Can. J. Math., Vol. XXXV, No. 1, 1983, pp. 117–130

NEW LATTICE PACKINGS OF SPHERES

E. S. BARNES AND N. J. A. SLOANE

1. Introduction. In this paper we give several general constructions for lattice packings of spheres in real n-dimensional space $\mathbf{R}^n$ and complex space $\mathbf{C}^n$. These lead to denser lattice packings than any previously known in $\mathbf{R}^{36}, \mathbf{R}^{64}, \mathbf{R}^{80}, \ldots, \mathbf{R}^{128}, \ldots$. A sequence of lattices is constructed in $\mathbf{R}^n$ for $n = 24m \leqq 98328$ (where m is an integer) for which the density Δ satisfies $\log_2 \Delta \approx -(1.25\ldots)n$, and another sequence in $\mathbf{R}^n$ for $n = 2^m$ (m any integer) with

$$\log_2 \Delta \sim -\tfrac{1}{2} n \log_2 \log_2 n.$$

The latter appear to be the densest lattices known in very high dimensional space. (See, however, the Remark at the end of this paper.) In dimensions around 2^{16} the best lattices found are about 2^{131000} times as dense as any previously known.

Minkowski proved in 1905 (see [**20**] and Eq. (23) below) that lattices exist with $\log_2 \Delta > -n$ as $n \to \infty$, but no infinite family of lattices with this density has yet been constructed. Lattices with $\log_2 \Delta \sim -\frac{1}{4} n \log_2 n$ were given in [**2**] (see also 2.2(e) below), nonlattice packings with $\log_2 \Delta \sim -\frac{1}{2} n \log_2 \log_2 n$ were given in [**14**], [**15**], and nonlattices with $\log_2 \Delta > -6n + o(n)$ in [**21**]. The latter two families of packings were obtained by applying Construction C of [**15**] to certain sequences of codes.

Our first construction, Construction D (see 2.1), resembles Construction C in that it is also based on a sequence of codes, but differs in producing lattices provided only that the codes are binary, linear and nested. In this way we obtain new record densities for lattices in dimensions 36, 64, etc., and an infinite sequence of lattices with

$$\log_2 \Delta \sim -\tfrac{1}{2} n \log_2 \log_2 n$$

(see 2.2(f) and Table I). We also give a complex version of Construction D (2.3), which applies to codes over $GF(3)$ and $GF(4)$, and another version, Construction D′ (2.5), which defines a new lattice by congruences (obtained from the parity-check equations defining a nested family of codes) rather than by a set of generating vectors.

In a recent paper Bos [**3**] has generalized Construction C so as to combine several copies of an m-dimensional lattice Λ to produce what is

Received September 28, 1981 and in revised form December 4, 1981. The first author gratefully acknowledges the support of the Mathematics Department of the University of Toronto during the final preparation of this paper.

TABLE I Center density δ of n-dimensional lattice packing B_n obtained from BCH codes. (*: equals old record; **: new record)

n	$\log_2 \delta$	n	$\log_2 \delta$	n	$\log_2 \delta$
4	−3*	256	250**	16384	57819**
8	−4*	512	698**	32768	130510**
16	−4*	1024	1817**	65536	290998**
32	0*	2048	4502**	131072	642300**
64	19	4096	10794**	...	...
128	85	8192	25224**		

in general a nonlattice packing in dimension mn (Construction C is the case $m = 1$). In Section 3 we give a new general construction which was inspired by Bos's, but differs from it in always producing lattices. Our construction also differs from his in making essential use of a certain linear transformation T that maps the minimal vectors of Λ into "deep holes" in that lattice, i.e., into points of $\mathbf{R}^m$ which are at maximal distance from the nearest point of Λ (cf. [**7**], [**10**]). By means of this construction we are able to construct several new and very dense lattices having the same density as Bos's nonlattice packings (see 3.7 and Table II). Furthermore, using knowledge of the holes in the Leech lattice (see [**7**], [**9**], [**10**]), we use that lattice to construct the extremely good sequence of lattices in dimensions $24m \leqq 98328$ mentioned in the opening paragraph (see 3.7(d) and Table III). Finally, Table IV shows the quite spectacular improvement obtained in dimensions around 2^{16}.

Notation. (See [**15**], [**17**], [**20**], [**22**].) The norm of a vector x is its squared length $x \cdot x$. The minimal norm M of a lattice L in $\mathbf{R}^n$ is min $\{x \cdot x | x \in L, x \neq 0\}$, its determinant det L is the volume of a fundamental parallelepiped, and the density of the packing is

$$\Delta = (\tfrac{1}{2}\sqrt{M})^n V_n/\det L,$$

where V_n is the volume of a sphere of radius 1 in $\mathbf{R}^n$. The center density $\delta = \Delta/V_n$.

An $[n, k, d]$ code over $GF(q)$ is a linear code containing q^k codewords of length n separated by a Hamming distance of at least d.

