Dense sphere packings from new codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

and
Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)

December 2, 1998

Abstract

The idea behind the **coset code** construction (see [6, 7]) is to reduce the construction of sphere packings to error-correcting codes in a unified way. We give here a short self-contained description of this method. In recent papers [1, 2, 3, 4] we constructed a large number of new binary, ternary and quaternary linear error-correcting codes. In a number of dimensions our new codes yield improvements. Recently Vardy [8, 9] has found a construction, which yields record densities in dimensions 20,27,28,29 and 30. We give a short description of his method using the language of coset codes. Moreover we are able to apply this method in dimension 18 as well, producing a sphere packing with a record center density of $(3/4)^9$.

1 Sphere packings and coset codes

Let $E = I\!\!R^N$ be the N-dimensional Euclidean space, $\Gamma \subset E$ a discrete subset. Denote by $\|x\|$ the Euclidean distance of x from the origin, by $\mu(\Gamma)$ the minimum norm (= square of the distance) between different elements of Γ. The value $\rho(\Gamma) = \sqrt{\mu(\Gamma)}/2$ is called the **packing radius** of Γ. The meaning of ρ is that open balls of radius ρ centered at the lattice points do not intersect, and ρ is the maximum such radius. We will be mainly interested in the parameter

$$\delta = \delta(\Gamma) = \frac{\rho^N}{vol(\Gamma)},$$

the **center density** of Γ. As the discrete sets Γ constructed in this paper will be unions of cosets of lattices the determination of the volume will be no problem (if Γ is the union of M different cosets of a lattice of volume ν, then Γ has volume ν/M). Observe that δ is unchanged if a constant positive nonzero multiplicative factor is applied: $\delta(c \cdot \Gamma) = \delta(\Gamma)$. We can therefore assume $\rho = 1$. Then δ is the reciprocal of the volume of Γ. Our objective is to construct sphere packings with a high center density.

1.1 Coset codes

Let $\mathcal{A}_0 \supset \mathcal{A}_1 \supset \ldots \supset \mathcal{A}_l$ be a chain of m-dimensional lattices, where the factor group $\mathcal{A}_{i-1}/\mathcal{A}_i$ is isomorphic to the abelian group A_i of order $a_i, i = 1, 2 \ldots, l$. Let further C_i be an a_i-ary code with M_i elements and minimum distance d_i. We choose representatives $\alpha_{ij}, j = 1, 1, \ldots, a_i$ for the cosets of $\mathcal{A}_i$ in $\mathcal{A}_{i-1}$. Choose $\alpha_{i1} = 0$. Put $A_i = \{\alpha_{ij}, j = 1, 2, \ldots, a_i\}$. Choose A_i as the alphabet over which the code C_i is defined. It is convenient and no loss of generality to assume that the all-0 word belongs to C_i. The $N = nm$-dimensional packing

$$\Gamma = \Gamma(\mathcal{A}_0 \supset \mathcal{A}_1 \supset \ldots \supset \mathcal{A}_l; C_1, C_2, \ldots, C_l)$$

is defined as the union of $M_1 M_2 \ldots M_l$ cosets of the sublattice $(\mathcal{A}_l)^n$. The cosets are parametrized by l-tupels of codewords $(v_1, v_2, \ldots, v_l)$, where $v_i \in C_i$. Let $v_i = (v_{i1}, \ldots, v_{in})$, where $v_{ij} \in A_i$. Then the coset $N(v_1, v_2, \ldots, v_l)$ is defined as

$$N(v_1, v_2, \ldots, v_l) = (\sum_{i=1}^{l} v_{ij})_{j=1}^{n} + (\mathcal{A}_l)^n.$$

Observe that $N(0,0,\ldots,0) = (\mathcal{A}_l)^n$. It is clear that these cosets are distinct so that

$$vol(\Gamma) = \frac{vol(\mathcal{A}_l)^n}{M_1 \ldots M_l}.$$

How about the minimal norm? Let $x, y \in \Gamma, x \neq y$. If x and y belong to the same coset, then their difference is in $(\mathcal{A}_l)^n$. It follows $\|x - y\| \geq \sqrt{\mu(\mathcal{A}_l)}$. So assume they are in different cosets. Let $x \in N(v_1, v_2, \ldots, v_l), y \in N(v_1', v_2', \ldots, v_l')$ and i minimal such that $v_i \neq v_i'$. As C_i has minimum distance d_i it follows that $x - y$ has in d_i of its n components an entry in $\mathcal{A}_{i-1} \backslash \mathcal{A}_i$. It follows $\|x - y\| \geq \sqrt{d_i \cdot \mu(\mathcal{A}_{i-1})}$.

