Spherepackings in high-dimensional space

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE

EINDHOVEN UNIVERSITY OF TECHNOLOGY
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS

Spherepackings in high-dimensional space

by

A.Bos

T.H. - Report 80-WSK-03

July 1980

Spherepackings
in
high-dimensional space

by

A.Bos.

Abstract

A new construction of spherepackings using codes is given, which covers the construction of Leech and Sloane [3]. The dense packings of Sloane [10] are also obtained here, but without the use of complex numbers. Several new records on the packing desity in high dimensions are given. In the second part of this paper three new alternatives of a construction, which leads to the Leech lattice in $\mathbb{R}^{24}$, are given.

Introduction

In section 1.1 some prelimanaries about spherepackings and codes are collected. For more information about packings we refer to Leech & Sloane [3], and Rogers [8]; for more coding theory, see the book by MacWilliams and Sloane [6].
In section 1.2 we give the general construction and show that it is a generalization of construction C of Leech and Sloane [3].
In 1.3 up to 1.6 we give several examples, each time based on a different tower of lattices, including in the last section packings in dimension 80, 88, 96, 104, 112, 120 and 128 with new high densities. Also the results of Sloane obtained by use of complex numbers (cf. [10]), are obtained (The new record of Sloane in $\mathbb{R}^{36}$ has been improved meanwhile). A list of densest known spherepackings in dimensions up to 128 is given in 1.7.

In section 2.1 and 2.2 four constructions for the Leech lattice are given. The first one is the original construction (cf. [3]), the others are equivalent to the construction of Tits [11], [12], which uses the complex numbers, the quaternions and an algebraic extension of the quaternions, respectively.

1.1 Some definitions

A *spherepacking* is a collection of spheres in euclidean space $\mathbb{R}^n$ such that no two spheres have an inner point in common.
The *density* Δ of a packing is the fraction of $\mathbb{R}^n$ which lies inside the spheres. The *centerdensity* δ is defined by $\delta := \Delta/V_n$, where $V_n = \pi^{n/2}/\Gamma(\frac{n}{2}+1)$ is the volume of a unit sphere in $\mathbb{R}^n$.
A *lattice* L is an abelian group of vectors in $\mathbb{R}^n$, such that $\mathbb{R} \otimes L = \mathbb{R}^n$.
If the centers of the spheres form a lattice, the packing is called a *lattice packing*.
The minimum distance between two different points of L is denoted by $d_{min}(L)$.
The *kissing number* of a lattice packing is the number of spheres that touch one sphere.
An *alphabet* A is a finite set with a metric d on it, such that $d : A \times A \to \mathbb{Z}$ and $\gcd\{d(x,y) \mid x,y \in A\} = 1$. As alphabets we will only consider the fields $F = GF(q)$, where $q = p^r$, a prime power, with the Hamming metric. The metric on F^n is the componentwise sum of the metric on F.
A *code* C is a subset of F^n. A code is *linear* if it is an abelian group.
The *weight* of a vector is the distance to the null vector, i.e. the number of nonzero coordinates. We will denote the minimum distance in a code by d and the number of codewords by M.

If the code is linear over GF(q), then there is a $k \in \mathbb{N}$, called the *dimension* of the code, such that $M = q^k$. A code is often denoted by (n,M,d) or by (n,q^k,d) if it is linear.
$M_q(n,d)$ is the number of codewords for which a code with length n and minimum distance d over GF(q) exists.
For two codewords x and y in C we define

$x * y := (x_1\delta_{x_1,y_1}, x_2\delta_{x_2,y_2}, \dots, x_n\delta_{x_n,y_n})$ with Kronecker δ and

$C^* := \{x * y \mid x,y \in C\}$. Note that $C \subseteq C^*$.
From now on "distance" means the squared euclidean distance.

1.2 The construction

Let $L_0 \subseteq L_1 \subseteq \dots \subseteq L_k$ be a tower of lattices in $\mathbb{R}^m$. For i=1,2,....,k L_i/L_{i-1} is a group with a metric induced by the euclidean metric of $\mathbb{R}^m$.
Denote $\underline{a} + L_{i-1}$ by $\tilde{\underline{a}}$. As usual define, for $\underline{x} \in \mathbb{R}^m$ and $V \subset \mathbb{R}^m$,

$d(\underline{x},V) := \inf_{\underline{y} \in V} d(x,\underline{y})$. Then $d(\tilde{\underline{a}},\tilde{\underline{b}}) = d(\underline{a}+L_{i-1},\underline{b}+L_{i-1}) = d(\underline{a}-\underline{b},L_{i-1})$
is uniquely determined.

If G and H are groups with metrics σ_1 and σ_2 respectively, we write $G \simeq H$ if a group iromorfism $\varphi : G \to H$ and a $c \in \mathbb{R}$ exists such that for all $x,y \in G$ $\sigma_1(x,y) = c.\sigma_2(\varphi x,\varphi y)$. For example $G \simeq \mathbb{Z}/\frac{1}{2}\mathbb{Z}$ where G = GF(2) with the Hamming metric and c = 4.

$$\varphi^n : \prod_{i=1}^{n} G \to \prod_{i=1}^{n} H \text{ is also denoted by } \varphi.$$

<u>Theorem</u> 1 : Let $L_0 \subsetneq L_1 \subsetneq \dots \subsetneq L_k$ be a tower of lattices in $\mathbb{R}^m$.
For i=1,2,....,k let $G_i \xrightarrow[\varphi_i]{\simeq} L_i/L_{i-1}$ and let

$C_i = (n,M_i,d_i)$ be a code over G_i.