2. Constructions D and D′.

2.1 *Construction* D. This construction uses a nested family of binary codes to produce a lattice packing L in $\mathbf{R}^n$. It generalizes a construction of Barnes and Wall [**2**], and has some features in common with Construction C of [**15**], although differing from it in always producing lattice packings.

Let $\gamma = 1$ or 2, and let $C_0 \supseteq C_1 \supseteq \ldots \supseteq C_a$ be binary linear codes, where C_i has parameters $[n, k_i, d_i]$, with $d_i \geqq 4^i/\gamma$ for $i = 1, \ldots, a$,

https://doi.org/10.4153/CJM-1983-008-1 Published online by Cambridge University Press

and C_0 is the trivial $[n, n, 1]$ code $GF(2)^n$. Choose a basis $c_1, \ldots, c_n$ for $GF(2)^n$ such that $c_1, \ldots, c_{k_i}$ span C_i for $i = 0, \ldots, a$. Define the map $\sigma_i : GF(2) \rightarrow \mathbf{R}$ by $\sigma_i(x) = x/2^{i-1}$ ($x = 0$ or 1), for $i = 1, \ldots, a$, and let the same symbol σ_i denote the map $GF(2)^n \rightarrow \mathbf{R}^n$ given by

$$\sigma_i(x_1, \ldots, x_n) = (\sigma_i(x_1), \ldots, \sigma_i(x_n)).$$

Also let $k_{a+1} = 0$. Then the new lattice L in $\mathbf{R}^n$ consists of all vectors of the form

$$(1) \qquad l + \sum_{i=1}^{a} \sum_{j=1}^{k_i} \alpha_j^{(i)} \sigma_i(c_j),$$

where $l \in (2\mathbf{Z})^n$ and $\alpha_j^{(i)} = 0$ or 1.

THEOREM 1. *L is a lattice, with minimal norm at least $4/\gamma$, determinant*

$$(2) \qquad \det(L) = 2^{n - \sum_{i=1}^{a} k_i}$$

and hence center density

$$(3) \qquad \delta \geqq \gamma^{-n/2} 2^{\sum_{i=1}^{a} k_i - n}.$$

This is a consequence of Theorem 3 below.

An integral basis for L is given by the vectors $\sigma_i(c_j)$ for $i = 1, \ldots, a$, $j = k_{i+1} + 1, \ldots, k_i$, plus $n - k_1$ vectors of the shape $(0, \ldots, 0, 2, 0, \ldots, 0)$.

2.2. *Examples.* (a) If $a = \gamma = 1$ and C_1 has minimum distance 4, Construction D coincides with an important special case of Construction A of [**15**]. A typical example is obtained when C_1 is the [8, 4, 4] Hamming code (see [**17**]). We may take

$$\begin{aligned}
c_1 &= (1, 1, 1, 1, 0, 0, 0, 0),\\
c_2 &= (0, 0, 0, 0, 1, 1, 1, 1),\\
c_3 &= (1, 1, 0, 0, 1, 1, 0, 0),\\
c_4 &= (1, 0, 1, 0, 1, 0, 1, 0),\\
c_5 &= (1, 0, 0, 0, 0, 0, 0, 0),\\
c_6 &= (0, 1, 0, 0, 0, 0, 0, 0),\\
c_7 &= (0, 0, 1, 0, 0, 0, 0, 0),\\
c_8 &= (0, 0, 0, 0, 1, 0, 0, 0).
\end{aligned}$$

Then L is a version of the E_8 lattice (see [**5**], [**10**], [**15**]), is spanned by

https://doi.org/10.4153/CJM-1983-008-1 Published online by Cambridge University Press

the rows of the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}$$

and has minimal norm 4, determinant 2^4, and $\delta = 2^{-4}$.

(b) When $a = \gamma = 2$, C_1 is the trivial $[n, n-1, 2]$ code, and C_2 has minimum distance 8, Construction D coincides with an important special case of Construction B of [**15**]. For example if C_2 is the [16, 5, 8] Reed-Muller code (see [**17**]) we obtain Barnes and Wall's 16-dimensional lattice Λ_{16} with center density $\delta = 2^{-4}$ (see [**2**], [**10**], [**15**]).

(c) Whenever Construction C of [**15**] can be applied to codes which are linear and nested, Construction D produces a lattice packing with the same density.

For example let C_1 and C_3 be the trivial [36, 35, 2] and [36, 1, 36] codes, and let C_2 be the [36, 20, 8] code found by Rao and Reddy [**19**]. Then L is a 36-dimensional lattice with $\delta = 4$, a new record. Similarly one can obtain $\delta = \sqrt{2}$, 2 and $2\sqrt{2}$ in dimensions 33, 34 and 35 respectively. Bos [**3**] had used Construction C with these codes to obtain nonlattice packings with the same densities.