1.2 The case $m = 1$

We have $\mathcal{A}_0 = \mathbb{Z}, \mathcal{A}_i = q_1 \ldots q_i \mathbb{Z}$ $(i = 1, 2, \ldots, l), \mu(\mathcal{A}_i) = (q_1 \ldots q_i)^2$, thus

$$\mu(\Gamma) \geq Min\{d_1, d_2 q_1^2, \ldots, d_l (q_1 \ldots q_{l-1})^2, (q_1 q_2 \ldots q_l)^2\}.$$

If we use linear codes $[n, k_i, d_i]_{q_i}$ we obtain

$$\delta(\Gamma) \geq \frac{1}{2^n} \prod_{i=1}^{l} q_i^{k_i - n} \cdot \mu(\Gamma)^{n/2}.$$

1.3 The case $m = 2$

Let $\mathcal{A}_0 =< (1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2}) >=< a_0, b_0 >$ be the hexagonal lattice (as generated by root systems of types A_2 and G_2). The lattice $\mathcal{A}_0$ has volume $\frac{\sqrt{3}}{2}$ and minimum norm 1. The image $\mathcal{A}_{1,0}$ of $\mathcal{A}_0$ under the linear mapping with matrix $M = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$ (with respect to basis a_0, b_0) has index 3 in $\mathcal{A}_0$, is generated by $a_0 + b_0$ and $-a_0 + 2b_0$ and has minimum distance $\|a_0 + b_0\| = \sqrt{3}$. As $a_0 + b_0$ and $-a_0 + 2b_0$ have the same length and include an angle of $\pi/3$ we see that $\mathcal{A}_{1,0}$ is similar to $\mathcal{A}_0$. Applying the same matrix repeatedly we get $\mathcal{A}_{j,0} = \mathcal{A}_0 M^j$, for instance $\mathcal{A}_{2,0} = 3 < b_0, -a_0 + b_0 >= 3\mathcal{A}_0$. Aside of this operation we also consider sublattices of index 4 obtained by multiplication with the constant 2. This leads to the following Definition: $\mathcal{A}_{j,k} = 2^k \mathcal{A}_0 M^j$. It is clear that $vol(\mathcal{A}_{j,k}) = 4^k 3^j \frac{\sqrt{3}}{2}$ and $\mu(\mathcal{A}_{j,k}) = 4^k 3^j$. We apply the coset code construction with $\mathcal{A}_i = \mathcal{A}_{j(i),k(i)}$, where $j(i)+k(i) = i$ and either $\mathcal{A}_{i+1} = \mathcal{A}_{j(i)+1,k(i)}$ or $\mathcal{A}_{i+1} = \mathcal{A}_{j(i),k(i)+1}$, of index 3 or 4 in $\mathcal{A}_i$. We have

$$vol(\Gamma) = \frac{(2^{2k(l)-1} 3^{j(l)+1/2})^n}{\mid C_1 \mid \dots \mid C_l \mid}$$

and

$$\mu(\Gamma) \geq Min\{\mu(\mathcal{A}_l); d_{i+1}\mu(\mathcal{A}_i), i = 0, 1, \dots, l-1\}.$$

2 A variant of the coset code-construction

We use the following chain of 1-dimensional lattices: $\mathcal{A}_0 = \mathbb{Z} \supset \mathcal{A}_1 = 2\mathbb{Z} \supset \mathcal{A}_2 = 4\mathbb{Z} \supset \mathcal{A}_3 = 8\mathbb{Z}$ and the following codes: $C_1 = [n,1,n]$ (the repetition code),$C_3 = C_1^{\perp} = [n, n-1, 2]$ and binary codes C_2, C_2' of length n, minimum distances $\geq d$ and $\geq d'$, respectively. Observe that C_2, C_2' are not required to be linear codes. As alphabets for our codes we use $A_1 = \{0,1\}, A_2 = \{0,-2\}, A_3 = \{0,4\}$. With this notation we define $\Gamma = \Gamma^*(\mathcal{A}_0 \supset \mathcal{A}_1 \supset \mathcal{A}_2 \supset \mathcal{A}_3; C_1, (C_2, C_2'), C_3)$ as the union of the following cosets of $(8\mathbb{Z})^n$ in $\mathbb{Z}^n$:

$$N(\mathbf{0}, v_2, v_3), \text{ where } v_2 \in \mathbf{1} + C_2, v_3 \in C_3 \text{ (vectors of } \textbf{even type}\text{)}$$

$$N(\mathbf{1}, v_2, v_3), \text{ where } v_2 \in C_2', v_3 \notin C_3 \text{ (vectors of } \textbf{odd type}\text{)}.$$