Then

$$\bigcup_{(\underline{c}_1,\ldots,\underline{c}_k)\in C_1 \times C_2 \times \ldots \times C_k} \left(\sum_{i=1}^{k} \varphi_i \underline{c}_i + L_0^n \right)$$

is a set of centers of a packing in $\mathbb{R}^{nm}$ with centerdensity

$$\delta_{nm} = \left(\delta_{L_0}\right)^n \left(\frac{1}{2}\sqrt{d}\right)^{nm} \prod_{i=1}^{k} M_i ,$$

where $d = \min_{i=0,1,\ldots,k} \left(d_{\min}(L_i).d_i\right)$ with $d_0=1$.

A lattice packing is obtained iff all codes are linear and for all $i=2,3,\ldots,k$

$\{\varphi_i \underline{x}_i + \varphi_i \underline{y}_i - \varphi_i(x_i + \underline{y}_i)\} \bmod L_{i-2}^n \in C_{i-1}$ and

$\varphi_1 \underline{x}_1 + \varphi_1 \underline{y}_1 - \varphi_1(x_1 + \underline{}_1) \in L_0^n$.

Proof : The only nontrivial fact is the minimum distance d.

Suppose $\underline{a} \in \sum_{i=1}^{k} \varphi_i \underline{x}_i + L_0^n$ and

$\underline{b} \in \sum_{i=1}^{k} \varphi_i \underline{y}_i + L_0^n$, with $\underline{x}_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ and

$\underline{y}_i = (y_{i1}, y_{i2}, \ldots, y_{in})$ both in C_i for $i=1,2,\ldots,k$.

If $\underline{x}_i = \underline{y}_i$ for $i=j+1, j+2,\ldots,k-1,k$ then

$$d(\underline{a},\underline{b}) = d\left(\sum_{i=1}^{j} \varphi_i \underline{x}_i , \sum_{i=1}^{j} \varphi_i \underline{y}_i + L_0^n \right) =$$

$$= \sum_{s=1}^{n} d\left(\sum_{i=1}^{j} \varphi_i x_{is}, \sum_{i=1}^{j} \varphi_i y_{is} + L_0 \right) \geq$$

$$\geq \sum_{s=1}^{n} d\left(\varphi_j x_{js}, \varphi_j y_{js} + L_{j-1}\right) \geq d_j . d_{\min}(L_j) ,$$

because at least d_j times $x_{js} \neq y_{js}$. □

In their construction of spherepackings, Leech and Sloane [3] used the tower $L_0 = 2\,Z$, $L_i = 2^{-i}L_0$ in $\mathbb{R}$ with $L_i/L_{i-1} \simeq GF(2)$ with the Hamming metric.
Due to the fact that several good codes over this alphabet exist, most dense spherepackings are constructed in this way, see the table in section 1.7.
Observe that in the case with $d_1 \equiv 0 \pmod 2$ the codes $C_2, C_3, \ldots\ldots, C_k$ have to be self-orthogonal in order to give a lattice packing. Since such codes have dimensions at most $n/2$, it is obvious that dense lattice packings in high dimensions, say ≥ 80, cannot be obtained in this way.

1.3 Packings from $\Lambda_2 \subseteq \frac{1}{2}\Lambda_2 \subseteq \frac{1}{4}\Lambda_2 \subseteq \ldots\ldots$ in $\mathbb{R}^2$.

In this section L_0 is the 2-dimensional lattice in $\mathbb{R}^2$ generated by $(2,0)$ and $(1, \sqrt{3})$ with $d_{min}(L_0) = 4$. This is the well known hexagonal lattice, called Λ_2 in [3], providing the densest packing in 2 dimensions with

$$\delta_{L_0} = 2^{-1}3^{-\frac{1}{2}}, \text{ according to } \Delta_{L_0} = \frac{\pi}{\sqrt{12}} = 0.907 \ldots\ldots$$

Now we form te tower of lattices $L_0 \subseteq L_1 \subseteq \ldots\ldots \subseteq L_k$ in $\mathbb{R}^2$ with $L_i := 2^{-i}.L_0$, so $d_{min}(L_i) = 2^{2(1-i)}$ for $i=1,2,\ldots\ldots,k$. Then we find $L_i/L_{i-1} \simeq GF(4)$ with the Hamming metric for all $i=1,2,\ldots\ldots,k$.
Translating theorem 1 to this special case we obtain

<u>Corollary</u> 2 : For $i=1,2,\ldots\ldots,k$ let C_i be an (n,M_i,d_i) code over $GF(4)$, with $1 < d_1 \leq 4$, $d_i < d_{i+1} \leq 4d_i$ and $d_k \leq n$. Then a packing of spheres exist in $\mathbb{R}^{2n}$ with density

$$\delta_{2n} = (2^{-1}3^{-\frac{1}{2}})^n \left(\frac{1}{2}\sqrt{d}\right)^{2n} \prod_{i=1}^{k} M_i \quad \text{with}$$

$$d = \min_{i=1,\ldots,k} \left(2^{2(1-i)} d_i\right)$$

A lattice packing is obtained iff all codes are linear and for $i=1,2,3,\ldots\ldots,k$ $C_i^* \subset C_{i-1}$ and $C_1^* \subset L_0^n$. □

This construction is the real version of the complex construction of Sloane [10].

The best results are obtained with codes C_i such that $d_{i+1}=4d_i$.

The first example gives the only known case in which the density of a packing, constructed with binary codes, is improved.