(d) We obtain a new record of $\delta = 2^{22}$ for lattice packings in $\mathbf{R}^{64}$ using the following sequence of extended cyclic codes: $[64, 64, 1] \supseteq [64, 57, 4] \supseteq [64, 28, 16] \supseteq [64, 1, 64]$ (cf. § 6.6 of [**15**]).

(e) Generalizing Example (b), if the C_i are all Reed-Muller codes of length $n = 2^m$, we obtain a sequence of lattices found by Barnes and Wall [**2**]. Asymptotically these have $\log_2 \Delta \sim -\frac{1}{4} n \log_2 n$, and contact number

$$\tau = (2 + 2)(2 + 2^2) \ldots (2 + 2^m) \sim 4.768 \ldots 2^{m(m+1)/2}.$$

Nonlattice packings with the same parameters had been obtained in [**15**] using Construction C.

(f) Similarly the 2^m-dimensional nonlattice packings $P2^m b$ obtained from BCH codes in [**15**] may now be converted to equally dense lattice packings B_{2^m}. We have calculated their density by computer for $m \leqq 17$, and the results are shown in Table I. The BCH bound [**17**, Chapter 7] was used to estimate the dimension of the codes involved, so except in small dimensions the actual density of these packings may be slightly greater than is shown in the table. (Tables of BCH codes of modest length are given in [**17**], [**18**].) In Tables I–III, a star indicates that the density equals the old record for a lattice packing, while two stars indicate a new record. Asymptotically the density of B_n, $n = 2^m$, satisfies

$$\log_2 \Delta \sim -\tfrac{1}{2} n \log_2 \log_2 n$$

(as was proved for the corresponding nonlattice packings in [**15**]). For $n \geqq 2^{17}$ these seem to be the densest lattices yet constructed, although for $500 < n \leqq 98328$ we shall construct denser lattices in 3.7(d). The contact number of B_{2^m} is at present unknown.

2.3. *A complex version of Construction* D. Just as Constructions A and B of [**15**] can be generalized to complex lattices (see [**23**], [**24**]), so can Construction D. We shall give a version which is applicable to codes over $GF(3)$ and $GF(4)$, although since this has not yet led to any new lattices our treatment will be brief.

The lattices produced are $\mathbf{Z}[\omega]$-modules in $\mathbf{C}^n$, where $\omega = e^{2\pi i/3}$, or in other words they are closed under addition and under scalar multiplication by the Eisenstein integers $\mathbf{E} = \{a + b\omega | a, b \in \mathbf{Z}\}$. The construction works because $\theta = 1 + 2\omega = \sqrt{-3}$ and 2 are primes in $\mathbf{E}$ with $\mathbf{E}/\theta\mathbf{E} \cong GF(3)$ and $\mathbf{E}/2\mathbf{E} \cong GF(4)$ (see [**24**]).

The complex Construction D. Let $\pi = \theta$ and $q = 3$, or $\pi = 2$ and $q = 4$. Let $C_0 \supseteq C_1 \supseteq \ldots \supseteq C_a$ be linear codes over $GF(q)$, where C_i has parameters $[n, k_i, d_i]$ and C_0 is the trivial $[n, n, 1]$ code. Choose a basis $c_1, \ldots, c_n$ for $GF(q)^n$ such that $c_1, \ldots, c_{k_i}$ is a basis for C_i, $i = 0, \ldots, a$. Define $\sigma_i(x) = \pi^{-(i-1)} \cdot x$ and $k_{a+1} = 0$. Then the new lattice L in $\mathbf{C}^n$ consists of all Eisenstein-integral combinations of the vectors $l \in \mathbf{E}^n$ and $\sigma_i(c_j)$, for $i = 1, \ldots, a$ and $k_{i+1} + 1 \leqq j \leqq k_i$.

2.4. *Examples.* (a) With $\pi = \theta$ and $a = 1$, the trivial [3, 1, 3] ternary code produces a complex 3-dimensional lattice for which the corresponding 6-dimensional real lattice is the root lattice E_6 (cf. [**24**, § 5.8.2]). This is perhaps the simplest presentation of E_6.

(b) When $\pi = \theta$, $a = 1$ and C_1 is the [4, 2, 3] ternary code we obtain a complex 4-dimensional version of E_8 (cf. [**24**, § 5.8.3]).

(c) When $\pi = \theta$, $a = 2$ and C_1, C_2 are the trivial [6, 5, 2] and [6, 1, 6] ternary codes, we obtain a complex 6-dimensional version of the Coxeter-Todd lattice K_{12} (see [**11**], [**24**, § 5.8.5]).

(d) When $\pi = 2$, $a = 1$ and C_1 is the [6, 3, 4] hexacode over $GF(4)$ we again get K_{12} ([**24**, § 5.7.3]).