Here **0** and **1** stand for the vectors of length n with all entries 0 and 1, respectively. It is clear that the addition of cosets if as follows:

$$\begin{aligned}
N(0, v_2, v_3) + N(0, w_2, w_3) &= N(0, v_2 + w_2, v_3 + w_3 + v_2 \cap w_2) \\
N(0, v_2, v_3) + N(1, w_2, w_3) &= N(1, v_2 + w_2, v_3 + w_3 + v_2 \cap w_2) \\
N(1, v_2, v_3) + N(1, w_2, w_3) &= N(0, v_2 + w_2 + 1, v_3 + w_3 + v_2 \cup w_2 + 1)
\end{aligned}$$

Let us determine the minimum Euclidean distance between different elements of Γ. Assume at first x, y are both of even type, $x \in N(0, v_2, v_3), y \in N(0, w_2, w_3)$. If $v_2 \neq w_2$, then $\|x - y\| \geq 2\sqrt{d}$. If $v_2 = w_2, v_3 \neq w_3$, then $\|x - y\| \geq 2\sqrt{2} = \sqrt{32}$. If finally $v_2 = w_2, v_3 = w_3$, then $\|x - y\| \geq 8$. The same arguments apply if x and y are both of odd type. We just have to replace d by d'. Let finally $x \in N(1, v_2, v_3)$ be of odd type and $y \in N(0, w_2, w_3)$ of even type. All entries of $x - y$ are odd integers. We wish to impose conditions on C_2, C_2' ensuring that for at least one coordinate the entry of $x - y$ is $\pm 3 (\mathrm{mod}\ 8)$. If this is the case, then $\|x - y\| \geq \sqrt{n - 1 + 9} = \sqrt{n + 8}$. Assume to the contrary all entries of $x - y$ are $\pm 1 (\mathrm{mod}\ 8)$. Fix a coordinate. Consider the 16 possibilities of how it may be distributed on the vectors v_2, v_3, w_2, w_3. Eight of these are excluded as they lead to a difference $\pm 3 (\mathrm{mod}\ 8)$. Write $v_2 = 1 + u_2$, where $u_2 \in C_2$. The eight remaining cases are the following:

u_2	v_3	w_2	w_3	$N(1, v_2, v_3) - N(0, w_2, w_3)$
1	0	0	0	1-0=1
1	0	1	1	1-2=-1
1	1	0	1	5-4=1
1	1	1	0	5-(-2)=-1
0	0	0	0	-1-0=-1
0	0	1	0	-1-(-2)=1
0	1	0	1	3-4=-1
0	1	1	1	3-2=1

Here the entry in the last column is to be taken as an integer mod 8, whereas the entries in the first four columns are 1 or 0. As an example consider the second row of this table: as $u_2 = 1$ (equivalently $v_2 = 0$) and $v_3 = 0$, the entry in $N(1, v_2, v_3)$ is 1+0+0=1. As $w_2 = w_3 = 1$, the entry in $N(0, w_2, w_3)$ is -2+4=2. This explains the last entry $1 - 2 = -1$ (mod 8).

This table shows $v_3 + w_3 = w_2 \cap u_2$ (here $v + w$ is the symmetric difference of v) Observe that $v_3 + w_3$ has odd weight. We will get the desired contradiction if $w_2 \cap u_2$ is even, equivalently if C_2 and C_2' are orthogonal codes.

Theorem 1 *Let C_2, C_2' be binary codes of length n and minimum distances d, d', respectively, which are orthogonal to each other. Then the n-dimensional sphere packing*

$$\Gamma = \Gamma^*(\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z}; [n, 1, n], (C_2, C_2'), [n, n-1, 2])$$

has minimum Euclidean distance $min\{2\sqrt{d}, 2\sqrt{d'}, \sqrt{32}, \sqrt{n+8}\}$ and volume $vol(\Gamma) = 2^{2n+1}/\{|C_2| + |C_2'|\}$. If $C_2 = C_2'$ is a self-orthogonal linear code containing the all-1 vector, then Γ is a lattice.

Proof: The statements concerning the minimum Euclidean distance and volume are by now obvious. Γ is a lattice if and only if the cosets it consists of form a subgroup of $(\mathbb{Z})^n/(8\mathbb{Z})^n$. The last claim follows from the addition rules given earlier. ■

This method yields the densest known packings in dimensions $18, 20, 24, 27, 28, 29, 30$. In each case C_2, C_2' are an orthogonal pair of linear codes with the same parameters. These parameters are

$$[18, 9, 6], [20, 9, 7], [24, 12, 8], [27, 13, 8], [28, 14, 8], [29, 14, 8], [30, 15, 8].$$

Only in dimension 24 can we choose $C_2 = C_2'$. This is the extended binary Golay code and we obtain a construction of the famous Leech lattice. All the other packings are non-lattice packings. The orthogonal pair with parameters $[20, 9, 7]$ may be derived from the extended Golay code G : choose C_2 to be the subcode vanishing in the first three coordinates, projected to the last 20 coordinates, and C_2' the subcode vanishing at coordinates 1,2 and 4, also projected to the last 20 coordinates. The orthogonal pair in dimension 18 can be chosen as extended quadratic residue codes.