Example 1:

i) $k=1$, $C_1=(6,4^3,4)$ produces a lattice packing in $\mathbb{R}^{12}$ with highest known density $\delta_{12} = 3^{-3}$.

ii) $k=2$, $C_1=(18,4^{17},2)$ and $C_2= (18,4^9,8)$ (cf.[5]) produces a lattice packing in $\mathbb{R}^{36}$ with centerdensity $\delta_{36} = 2^{16}3^{-9} = 3{:}33\ldots.$
Note that a nonlattice packing exists with $\delta_{36} = 4$, see the table in section 1.7.

1.4 Packings from $\Lambda_2 \subseteq \Lambda'_2 \subseteq \frac{1}{3}\Lambda_2 \subseteq \frac{1}{3}\Lambda'_2 \subseteq \ldots\ldots$ in $\mathbb{R}^2$

As in the previous section L_0 is the lattice Λ_2 in $\mathbb{R}^2$. But now $L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots\ldots \subseteq L_k$ with L_1 generated by L_0 and $\left(1,\sqrt{\frac{1}{3}}\right)$, $L_{2i} := 3^{-i}L_0$ and $L_{2i+1} := 3^{-i}L_1$. It is clear that $d_{min}(L_i) \doteq 4.3^{-i}$ and $L_i/L_{i-1} \simeq GF(3)$ with the Hamming metric, for $i=1,2,\ldots\ldots,k$.

So we get

Corollary 3 : For $i=1,2,\ldots\ldots,k$ let C_i denote an (n,M_i,d_i) code over GF(3) with

$1 < d_1 \leq 3$, $d_i < d_{i+1} \leq 3d_i$ and $d_k \leq n$.

Then a packing of spheres exists in $\mathbb{R}^{2n}$ with density

$$\delta_{2n} = (2^{-1}3^{-\frac{1}{2}})^n \left(\frac{1}{2}\sqrt{d}\right)^{2n} \prod_{i=1}^{k} M_i \quad \text{where}$$

$$d = \min_{i=1,2,\ldots,k} (4.3^{-i}d_i).$$

A lattice packing is obtained iff all codes are linear and $C_1^* \subset C_{i-1}$ for $i=2,3,\ldots\ldots,k$ and $C_1^* \subset L_0^n$. □

This construction is new and the best results are obtained if $d_{i+1} = 3d_i$.

The following examples, except the last one which is needed in section 2, give the densest known packings obtained with this construction.

Example 2 :

i) $k=1$, $C_1 = (3,3^1,3)$ yields a lattice packing in $\mathbb{R}^6$ with highest possible density $\delta_6 = 2^{-3}3^{-\frac{1}{2}}$.

ii) $k=1$, $C_1 = (4,3^2,3)$ yields a lattice packing in $\mathbb{R}^8$ with highest possible density $\delta_8 = 2^{-4}$.

iii) $k=2$, $C_1 = (6,3^5,2)$, $C_2 = (6,3^1,6)$ yields in $\mathbb{R}^{12}$ the densest known lattice packing with density $\delta_{12} = 3^{-3}$.

iv) $k=2$, $C_1 = (12,3^{11},2)$, $C_2 = (12,3^6,6)$ yields $\delta_{24} = 3^{-1}$ for a lattice packing in $\mathbb{R}^{24}$.

1.5 Packings from a lattice tower in $\mathbb{R}^4$.

Let L_0 be the lattice in $\mathbb{R}^4$ generated by $(2\,\mathbb{Z})^4$ and $(1,1,1,1)$. This lattice is called Λ_4 in [3], has density $\delta_4 = 2^{-3}$ and minimum distance 4. Define L_1 to be the lattice generated by L_0 and $(1,1,0,0)$, $(1,0,1,0)$ and $(0,1,1,0)$, $L_{2i} := 2^{-i}L_1$ and $L_{2i+1} := 2^{-i}L_1$. It is clear that for $i=1,2,3,\ldots\ldots,k$ $L_i/L_{i-1} \cong GF(4)$ with the Hamming metric and $d_{min}(L_i) = 2^{2-i}$

<u>Corollary</u> 4 : For $i=1,2,\ldots\ldots,k$ let C_i denote an (n,M_i,d_i) code over GF(4) with

$d_1=2$, $d_i < d_{i+1} \leq 2d_i$ and $d_k \leq n$.

Then a packing in $\mathbb{R}^{4n}$ exists with density

$$\delta_{4n} = 2^{-3n}\left(\frac{1}{2}\sqrt{d}\right)^{4n} \prod_{i=1}^{k} M_i \quad \text{with}$$

$$d = \min_{i=1,\ldots\ldots,k} \left(2^{2-i} d_i\right).$$

The construction is new but no improvements of the results using binary codes are obtained. The best densities are with $d_{i+1} = 2d_i$. The last example is needed in section 2.
In all examples $C_1 = (n,4^{n-1},2)$.

<u>Example</u> 3 :

i) $k=1$, $C_1= (2,4,2)$ gives highest possible lattice density $\delta_8 = 2^{-4}$ in $\mathbb{R}^8$;

ii) $k=2$, $C_2= (4,4^1,4)$ gives highest known density $\delta_{16}= 2^{-4}$;

iii) $k=2$, $C_2= (5,4^2,4)$ gives highest known density $\delta_{20}= 2^{-3}$;

iv) $k=3$, $C_2= (8,4^4,4)$, $C_3= (8,4^1,8)$ gives highest known density $\delta_{32} = 2^0 = 1$;

v) $k=3$, $C_2= (10,4^6,4)$, $C_3= (10,4^2,8)$ gives highest known density $\delta_{40} = 2^4$;

vi) $k=2$, $C_2= (6,4^3,4)$ gives $\delta_{24} = 2^{-2}$ for a lattice packing in $\mathbb{R}^{24}$.