2.5. *Construction* D′. This construction generalizes another of the constructions in [**2**], and converts a set of parity-checks defining a family of codes into congruences for a lattice, in the same way that Construction D converts a set of generators for a family of codes into generators for a lattice.

https://doi.org/10.4153/CJM-1983-008-1 Published online by Cambridge University Press

Let $\gamma = 1$ or 2, and let $C_0 \supseteq C_1 \supseteq \ldots \supseteq C_a$ be binary linear codes, where C_i has parameters $[n, k_i, d_i]$ and $d_i \geqq \gamma \cdot 4^i$ for $i = 0, \ldots, a$. Let $h_1, \ldots, h_n$ be linearly independent vectors in $GF(2)^n$ such that, for $i = 0, \ldots, a$, C_i is defined by the $r_i = n - k_i$ parity-check vectors $h_1, \ldots, h_{r_i}$, and let $r_{-1} = 0$. Considering the vectors h_j as integral vectors in $\mathbf{R}^n$, with components 0 or 1, we define the new lattice L' to consist of those $x \in \mathbf{Z}^n$ that satisfy the congruences

$$(4) \qquad h_j \cdot x \equiv 0 (\mathrm{mod}\ 2^{i+1})$$

for all $i = 0, \ldots, a$ and $r_{a-i-1} + 1 \leqq j \leqq r_{a-i}$.

THEOREM 2. *The minimal norm of L' is at least $\gamma \cdot 4^a$, and*

$$(5) \qquad \det L' = 2^{\sum_{i=0}^{a} r_i}.$$

Proof. (5) holds because for each $i = 0, \ldots, a$ the lattice satisfies $r_{a-i} - r_{a-i-1}$ independent congruences modulo 2^{i+1}. The proof of the minimal norm is straightforward and is omitted.

By changing the scale and relabelling the codes, Construction D may be restated in such a way that the norms and determinants of L and L' agree. Then if the C_i are Reed-Muller codes, as in Example 2.2(e), the two lattices coincide. In general however the two constructions produce inequivalent lattices with the same density.

3. A new general construction. The following rather general construction includes Construction D as a special case. Starting with a lattice Λ in $\mathbf{R}^m$ that satisfies certain conditions, we form a new lattice in $\mathbf{R}^{mn}$ from a union of cosets of $\Lambda^n = \Lambda \oplus \Lambda \oplus \ldots \oplus \Lambda$, the cosets being specified by a family of linear codes $C_0 \supseteq C_1 \supseteq \ldots \supseteq C_a$ over a field $GF(2^b)$. Construction D corresponds to the case $m = 1$, $\Lambda = 2\mathbf{Z}$.

3.1. *Conditions to be satisfied by* Λ. We assume that Λ satisfies four conditions.

(i) The minimal vectors of Λ span Λ.

(ii) There is a linear map T from $\mathbf{R}^m$ to $\mathbf{R}^m$ that sends all the minimal vectors of Λ into elements of $\frac{1}{2}\Lambda$ which have norm R^2 and are at a distance R from Λ.

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

$$(6) \qquad T^\nu = \tfrac{1}{2}A$$

and

$$(7) \qquad \tfrac{1}{2}(A^2 - A) = \sum_{i=0}^{\nu-1} a_i T^i, \quad a_i \in \mathbf{Z}.$$

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

https://doi.org/10.4153/CJM-1983-008-1 Published online by Cambridge University Press

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

(8) $\quad [T\Lambda : \Lambda] = q.$

It follows from (6) that $T = tP$ where $t = 2^{-1/\nu}$ and P is an orthogonal transformation satisfying $P^\nu = A$. If M is the minimal norm of Λ, we have $t = R/\sqrt{M}$, and from (8)

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

These conditions are quite restrictive, but as we shall see there are several lattices which satisfy them. Condition (7) is imposed only to ensure that the new packing is a lattice, and the construction (see 3.6) may still be successful even if (7) fails. In most of our examples $A = I$ and (7) is trivially satisfied. The construction may be generalized to allow T to map Λ into $(1/p)\,\Lambda$ for a prime $p > 2$, although we shall not discuss this in the present paper.

3.2. *Examples.* In these examples R is the covering radius of Λ and T maps the minimal vectors of Λ into deep holes in Λ (cf. [**7**], [**10**]).

(a) Take $\Lambda = 2\mathbf{Z}$, $T = \frac{1}{2}I$, where I denotes the identity map; then $m = \nu = 1$, $t = \frac{1}{2}$, $A = I$ and $q = 2$.

(b) Let Λ be the root lattice D_4 (see [**1**], [**5**], [**8**], [**15**]), in the version in which the minimal vectors have the shape $(\pm 2^1, 0^3)$ and $(\pm 1^4)$, and let

$$T = \tfrac{1}{2}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix};$$

then T does map the minimal vectors of D_4 into the 24 deep holes with coordinates of the shape $(\pm 1^2, 0^2)$ and $m = 4$, $\nu = 2$, $t = 1/\sqrt{2}$, $A = I$ and $q = 4$.

