5) implies in turn that

$$|B_{n,p}(w)| = \operatorname{Vol}(S_n(w))\,(1+o(1)). \tag{11}$$

A vector of type 1 in $B_{n,p}(w)$ is a vector $\mathbf{x}$ such that

$$\mathbf{x}_L = \alpha(1,1,\dots,1) \quad \text{and} \quad \mathbf{x}_R = \beta(1,1,\dots,1).$$

The number $N_1(w)$ of possible values of (α,β) such that $\|\mathbf{x}\|_2 \leqslant w$ is,

$$N_1(w) = \#\left\{(\alpha,\beta) \in \mathbb{F}_p^2 \mid \alpha^2\frac{n}{2} + \beta^2\frac{n}{2} \leqslant w^2\right\}.$$

Therefore, for $w < (p-1)/2$ (which is always going to be satisfied for n large enough and p chosen as in Lemma 4),

$$N_1(w) = \#\left\{(\alpha,\beta) \in \mathbb{Z}^2 \mid \alpha^2 + \beta^2 \leqslant \frac{2w^2}{n}\right\}$$

and, bounding from above by the area of a 2-dimensional disc,

$$N_1(w) \leqslant \pi\left(w\sqrt{\frac{2}{n}} + \sqrt{2}\right)^2.$$

Therefore (2) gives

$$N_1(w) \leqslant \frac{p}{e}\big(1+o(1)\big). \tag{12}$$

We now switch to evaluating the cardinality $N_2(w)$ of the set A of vectors of type 2 in $B_{n,p}(w)$. Now let B be the set of vectors $\mathbf{y}$ of $\mathbb{F}_p^n$ obtained by the following procedure:

1. Choose $\mathbf{x} = (x_1 \dots x_n) \in A$;
2. Choose i, j with $1 \leqslant i \leqslant q$, $q+1 \leqslant j \leqslant 2q$;
3. Choose two integers l, r such that $|l| \leqslant \lceil\sqrt{tp}\rceil$ and $|r| \leqslant \lceil\sqrt{tp}\rceil$, where t is a constant to be determined later;
4. Define $\mathbf{y} = (y_1 \dots y_n)$ by $y_i = l$, $y_j = r$ and $y_h = x_h$ for $h \neq i, j$.

We now define the bipartite graph with vertex set $A \cup B$ by putting an edge between $\mathbf{x} \in A$ and $\mathbf{y} \in B$ if $\mathbf{y}$ is obtained from B by the above procedure. Let E be the set of edges of this graph. The degree of a vertex $\mathbf{x} \in A$ is clearly $q^2(2\lceil\sqrt{tp}\rceil+1)^2 \geqslant 4tpq^2$ so that we have $|E| \geqslant |A|4tpq^2$. Recall that $\mathbf{x}$ is of type 2 means that $x_1 + \cdots + x_q = 0$ and $x_{q+1} + \cdots + x_{2q} = 0$. Now let $\mathbf{y} \in B$. There is at most one way of modifying two given coordinates i, j, $1 \leqslant i \leqslant q$, $q+1 \leqslant j \leqslant 2q$, so as to obtain a vector $\mathbf{x} \in A$. In other words the degree of a vertex $\mathbf{y} \in B$ is at most q^2 and $|E| \leqslant |B|q^2$. We have therefore

$$|A| \leqslant \frac{1}{4tp}|B|. \tag{13}$$

Now notice that if $\mathbf{x} \in A$ and $\mathbf{y} \in B$ are adjacent in the bipartite graph we have

$$\|\mathbf{y}\|_2^2 \leqslant \|\mathbf{x}\|_2^2 + 2\lceil\sqrt{tp}\rceil^2$$

so that $B \subset B_{n,p}(w')$ with $w' = \sqrt{w^2 + 2\lceil\sqrt{tp}\rceil^2}$. Since $w = \rho(1+o(1))$, this gives

$$w' = w\sqrt{1 + 2tp\rho^{-2}(1+o(1))}. \tag{14}$$

In particular we have $w' = \rho(1+o(1))$ so that, applying (11), we get

$$\begin{aligned} |B| \leqslant |B_{n,p}(w')| &= \mathrm{Vol}\,(S_n(w'))\,(1+o(1)) = \mathrm{Vol}\,(S_n)\,w'^n(1+o(1)) \\ &= \mathrm{Vol}\,(S_n(w))\,\frac{w'^n}{w^n}(1+o(1)) = |B_{n,p}(w)|\frac{w'^n}{w^n}(1+o(1)). \end{aligned}$$

Now (14) and (2) give:

$$|B| \leqslant |B_{n,p}(w)|\Big(1 + \frac{4te\pi}{n}\Big)^{n/2}(1+o(1)).$$

Together with (13) we obtain the following bound on $N_2(w) = |A|$:

$$N_2(w) \leqslant \frac{e^{2te\pi}}{4tp}|B_{n,p}(w)|(1+o(1)).$$

Now choose $t = (2e\pi)^{-1}$ so as to minimize $e^{2te\pi}/4tp$ and we get:

$$N_2(w) \leqslant \frac{e^2\pi}{2p}|B_{n,p}(w)|(1+o(1)). \tag{15}$$

3.4. Proof of Theorem 1 and Corollary 2

We are now ready to prove the main result.