1.6 Packings from a lattice tower in $\mathbb{R}^8$

Let L_0 be the lattice Λ_8 (cf.[3]) in $\mathbb{R}^8$ with density 2^{-4}, generated by $(2\mathbb{Z})^8$ and the vectors of the binary $(8,2^4,4)$ code (see also examples 2ii and 3i). Define L_1 to be generated by L_0, the vectors of the binary $(8,2^7,2)$ code and $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. Further define $L_{2i} := 2^{-i}L_0$ and $L_{2i+1} := 2^{-i}L_1$, then $L_i/L_{i-1} \simeq GF(16)$ with the Hamming metric and $d_{min}(L_i) = 2^{2-i}$, $i=0,1,\ldots,k$.

Corollary 5 : For $i=1,2,\ldots,k$ let C_i denote an (n,M_i,d_i) code over GF(16) with $d_1 = 2_1$, $d_i < d_{i+1} \leq 2d_i$ and $d_k \leq n$. Then a packing in $\mathbb{R}^{8n}$ exists with density

$$\delta_{8n} = (2^{-4})^n \left(\frac{1}{2}\sqrt{d}\right)^{8n} \prod_{k=1}^{n} M_i \quad \text{with}$$

$$d = \min_{i=1,\ldots,k} \left(2^{2-i} d_i\right)$$

A lattice packing is obtained iff all codes are linear and for $i=2,3,\ldots,k$ $C_i^* \subset C_{i-1}$ and $C_1^* \subset L_0^n$. □

This construction is new and gives several new record densities. In the following examples $C_1 = (n,16^{n-1},2)$, while the last example is used in section 2.

Example 4 :

i) $k=1$, $C_1 = (2,16,2)$ gives highest known density $\delta_{16} = 2^{-4}$;

ii) $k=2$, $C_2 = (4,16^1,4)$ gives highest known density $\delta_{32} = 2^0 = 1$;

iii) $k=2$, $C_2 = (5,16^2,4)$ gives highest known density $\delta_{40} = 2^4$;

iv) $k=3$, $10 \leq n \leq 15$, $C_2 = (n,16^{n-3},4)$, $C_3 = (n,16^{n-7},8)$ gives density $\delta_{8n} = 2^{8n-44}$, which are all better than any packing density in those dimensions previously known.

v) k=4, $C_2 = (16,16^{13},4)$, $C_3 = (16,16^9,8)$, $C_4 = (16,16^1,16)$ give $\delta_{128} = 2^{88}$, also a new record, the old one being 2^{85} (cf.[3]).

vi) k=1, $C_1 = (3,16^2,2)$ gives a lattice in $\mathbb{R}^{24}$ with density $\delta_{24} = 2^{-4}$.

1.7 A table of dense packings

Two tables are given which yield the densest packings obtainable with the methods described in the foregoing sections. Also the highest known densities and upper bounds are given. In the first table the dimension is at most 32 and the densities and bounds are given in their numerical values, whereas in the second table the logarithm to the base two of the densities and bounds are given.

The first column gives the dimension, the second the highest density obtained by the above described construction and the third column the section in which the packing is constructed, where 1.2 refers to construction C of Leech and Sloane (cf.[3]), using the binary codes which are given in Appendix A of [6]. The fourth value is the maximum known density if this is higher than the one in column two. These packings can be found in [3], except for the dimensions 25 up to 32, but there the method is the same as in 24 dimensions.

The last column gives the best known upper bound. This appears to be Rogers bound (cf.[3]) up to dimension 96 and the recent Levenstein bound (cf.[4])for higher dimensions.

Dim.	Density	Section	Max. Density	Bound
1	2^{-1} = 0.500	1.2		0.500
2	$2^{-1}.3^{-\frac{1}{2}}$ = 0.289	1.3		0.289
3	$2^{-2\frac{1}{2}}$ = 0.177	1.2		0.186
4	2^{-3} = 0.125	1.2		0.131
5	$2^{-3\frac{1}{2}}$ = 0.088	1.2		0.100
6	$2^{-3}3^{-\frac{1}{2}}$ = 0.072	1.4		0.081
7	2^{-4} = 0.063	1.2		0.070
8	2^{-4} = 0.0625	1.2, 1.4, 1.5		0.0633
9	$2^{-4\frac{1}{2}}$ = 0 044	1.2		0.060
10	$2^{-7}.5$ = 0.039	1.2		0.060
11	$2^{-8}3^{2}$ = 0.035	1.2		0.061
12	3^{-3} = 0.037	1.3, 1.4		0.066
13	2^{-5} = 0.031	1.2	$2^{-8}.3^{2}$ = 0.035	0.073
14	2^{-5} = 0.031	1.2	$2^{-4}.3^{-\frac{1}{2}}$= 0.036	0.083
15	$2^{-4\frac{1}{2}}$ = 0.044	1.2		0.097
16	2^{-4} = 0.063	1.2, 1.5, 1.6		0.118
17	$2^{-4\frac{1}{2}}$ = 0.044	1.2	2^{-4} = 0.063	0.146
18	$3^{-2\frac{1}{2}}$ = 0.064	1.3	$2^{-3}3^{-\frac{1}{2}}$ = 0.072	0.186
19	$2^{-3\frac{1}{2}}$ = 0.088	1.2		0.243
20	2^{-3} = 0.125	1.2, 1.5		0.325
21	$2^{-2\frac{1}{2}}$ = 0.177	1.2		0.443
22	2^{-2} = 0.250	1.2	$2^{-1}3^{-\frac{1}{2}}$ = 0.289	0.617
23	$2^{-1\frac{1}{2}}$ = 0.354	1.2	2^{-1}= 0.500	0.878
24	2^{-1} = 0.500	1.2	2^{0} = 1.000	1.273
25	$2^{-1\frac{1}{2}}$ = 0.354	1.2	$2^{-\frac{1}{2}}$ = 0.707	1.880
26	2^{-2} = 0.250	1.2	2^{-1} = 0.500	2.827
27	$2^{-1\frac{1}{2}}$ = 0.354	1.2		4.325
28	2^{-1} = 0.500	1.2		6.730
29	$2^{-1\frac{1}{2}}$ = 0.354	1.2	$2^{-\frac{1}{2}}$ = 0.707	10.642
30	2^{-1} = 0.500	1.2	2^{0} = 1.000	17.094
31	$2^{-\frac{1}{2}}$ = 0.707	1.2		27.880
32	2^{0} = 1.000	1.2, 1.5, 1.6		46.147