(c) Let Λ be the version of E_8 constructed in Example 2.2(a), with minimal vectors of the shape $(\pm 2^1, 0^7)$ and $(\pm 1^4, 0^4)$, and let

$$T = \tfrac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix};$$

then $m = 8, \nu = 2, t = 1/\sqrt{2}, A = I$ and $q = 2^4$. Again it is easy to check that T maps minimal vectors into deep holes (cf. [**8**], [**10**]).

(d) Let Λ be the Leech lattice Λ_{24} ([**6**], [**13**], [**15**]) in Miracle Octad Generator (or MOG) coordinates (see [**7**], [**10**]), with det $\Lambda = 1$, $M = 4$, and $R = \sqrt{2}$. We take $T = \frac{1}{2}(I + i)$, where i is the element of the Conway group Aut $(\Lambda_{24}) = \cdot 0$ shown in Figure 1. This element satisfies

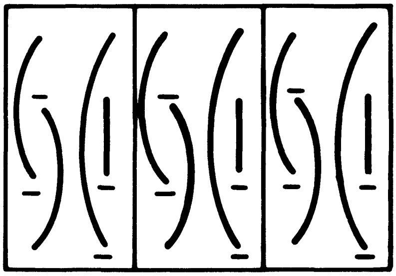

FIGURE 1. The element i of Aut (Λ_{24}) in MOG notation. In the first column the 1st and 3rd components are to be exchanged, and the 2nd and 4th, and then the 2nd and 3rd components are negated. Similarly for the other columns.

$i^2 = -I$, and T maps the minimal vectors of Λ_{24} into deep holes of type $A_1{}^{24}$ (see [**7**], [**9**]). We have $m = 24$, $\nu = 2$, $t = 1/\sqrt{2}$, $A = i$ and $q = 2^{12}$. Equation (7) reads

$$\tfrac{1}{2}(i^2 - i) = -T.$$

3.3. *The lattices* Λ_i. Let $v_1, \ldots, v_m$ be minimal vectors of Λ that span Λ. Then $Tv_1, \ldots, Tv_m$ span the lattice $T\Lambda$. From (8), $T\Lambda/\Lambda$ is an elementary abelian group of order $q = 2^b$, so that there are b vectors

$$u_1{}^{(1)} = Tv_{r_1}, \ldots, u_b{}^{(1)} = Tv_{r_b},$$

for appropriate $r_1, \ldots, r_b$, such that $T\Lambda/\Lambda$ is isomorphic to the modulo-2 span of $u_1{}^{(1)}, \ldots, u_b{}^{(1)}$. Define

$$\Lambda_i = T^i\Lambda,$$
$$u_j{}^{(i)} = T^i v_{r_j} \in \Lambda_i, j = 1, \ldots, b,$$

for all $i \in \mathbf{Z}$. The lattice Λ_i has minimal norm $t^{2i}M$, and

(10) $\quad$ dist $(u_j{}^{(i)}, \Lambda_{i-1}) \geqq t^{i-1}R.$

The vectors in Λ will be said to have *level* 0, and those in $\Lambda_i \backslash \Lambda_{i-1}$ for some $i = 1, 2, \ldots$ to have *level* i.

3.4. *The maps* σ_i. Let $\omega_1, \ldots, \omega_b$ be generators for $GF(2^b)$ over $GF(2)$, so that a typical element of $GF(2^b)$ can be written as

$$\sum_{j=1}^{b} \alpha_j \omega_j, \quad \alpha_j = 0 \text{ or } 1.$$

Define $\sigma_i : GF(2^b) \to \Lambda_i$ by

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

where on the right-hand side α_j is regarded as a real number. We use the same symbol σ_i for the map $GF(2^b)^n \to \mathbf{R}^{mn}$ given by

(11) $\sigma_i(\xi_1, \ldots, \xi_n) = (\sigma_i(\xi_1), \ldots, \sigma_i(\xi_n)).$

Note that, for $\xi \in GF(2^b)$, $\sigma_i(\xi) = 0$ if and only if $\xi = 0$; hence in (11) the number of nonzero components on the right-hand side is equal to the Hamming weight of $(\xi_1, \ldots, \xi_n)$, and the norm of the right-hand side of (11) is at least

(12) $t^{2i-2}R^2 \cdot wt(\xi_1, \ldots, \xi_n).$

3.5. *The codes* C_i. Let $C_0 \supseteq C_1 \supseteq \ldots \supseteq C_a$ be linear codes over $GF(2^b)$, where C_i has parameters $[n, k_i, d_i]$ and C_0 is the trivial $[n, n, 1]$ code. Set $C_i = C_0$ for $i < 0$. Choose vectors $c_1, \ldots, c_{bn}$ in $GF(2^b)^n$ such that

$$C_i = \left\{\sum_{j=1}^{bk_i} \alpha_j c_j | \alpha_j = 0 \text{ or } 1\right\}$$

for all $i \in \mathbf{Z}$.