Proof of Theorem 1 . — Choose p as in Lemma 4 and choose w such that $\mathrm{Vol}\,(S_n(w)) = cnp^{n/2}$, c a constant to be determined later. This clearly implies $w = \rho(1 + o(1))$ so that, by (11), we have $|B_{n,p}(w)| = cnp^{n/2}(1 + o(1))$. The upper bounds (12) and (15) apply and (10) yields:

$$\begin{aligned}\mathrm{P}\,(X(w) > 0) &\leqslant N_1(w)\frac{p^{-1}}{2} + N_2(w)\frac{p^{1-n/2}}{n} + |B_{n,p}(w)|\frac{p^{-n/2}}{n}\\ &\leqslant \frac{1}{2e} + \frac{e^2\pi}{2}c + c + o(1).\end{aligned}$$

We obtain therefore $\mathrm{P}\,(X(w) > 0) < 1$ for n large enough and

$$c < \frac{2 - \frac{1}{e}}{2 + e^2\pi} \approx 0.064.$$

We have proved that for such a value of c, some double circulant codes with minimum norm $d \geqslant w$ must exist. □

Proof of Corollary 2. — Let C be the code in Theorem 1. By inequality (5), since $cnp^{n/2} \leqslant |B_{n,p}(d)|$, the quantity $d + \sqrt{n}/2$ must be greater than the radius of a Euclidean ball of volume $cnp^{n/2}$. As before, by equality (2), the code's minimum norm d must be greater than $\sqrt{pn}$ multiplied by a constant, so that the term $(1 + \sqrt{n}/2d)^{-n}$ in (7) converges to 1 when $n \to \infty$, since $\sqrt{p}/n \to \infty$. Therefore (7) yields the announced density for the lattice deduced from the code C by construction A.

Construction A yields an injective homomorphism from the automorphism group of the code into the automorphism group of the lattice. The construction complexity is simply that of going over all double circulant codes of length n over $\mathbb{F}_p$ (there are $p^{n/2}$ of them), and checking, by exhaustive search over the $p^{n/2}$ codevectors, whether they contain a vector of norm less than the required bound. The resulting complexity equals therefore p^n times quantities of a lesser order of magnitude, *i.e.* $p^{n(1+o(1))}$ which is not more, by Lemma 4, than $2^{2L(1+o(1))n\log_2(n)}$. □

4. Concluding comments

The proof of Theorem 1 shows that, by lowering the value of c, we can make all the contributions to the probability of the existence of a codevector of weight $\leqslant w$ vanish, except for the codevectors of type 1. In other words, for small values of the constant c, the asymptotic probability that the double circulant code-random lattice yields a packing of density less than $cn2^{-n}$ equals the non-vanishing probability (not more than $1 - \frac{1}{2e}$) that codevectors of type 1 exist. When this happens, not only does the packing density drop below $cn2^{-n}$, but it drops below the Minkowski density altogether. In contrast, typical random lattice packings have a density of order $1/2^n$ [11].

The action of the automorphism group of the lattices presented here is not transitive on the set of coordinates, it has two orbits. Can one construct dense lattices having an automorphism group acting transitively on some orthonormal basis?

The automorphism group here has size (at least) n. Could alternative constructions yield an automorphism group of guaranteed larger size (potentially resulting in increased packing densities)?

BIBLIOGRAPHY

[1] R. Bacher, "A new inequality for the Hermite constants", arXiv:math.NT/0603477, 2006.

[2] K. Ball, "A lower bound for the optimal density of lattice packings", *Internat. Math. Res. Notices* **10** (1992), p. 217-221.

[3] J. Conway & N. J. A. Sloane, *Sphere packings, lattices and groups*, vol. 290, Springer-Verlag, New-York (third edition), 1999.

[4] H. Davenport & C. A. Rogers, "Hlawka's theorem in the geometry of numbers", *Duke Math. J.* **14** (1947), p. 367-375.

[5] P. Gaborit & G. Zémor, "Asymptotic improvement of the Gilbert-Varshamov bound for linear codes", in *Inter. Symp. Inf. Theo., ISIT 2006, Seattle*, 2006, p. 287-291.

[6] D. R. Heath-Brown, "Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression", *Proc. London Math. Soc. (3)* **64** (1992), no. 2, p. 265-338.

[7] M. Krivelevich, S. Litsyn & A. Vardy, "A lower bound on the density of sphere packings via graph theory", *Int. Math. Res. Not.* (2004), no. 43, p. 2271-2279.

[8] C. A. Rogers, "Existence theorems in the geometry of numbers", *Ann. of Math. (2)* **48** (1947), p. 994-1002.

[9] J. A. Rush, "A lower bound on packing density", *Invent. Math* **98** (1989), no. 3, p. 499-509.

[10] J. A. Rush & N. J. A. Sloane, "An improvement to the Minkowski-Hlawka bound for packing superballs", *Mathematika* **34** (1987), no. 1, p. 8-18.

[11] S. Shlosman & M. Tsfasman, "Random lattices and random sphere packings: typical properties", *Mosc. Math. J.* **1** (2001), no. 1, p. 73-89.

Manuscrit reçu le 23 juin 2006,
accepté le 29 septembre 2006.

Philippe GABORIT
Université de Limoges, XLIM
123 av. A. Thomas,
87000 Limoges (France)
gaborit@unilim.fr

Gilles ZÉMOR
Université Bordeaux I
351 av. de la Libération
33405 Talence (France)
Gilles.Zemor@math.u-bordeaux1.fr