TABLE I

Dim.	^{2}log(density)	Section	^{2}log(max. dens.)	^{2}log(bound)
33	0.5	1.2		6.28
34	1	1.2		7.04
35	1.5	1.2		7.83
36	2	1.2		8.64
37	1.5	1.2		9.46
38	2	1.2		10.31
39	2.5	1.2		11.17
40	4	1.5 ,1.6		12.04
41	3.5	1.2		12.94
42	4.2	1.2		13.85
43	4.5	1.2		14.78
44	5.6	1.2		15.72
45	6.2	1.2		16.68
46	6.6	1.2		17.65
47	7.2	1.2		18.64
48	8.2	1.2	14.0	19.64
49	8.5	1.2		20.66
50	9	1.2		21.69
51	10	1.2		22.73
52	10.3	1.2		23.79
53	11	1.2		24.86
54	12	1.2		25.95
55	13	1.2		27.04
56	14	1.2		28.15
57	14	1.2		29.27
58	15	1.2		30.41
59	16	1.2		31.55
60	17	1.2		32.71
61	18	1.2		33.88
62	19	1.2		35.06
63	20	1.2		36.25
64	22	1.2		37.45
65	21.3	1.2		38.66

Dim.	^{2}log(density)	Section	^{2}log(max. dens)	^{2}log(bound)
66	22.3	1.2		39.88
67	23.3	1.2		41.12
68	24.3	1.2		42.36
69	25.3	1.2		43.61
70	26.3	1.2		44.88
71	27.3	1.2		46.15
72	28.3	1.2		47.43
73	29.3	1.2		48.73
74	29.3	1.2		50.03
75	29.3	1.2		51.34
76	29.3	1.2		52.66
77	30.3	1.2		53.99
78	31.3	1.2		55.33
79	31.3	1.2		56.88
80	36	1.6		58.04
81	33.2	1.2		59.40
82	33.2	1.2		60.78
83	33.5	1.2		62.16
84	37	1.2		63.55
85	36.5	1.2		64.95
86	37	1.2		66.36
87	37.5	1.2		67.78
88	44	1.6		69.20

TABLE II

Dim.	^{2}log(density)	Section	^{2}log(max. dens.)
89	38.2	1.2	70.63
90	38.6	1.2	72.07
91	38.5	1.2	73.52
92	40	1.2	74.98
93	39.5	1.2	76.44
94	40	1.2	77.91
95	41.5	1.2	79.39
96	52	1.6	80.86
97	43.5	1.2	82.34
98	44	1.2	83.82
99	45.5	1.2	85.31
100	47	1.2	86.80
101	46.3	1.2	88.30
102	47.3	1.2	89.81
103	48.5	1.2	91.33
104	60	1.6	92.85
105	50.5	1.2	94.38
106	52	1.2	95.92
107	53.5	1.2	97.46
108	55	1.2	99.01
109	56.5	1.2	100.56
110	58	1.2	102.12
111	59.5	1.2	103.69
112	68	1.6	105.26
113	62.5	1.2	106.84
114	64	1.2	108.43
115	64.5	1.2	110.02
116	66	1.2	111.62
117	67.5	1.2	113.22
118	69	1.2	114.83
119	70.5	1.2	116.45
120	76	1.6	118.07

Dim.	^{2}log(density)	Section	^{2}log(max. dens.)
121	73.5	1.2	119.70
122	75	1.2	121.33
123	76.5	1.2	122.97
124	78	1.2	124.61
125	78.5	1.2	126.26
126	81	1.2	127.91
127	81.5	1.2	129.57
128	88	1.6	131.24

TABLE II (continued)

2.1 Translating lattices

In this section we give a general theory for translating lattices obtained from binary codes. This leads to the known construction of the Leech lattice and doubling the centerdensities in dimensions 25 up to 32.

We recall the important fact that the Leech lattice is the unique unimodular lattice, that is with centerdensity equal 1, in $\mathbb{R}^{24}$ with minimum distance 4 (cf.[2]).

First we extend our terminology of section 1.2. Recall that $\varphi_i : G_i \to L_i (\text{mod } L_{i-1})$ is a group isomorfism. Denote the "coset leader" $\varphi_i(1)$ by 1_i and $\varphi_i(\alpha)$ by $\alpha 1_i$ or $1_i\alpha$ for $\alpha \in G_i$.