3.6. *The construction.* Finally, after these preliminaries, we can give the construction. The new lattice L in $\mathbf{R}^{mn}$ consists of all vectors of the form

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

where $l \in \Lambda^n$ and $\alpha_j^{(i)} = 0$ or 1. If $x = (x_1, \ldots, x_n)$, $x_i \in \mathbf{R}^m$, we call the x_i the *components* of x.

THEOREM 3. *L is a lattice and is fixed under the transformation $\hat{A}$ which applies A simultaneously to each component. The minimal norm of L is*

(14) $\bar{M} = \min\left\{M, \frac{d_i R^{2i}}{M^{i-1}} \textit{for } i = 1, \ldots, a\right\},$

and its determinant is

(15) $\det L = \frac{(\det \Lambda)^n}{\prod_{i=1}^{a} 2^{bk_i}}.$

The center density of L is

(16) $\bar{M}^{mn/2}/2^{mn} \det L.$

Proof. Let the *level* of a vector $x \in L$ of the form (13) be the largest level of any of the components of x. Then the $\alpha_j^{(i)}$ in (13) are zero when i

exceeds the level of x. Let L_i consist of all points in L of level $\leqq i$, so that $L_0 = \Lambda^n$, and

$$L_i = \left\{ y + \sum_{j=1}^{bk_i} \alpha_j^{(i)} \sigma_i(c_j) \,|\, y \in L_{i-1}, \alpha_j^{(i)} = 0 \text{ or } 1 \right\}$$

for $i = 1, \ldots, a$. We first prove that L_i is a lattice fixed under $\hat{A}$, using induction on i. This is trivially true for $i = 0$. For the inductive step we shall show that $-\sigma_i(c_j)$ and $\hat{A}\,\sigma_i(c_j)$ are in L_i for all $j = 1, \ldots, bk_i$.

Let $\hat{T}$ be the transformation which applies T simultaneously to each component, so that $\hat{T}^\nu = \frac{1}{2}\hat{A}$. From the definition of σ_i we have

$$(17) \quad \sigma_i(c_j) = \hat{T}^h \sigma_{i-h}(c_j),$$

for $1 \leqq j \leqq bk_i$ and $h = 0, 1, 2, \ldots$. When $h = \nu$ we obtain

$$(18) \quad 2\sigma_i(c_j) = \hat{A}\sigma_{i-\nu}(c_j),$$

$$(19) \quad -\sigma_i(c_j) = \sigma_i(c_j) - \hat{A}\,\sigma_{i-\nu}(c_j).$$

It follows from (7) that

$$2\hat{T}^\nu \cdot \hat{T}^\nu \sigma_{i-\nu}(c_j) = \hat{T}^\nu \sigma_{i-\nu}(c_j) + \sum_{h=0}^{\nu-1} a_h \hat{T}^h \sigma_{i-\nu}(c_j)$$

for $1 \leqq j \leqq bk_i$, $i = 1, 2, \ldots$, or in other words

$$(20) \quad \hat{A} \cdot \sigma_i(c_j) = \sigma_i(c_j) + \sum_{h=0}^{\nu-1} a_h \sigma_{i+h-\nu}(c_j).$$

The identity (19) proves that L_i is closed under subtraction (since, by induction, $\hat{A}\sigma_{i-\nu}(c_j) \in L_{i-\nu} \subseteq L_{i-1}$) and hence is a lattice; and (20) shows that $\hat{A}$ leaves L_i invariant. Since $L_a = L$, this proves the first statement of the theorem.

It is easy to see that the representation (13) of a point x is unique, and so L is the union of $\prod_{i=1}^{a} 2^{bk_i}$ cosets of Λ^n. This implies (16).

Finally, to show that the minimal norm of L is given by (14), let $x \neq 0$ be a point of level i. If $i = 0$ then $N(x) \geqq M$ by the definition of M. If $i > 0$ we can write $x = y + z$, where $y \in L_{i-1}$ and

$$z = \sum_{j=1}^{bk_i} \alpha_j^{(i)} \sigma_i(c_j) \neq 0.$$

Since $T\Lambda \subseteq \frac{1}{2}\Lambda$, $2\sigma_i(\xi) \in \Lambda_{i-1}$ for all $\xi \in GF(2^b)$. Hence $x = y' + z'$ where $y' \in L_{i-1}$ and $z' \neq 0$ has level i. Also z' has at least d_i components of level i, namely those in the same positions as the codeword

$$\sum_{j=1}^{bk_i} \alpha_j^{(i)} c_j$$

of C_i. From (12) the norm of z (and therefore of x) is at least

$$d_i t^{2i-2} R^2 = d_i R^{2i}/M^{i-1}.$$

https://doi.org/10.4153/CJM-1983-008-1 Published online by Cambridge University Press

3.7. *Examples* (*continued*). (a) (continued). When $\Lambda = 2\mathbf{Z}$ we obtain Construction D. Theorem 1 then follows from Theorem 3.