3 Recursive constructions

The following are relatively straightforward recursive constructions.

Lemma 1 *If there are packings of center densities δ_N, δ_j in dimensions N and j, then there is an $(N+j)-$dimensional packing of center density $\delta_1\delta_2$.*

Proof: Let Γ_1, Γ_2 be the packings whose existence is assumed above. We can choose the minimum distance of both packings to be $= 2$. The $(N+j)-$dimensional packing $\Gamma_1 \oplus \Gamma_2$ still has minimum Euclidean distance 2, hence $\delta(\Gamma_1 \oplus \Gamma_2) = vol(\Gamma_1 \oplus \Gamma_2)^{-1} = \delta_1\delta_2$. ■

The following Theorem may be proved along the lines of [5], page 167:

Theorem 2 (Mordell's inequality) *Let $\Gamma \subset \mathbb{R}^n$ be an n-dimensional lattice of center density δ, not less dense than its dual Γ^*. Let $0 \neq x \in \Gamma^*$ be a vector of minimum norm. Then $< x >^\perp \cap \Gamma$ is an $(n-1)$-dimensional lattice of center density $\geq \frac{1}{2}\delta^{(n-2)/n}$.*

4 Some packings in high dimensions

We note that in a number of dimensions use of new codes constructed by us in [1, 2, 3, 4] as ingredients in the coset-codes construction yields packings, which are denser that what can be derived from known packings via Lemma 1 or Theorem 2. The new codes used in these constructions can be derived from the following codes: $[144, 51, 32]_2, [140, 50, 32]_2, [155, 132, 8]_2, [162, 138, 8]_2,$ $[86, 77, 5]_3, [85, 74, 6]_3, [86, 54, 14]_3$. Naturally it has to be expected that more sophisticated constructions will yield improvements in all these cases. Still it is noteworthy that the coset-code construction in its simplest form is capable of producing dense packings in low dimensions as well as in rather high dimensions. We conclude with a couple of examples.

In dimension 110 case $m = 2$ of the coset-code construction applied to ternary codes $[55, 1, 54]_3, [55, 25, 18]_3, [55, 44, 6]_3,$ and $[55, 54, 2]_3$ yields density $3^{41.5}$. In dimension 170 we can use ternary codes $[85, 16, 42]_3, [85, 53, 14]_3,$ $[85, 76, 5]_3$ and $[85, 84, 2]_3$ and obtain density $7^{85}/3^{68.5}$. In dimension 140 we can apply case $m = 1$ of the coset-code method. Binary codes $[140, 1, 128]_2,$ $[140, 50, 32]_2, [140, 117, 8]_2$ and $[140, 139, 2]_2$ yield a packing of density 2^{97}.

References

[1] J.Bierbrauer, Y.Edel: *New code parameters from Reed-Solomon subfield codes, IEEE Transactions on Information Theory* **43**(1997),953-968.

[2] J.Bierbrauer, Y.Edel: *Extending and lengthening BCH-codes, Finite Fields and Their Applications* **3**(1997),314-333.

[3] J.Bierbrauer, Y.Edel: *Inverting construction Y1 , IEEE Transactions on Information Theory* **44**(1998),1993.

[4] J.Bierbrauer, Y.Edel and L.Tolhuizen: *New codes via the lengthening of BCH codes with UEP codes,* submitted for publication in *Finite Fields and Their Applications.*

[5] J.H.Conway, N.J.A.Sloane : *Sphere packings, lattices and groups,* Springer 1988, ^{2}1993.

[6] G.D.Forney: *Coset Codes*, IEEE Transactions on Information Theory, *Part I:Introduction and Geometrical Classification*,1123-1151 *Part II: Binary lattices and related codes*,1152-1187.

[7] F.R.Kschischang and S.Pasupathy: *Some ternary and quaternary codes and associated sphere packings,* IEEE Transactions on Information Theory 38(1992), 227-246.

[8] A. Vardy: *A new sphere packing in 20 dimensions,* Inventiones Mathematicae **121**, 119-134.

[9] A. Vardy: *Density doubling, double-circulants, and new sphere packings,* manuscript.