For $\underline{c}_i = (c_{i1}, c_{i2}, \ldots\ldots, c_{in}) \in C_i$ and $\underline{a} = \sum_{i=1}^{k} \varphi_i \underline{c}_i$, we will denote

$$\underline{a} = \left(\sum_{i=1}^{k} c_{i1} 1_i, \sum_{i=1}^{k} c_{i2} 1_i, \ldots, \sum_{i=1}^{k} c_{in} 1_i \right) \text{ by}$$

$$\sum_{i=1}^{k} 1_i (c_{i1}, c_{i2}, \ldots\ldots, c_{in}) = \sum_{i=1}^{k} 1_i \underline{c}_i .$$

Let $w_\alpha(\underline{c}_j)$ be the number of coordinates of $\underline{c}_j$ equal to α. So for the Hamming weight $w(\underline{c}_j)$ we have

$$w(\underline{c}_j) = \sum_{\substack{\alpha \neq 0 \\ \alpha \in G_j}} w_\alpha(\underline{c}_j) \quad \text{and} \quad \sum_{\alpha \in G_j} w_\alpha(\underline{c}_j) = n.$$

If we write $\underline{c}_j$ as the j-th row of a kxn-matrix, then $w_{\alpha_1, \alpha_2, \ldots\ldots, \alpha_k}$ is the number of times the column $(\alpha_1, \ldots\ldots, \alpha_k)^t$ occurs in the matrix.

Note that $\sum_{\substack{\alpha, \ldots\ldots, \alpha_k \\ \alpha_j = \alpha}} w_{\alpha_1, \ldots\ldots, \alpha_k} = w_\alpha(\underline{c}_j)$.

Define $w^*(\underline{c}_j)$ to be the sum of the coordinates of $\underline{c}_j$, so

$$w^*(\underline{c}_j) = \sum_{\alpha \in G_j} \alpha . w_\alpha(\underline{c}_j).$$

Let $L_0 \subseteq L_1 \subseteq \ldots \subseteq L_k$ in $\mathbb{R}^m$, groups G_i and codes C_i over G_i for $i=1,\ldots,k$ be given as in theorem 1. Further let $L_k \subsetneq L_{k+1}$ and n be such that $n.d_{min}(L_{k+1}) < d$. Then, in general, it is not possible to find a subset of L_{k+1}^n at distance d from L_0^n. However sometimes one can find one or more such cosets of a lattice packing and increase the density in this way.

<u>Lemma</u> : Let $L_0 = 2\mathbb{Z}$, $L_i = 2^{-i}L_0$, so $G_i = GF(2)$, for $i=1,2,\ldots,k$.

Given codes $C_i = (n, M_i, d_i)$ for $i=1,2,\ldots,k$, with

$d_i < d_{i+1} \leq 4d_i$, $4(d_k - d_{k-1}) \leq n < 4d_k$ and C_{k-1} and

C_k being linear with $C_k^* \subset C_{k-1}$.

Then $\underline{x} \in L_{k+1}^n$ exists with $d(\underline{x} + \Gamma, \Gamma) \geq d$, where

$d = d_{min}(\Gamma)$ and Γ is the lattice obtained by theorem 1.

<u>Proof</u> : It is clear that $l_i = 2^{1-i}$ for $i=1,2,\ldots,k+1$.

Let $\underline{c}$ be such that $d(\underline{c}, C_{k-1}) \geq \frac{d_{k-1}}{2}$.

Define $\underline{x} := l_{k-1}\, \underline{c} + l_{k+1}\, (1,1,\ldots,1)$.

$d(l_{k+1}, (\alpha_1 l_1 + \ldots + \alpha_k l_k) \bmod L_0) \geq d(l_{k+1}, (\alpha_{k-1} l_{k-1} + \alpha_k l_k) \bmod L_{k-2})$

for all $\alpha_1, \alpha_2, \ldots, \alpha_{k-2} \in GF(2)$.

$d(l_{k+1}, \alpha_{k-1}\, l_{k-1} + \alpha_k l_k) = \frac{1}{4^k}$ if $(\alpha_{k-1}, \alpha_k) = (0,0)$ or $(0,1)$ and

$d(l_{k+1}, \alpha_{k-1} l_{k-1} + \alpha_k l_k) = \frac{9}{4^k}$ if $(\alpha_{k-1}, \alpha_k) = (1,0)$ or $(1,1)$.

For $\underline{a} \in GF(2)^n$ let $\underline{a}' := \underline{a} + \underline{c}$. Then we get, with $\underline{c}_i \in C_i$, $i=1,\ldots\ldots,k$

$$d(\underline{x}, \varphi_1\underline{c}_1 + \varphi_2\underline{c}_2 + \ldots\ldots + \varphi_k\underline{c}_k + L_0^n) \geq$$

$$\geq \sum_{i=1}^{n} d(1_{k+1}, c'_{k-1i} + c_{ki}1_k + L_{k-2}) =$$

$$= \sum_{\alpha \in GF(2)} (w_{0,\alpha}.4^{-k} + w_{1,\alpha}.9.4^{-k}).$$

But $w(\underline{c}_{k-1}) = w^*(\underline{c}_{k-1}) \geq d_{k-1}$ so $w(\underline{c}'_{k-1}) = w_{1,0} + w_{1,1} \geq \frac{d_{k-1}}{2}$,

thus $\sum_{\alpha \in GF(2)} (w_{0,\alpha}.4^{-k} + w_{1,\alpha}.9.4^{-k}) \geq (n - \frac{d_{k-1}}{2}).\frac{1}{4^k} + \frac{d_{k-1}}{2}.\frac{9}{4^k} =$

$$= \frac{n+4d_{k-1}}{4^k} \geq \frac{d_k}{4^{1-k}}$$

and since $d_{min}(\Gamma) = d = \min_{i=1,\ldots,k} (d_i.d_{min}(L_i)) = \min_{i=1,\ldots,k}\left(\frac{d_i}{4^{1-i}}\right)$,

we have $\frac{d_k}{4^{1-k}} \geq d$. □

Example 5 : $n=8$, $C_1 = (8,2^7,2)$, $C_2 = (8,2^4,4)$ given $\delta_\Gamma = 2^{-5}$ but translating Γ over $\underline{x} = (\frac{5}{4}, \frac{1}{4}^7)$ gives a doubled density of maximal value.