(c) (continued). Using $\Lambda = E_8$ we obtain a number of good lattice packings in dimension $\leqq 136$. We take

$$u_1^{(1)} = (1, 1, 0, 0, 0, 0, 0, 0),$$
$$u_2^{(1)} = (1, 0, 1, 0, 0, 0, 0, 0),$$
$$u_3^{(1)} = (1, 0, 0, 0, 1, 0, 0, 0),$$
$$u_4^{(1)} = (\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}),$$

and let C_i be an $[n, k_i = n - 2^i + 1, d_i = 2^i]$ maximal distance separable code over $GF(2^4)$ (see [**17**, Chapter 11, Theorem 9]). C_i exists provided $2^i \leqq n \leqq 17$. The resulting lattices, which exist in dimensions $N = 8n$ for $n \leqq 17$, have the density shown in Table II. In dimensions 8, 16, 32 and

TABLE II Center density δ of N-dimensional lattices obtained from E_8.

n	N	$\log_2 \delta$	n	N	$\log_2 \delta$	n	N	$\log_2 \delta$
1	8	−4*	7	56	12	13	104	60**
2	16	−4*	8	64	20	14	112	68**
3	24	−4	9	72	28**	15	120	76**
4	32	0*	10	80	36**	16	128	88**
5	40	4*	11	88	44**	17	136	100**
6	48	8	12	96	52**			

40 this density agrees with the present record (see [**10**], [**15**]), in dimensions 24, 48, . . . , 72 it is poor, but in dimensions 80, 88, . . . , 136 these appear to have a greater density than any lattice previously known. Bos [**3**] had earlier found nonlattice packings with the same parameters.

(d) (continued). Here $\Lambda = \Lambda_{24}$ and we take C_i to be an $[n, k_i = n - 2^i + 1, d_i = 2^i]$ maximal distance separable code over $GF(2^{12})$. C_i exists provided $2^i \leqq n \leqq 4097$. The construction gives a lattice Q_N in dimension $N = 24n$, for $1 \leqq n \leqq 4097$, for which the center density δ satisfies

$$(21) \quad \log_2 \delta = 12((m-1)n - 2^m + m + 1)$$

if $2^{m-1} \leqq n \leqq 2^m - 1$. Some examples are shown in Table III. The case $n = 2$ is the laminated lattice Λ_{48} (see [**10**]). We see that while the density of Q_N is poor for $N \leqq 150$, for $150 \leqq N \leqq 500$ it is quite respectable, and for $500 < N \leqq 24 \cdot 4097 = 98328$ these are easily the densest (lattice or nonlattice) packings known. Thus when $n = 2^m - 1$ the unnormalized density Δ of $Q_N \subseteq \mathbf{R}^N$, $N = 24n$, satisfies

$$(22) \quad \log_2 \Delta = -1.25 \ldots N + O(\log_2 N),$$

https://doi.org/10.4153/CJM-1983-008-1 Published online by Cambridge University Press

TABLE III Center density δ of N-dimensional lattices Q_N obtained from the Leech lattice

n	N	$\log_2 \delta$	n	N	$\log_2 \delta$	n	N	$\log_2 \delta$
1	24	0*	10	240	228	171	4104	11400**
2	48	12	11	264	264	342	8208	26808**
3	72	24	21	504	696**	683	16392	61608**
4	96	48	22	528	744**	1366	32784	139488**
5	120	72	43	1032	1896**	2731	65544	311496**
6	144	96	86	2064	4752**	4097	98328	491832**

from (21) (the coefficient of N is $-\frac{1}{2}\log_2(48/e\pi)$), which is not far off the Minkowski lower bound

$$(23) \quad \Delta \geqq \frac{\zeta(n)}{2^{n-1}}$$

(see [**20**, p. 4]). Unfortunately the maximal distance separable codes needed to construct Q_N have only been constructed for $n \leqq 4097$ (see [**17**, Chapter 11]). Beyond that one may use BCH codes over $GF(2^{12})$ [**17**, Chapter 9], but the results are not so impressive. Table IV compares

TABLE IV Comparison of center densities in dimensions near 65536

lattice	$\log_2 \delta$
Barnes and Wall (in $\mathbf{R}^{65536}$)	180224
B_{65536}	290998
Q_{65520}	311364
Q_{65544}	311496
Bounds in $\mathbf{R}^{65536}$:	
Minkowski lower bound	324603
Levenshtein (1979) upper bound	353768
Rogers upper bound	357385

the various densities in dimensions around 65536. This table gives Barnes and Wall's lattice [**2**] (the old record for a lattice), the BCH lattice B_{65536} (whose density is equal to the old record for a nonlattice packing), Q_N for values of N bracketing 65536, the Minkowski lower bound (23), the Rogers upper bound [**15**, p. 743], and Levenshtein's 1979 upper bound (see [**16**, Eq. (22)] and [**4**]). (The Kabatiansky and Levenshtein upper bound (see [**12**], [**25**]) appears to be weaker than the last two bounds in this dimension.)

Acknowledgment. We are grateful to A. Bos for allowing us to see a preprint of [**3**].

Added in proof. In a sequel to this paper even denser lattices have been constructed in $\mathbf{R}^n$, for n very large. See A. Bos, J. H. Conway and N. J. A. Sloane, *Further lattice packings in high dimensions*, Mathematika *29* (1982), 171–180.

References

1. E. S. Barnes, *The construction of perfect and extreme forms*, Acta Arithmetica *5* (1959), 57–79 and 205–222.

2. E. S. Barnes and G. E. Wall, *Some extreme forms defined in terms of Abelian groups*, J. Australian Math. Soc. *1* (1959), 47–63.

3. A. Bos, *Sphere packings in high-dimensional space*, preprint.

4. ——— *Upper bounds for sphere-packings in Euclidean space*, IEEE Trans. Information Theory, to appear.

5. N. Bourbaki, *Groupes et algèbres de Lie, Chapitres IV, V, VI* (Hermann, Paris, 1968).

6. J. H. Conway, *A characterisation of Leech's lattice*, Inventiones Math. *7* (1969), 137–142.

7. J. H. Conway, R. A. Parker and N. J. A. Sloane, *The covering radius of the Leech lattice*, Proc. Royal Soc. London, A*380* (1982), 261–290.

8. J. H. Conway and N. J. A. Sloane, *Voronoi regions of lattices, second moments of polytopes, and quantization*, IEEE Trans. Information Theory, IT-28 (1982), 211–226.

9. ——— *Twenty-three constructions for the Leech lattice*, Proc. Royal Soc. London (A)*381* (1982), 275–283.

10. ——— *Laminated lattices*, Annals of Math. *116* (1982), in press.

11. H. S. M. Coxeter and J. A. Todd, *An extreme duodenary form*, Can. J. Math. *5* (1953), 384–392.

12. G. A. Kabatiansky and V. I. Levenshtein, *Bounds for packings on a sphere and in space* (in Russian), Problemy Peredachi Informatsii *14*, No. 1 (1978), 3–25. English translation in Problems of Information Transmission *14*, No. 1 (1978), 1–17.

13. J. Leech, *Notes on sphere packings*, Can. J. Math. *19* (1967), 251–267.

14. J. Leech and N. J. A. Sloane, *New sphere packings in more than* 32 *dimensions*, Proc. Second Chapel Hill Conference on Combinatorial Mathematics and its Applications, Univ. of North Carolina at Chapel Hill (1970), 345–355.

15. ——— *Sphere packings and error-correcting codes*, Can. J. Math. *23* (1971), 718–745.

16. V. I. Levenshtein, *On bounds for packings in n-dimensional Euclidean space* (in Russian), Dokl. Akad. Nauk SSSR *245*, No. 6 (1979), 1299–1303. English translation in Soviet Math. Doklady *20*, No. 1 (1979), 417–421.

17. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes* (North-Holland, Amsterdam, 1977).

18. W. W. Peterson and E. J. Weldon, Jr., *Error-correcting codes* (MIT Press, Cambridge, MA, 2nd edition, 1972).

19. V. V. Rao and S. M. Reddy, *A* (48,31,8) *linear code*, IEEE Trans. Information Theory, IT-19 (1973), 709–711.

20. C. A. Rogers, *Packing and covering* (Cambridge University Press, Cambridge, 1964).

21. N. J. A. Sloane, *Sphere packings constructed from BCH and Justesen codes*, Mathematika *19* (1972), 183–190.

22. ——— *Binary codes, lattices and sphere packings*, in *Combinatorial Surveys* (Proc. 6th British Combinatorial Conference), (Academic Press, London, 1977), 117–164.

23. ——— *Codes over* $GF(4)$ *and complex lattices*, J. Algebra *52* (1978), 168–181.
24. ——— *Self-dual codes and lattices*, in *Relations between combinatorics and other parts of mathematics*, Proc. Sympos. Pure Math. *34* (Amer. Math. Soc., Providence, RI, 1979), 273–308.
25. ——— *Recent bounds for codes, sphere packings and related problems obtained by linear programming and other methods*, in *Papers in analysis, algebra and statistics* (Contemporary Math. *9*), (Amer. Math. Soc., Providence, R.I. 1982), 153–185.

The University of Adelaide,
Adelaide, Australia;
Bell Laboratories,
Murray Hill, New Jersey