Example 6: $n=24$, $C_1 = (24,2^{23},2)$, $C_2 = (24,2^{12},8)$ gives $\delta_\Gamma = 2^{-1}$. Translating over $\underline{x} = (\frac{5}{4}, \frac{1}{4}^{23})$ gives density $2^0=1$ and the famous Leech lattice is obtained.

Also in dimension 25 up to 32 the density can be doubled in the same way: see the fifth column of table 1. Possible dimensions for applying the lemma are 48 up to 64 with the sequence of codes $C_1 = (n,M_1,4)$ and $C_2 = (n,M_2,16)$ and dimensions 96 up to 128 with the codes $C_1 = (n,M_1,2)$, $C_2 = (n,M_2,8)$ and $C_3 = (n,M_3,32)$.

The only condition to be checked is wether $C_k^* \subset C_{k-1}$ for $k=2$ resp. 3.
The linearity of the codes C_k and C_{k-1} and the fact that $C_k^* \subset C_{k-1}$ is necessary, as the following example shows.

Example 7 : $n=16$, $C_1 = (16,2^{15},2)$, $C_2 = (16,2^8,6)$ give

$\delta_\Gamma = 2^{-17}.3^8 = 0.0501$, which is less than the highest known density in $\mathbb{R}^{16}$ of $2^{-4} = 0.0625$. Doubling δ_Γ by translating Γ over $\underline{x} = (\frac{5}{4}, \frac{1}{4}^{15})$ would yield a new record. However for

$\underline{a} = \varphi_1(1^4 0^{12}) + \varphi_2(0^4 1^6 0^6)$ and $\underline{b} = \varphi_2(0\ 1^6 0^9)$ one has

$d(\underline{x} + \underline{b}, \underline{a}) = \underline{d}(\underline{x}, \underline{a}-\underline{b}) = d\{(\frac{5}{4}, \frac{15}{4}), (1, \frac{1}{2}^3, 0^3, \frac{1}{2}^3, 0^6)\} = 1 < d = \frac{3}{2}$.

This is due to the fact that the Preparata code C_2 is not self-orthogonal, so $C_2^* \not\subset C_1$.

2.2 Three other constructions of the Leech lattice

In this paragraph we construct a lattice packing Γ in $\mathbb{R}^{24}$ with density δ_Γ and minimum distance d. Then we give $1/\delta_\Gamma$ vectors $\underline{x}_i$, with $\underline{x}_1=\underline{0}$, such that the cosets $\underline{x}_i + \Gamma$ $(i=1,2,\ldots\ldots,1/\delta_\Gamma)$ are mutually at distance d and the vectors form an additive group, isomorfic to the addition group of the field. So a lattice packing in $\mathbb{R}^{24}$ with density 1 is obtained, which has to be the Leech lattice.
Apply corollary 3 with $k=2$, $n=12$, $C_1 = (12,3^{11},2)$ and $C_2 = (12,3^6,6)$.
As in example 2 iv) a lattice packing Γ is obtained with $\delta_\Gamma = 3^{-1}$ and $d = \frac{8}{3}$. Note that $l_1 = (1, \sqrt{\frac{1}{3}})$, $l_2 = (\frac{1}{3}, \frac{1}{3\sqrt{3}})$ and $l_3 = \frac{1}{3} l_1$.

Define $\underline{x}_2 := l_3(1,1,1,\ldots\ldots,1) + l_1(1,0,0,\ldots\ldots,0)$ and $\underline{x}_3 := 2\underline{x}_2$. Then it can be proved that $d(\underline{x}_i,\Gamma) \geq d$ for i=2,3, using the fact $w_\alpha(\underline{c}_2) \equiv 0(3)$ for all $\alpha \in GF(3)$, which is clear by inspecting the complete weight enumerator of the ternary Golay code C_2 (cf.[5], Ch. 19, p.598).

Apply corollary 4 with k=2, n=6, $C_1 = (6,4^5,2)$ and $C_2 = (6,4^3,4)$. A lattice packing Γ in $\mathbb{R}^{24}$ is obtained with $\delta_\Gamma = \frac{1}{4}$ and $d_\Gamma = 4$. The field GF(4) is represented by $\{0,1,\varepsilon,1+\varepsilon\}$. Note that $l_1 = (1,1,0,0)$, $\varepsilon l_1 = (1,0,1,0)$, $l_2 = (1,0,0,0)$, $\varepsilon l_2 = (\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$ and $l_3 = \frac{1}{2}\, l_1$.
Define $\underline{x}_2 := l_3(1,1,\ldots\ldots,1) + \varepsilon l_1(1,0,0,\ldots\ldots,0)$,

$\underline{x}_3 = \varepsilon l_3(1,1,\ldots\ldots,1) + (1+\varepsilon)\, l_1\,(1,0,\ldots\ldots,0)$ and

$\underline{x}_4 := \underline{x}_2 + \underline{x}_3$. From the complete weight enumerator of C_2 (cf.[4], p.296) we learn $w_\alpha(\underline{c}_2) \equiv 0(2)$ for all $\alpha \in GF(4)$. Then it is not hard to prove that $d(\underline{x}_i,\Gamma) \geq d$ for i=2,3,4.

At last applying corollary 5 with k=1, n=3 and $C_1 = (3,16^2,2)$ a lattice packing Γ is obtained with $\delta_\Gamma = 16^{-1}$ and $d_\Gamma = 4$. We represent the field GF(16) by the 4-dimensional vector space over GF(2) with base $1,\varepsilon_2,\varepsilon_3,\varepsilon_4$.
Let $l_1 = (1,1,0^6)$, $\varepsilon_2 l_1 = (1,0,1,0^5)$, $\varepsilon_3 l_1 = (1,0^3,1,0^3)$, $\varepsilon_4 l_1 = (\frac{1}{2}^8)$, $l_2 = (\frac{1}{2}^4,0^4)$, $\varepsilon_2 l_2 = (0^2, \frac{1}{2}^4, 0^2)$, $\varepsilon_3 l_2 = (\frac{1}{2},0)^4$ and $\varepsilon_4 l_4 = (1,0^7)$.
Define $\underline{x}_2 := l_2(1,1,1) + l_1(\varepsilon_3,0,0)$, $\underline{x}_3 := \varepsilon_2 l_2(1,1,1) + l_1(\varepsilon_2,0,0)$. $\underline{x}_4 := \varepsilon_3 l_2(1,1,1) + l_1(1,0,0)$, $\underline{x}_5 := \varepsilon_4 l_2(1,1,1) + l_1(\varepsilon_4,0,0)$ and $\underline{x}_6,\ldots\ldots,\underline{x}_{16}$ to be the nonzero linear combinations of $\underline{x}_2,\ldots\ldots,\underline{x}_5$ over GF(2).

<u>Lemma</u> : $d(\underline{x}_2,\Gamma) \geq d_\Gamma = 4$.

<u>Proof</u> : Let $I \subset GF(16)$ be the coset of the subspace, generated by 1, ε_2 and ε_4 so

$$I := \{\varepsilon_3,\ 1+\varepsilon_3, \varepsilon_2+\varepsilon_3,\ \varepsilon_3+\varepsilon_4,\ 1+\varepsilon_2+\varepsilon_3,\ 1+\varepsilon_3+\varepsilon_4,$$
$$\varepsilon_2+\varepsilon_3+\varepsilon_4,\ 1+\varepsilon_2+\varepsilon_3+\varepsilon_4\}.$$

$$\text{Then } d(1_2,\alpha 1_1 + L_0 \begin{cases} = 2 \text{ for } \alpha \in I \text{ and} \\ = 1 \text{ for } \alpha \notin I. \end{cases}$$

Suppose $\underline{c}$ is such that $d(\underline{x}_2,\underline{\varphi}_1\underline{c} + L_0^3) < d_\Gamma = 4$, then

for all $\alpha \in I$, $w_\alpha(\underline{c} - (\varepsilon_3,0,0)) = 0$. But

$$w^*(\underline{c} - (\varepsilon_3,0,0)) = \sum_{\alpha \in GF(16)} \alpha .\ w_\alpha(\underline{c} - (\varepsilon_3,0,0)) = \varepsilon_3 \quad \text{thus}$$

$$\sum_{\alpha \in I} w_\alpha (\underline{c} - (\varepsilon_3,0,0)) \equiv 1(2), \quad \text{contradiction.}$$

Similar arguments can be applied to prove $d(\underline{x}_i,\Gamma) \geq d$ for $i = 3,\ldots\ldots,16$. □

So we constructed the Leech lattice in four different ways.

REFERENCES

[1] Bos, A. Spherepackings in Euclidean space, in "Packing and Covering in Combinatorics" (A.Schrijver ed), Mathematical Centre Tracts 106, Mathematisch Centrum, Amsterdam, 1979, pp. 161-177.

[2] Conway, J.H.
A characterisation of Leech's lattice, Inventiones Math., 7 (1969), 137-142.

[3] Leech, J., Sloane,N.J.A.
Spherepackings and error-correcting codes, Canad. J. Math., 23 (1971), 718-745.

[4] Levenstein, V.I.
On bounds for packings in n-dimensional Euclidean space, Soviet Math. Dokl., 20 (1979), 417-421.

[5] MacWilliams, F.J., Odlyzko, A.M., Sloane,N.J.A., Ward,H.N.
Self-dual codes over GF(4), J.Combinatorial Theory Ser. A, 25 (1978), 288-318.

[6] MacWilliams, F.J., Sloane,N.J.A.
The Theory of Error-correcting Codes, North-Holland, Amsterdam, 1977.

[7] Milnor, J., Husemöller, D.
Symmetric bilinear forms, Springer-Verlag, N.Y. 1973.

[8] Rogers, C.A.
Packing and Covering, Cambridge Univ. Press, Cambridge 1964.

[9] Solane, N.J.A.
Binary codes, lattices and spherepackings, in: "Combinatorial Surveys" (Proc. 6th British Comb. Conf., Egham, 1977; P.J.Cameron ed.), Academic Press, London, 1977, pp. 117-164.

[10] Sloane, N.J.A.,
Codes over GF(4) and complex lattices, J.Algebra, 52 (1978), 168-181.

[11] Tits, J. Quaternions over Q[$\sqrt{5}$], Leech's lattice and the sporadic group of Hall-Janko, preprint.

[12] Tits, J. Private communication.