Packings with large minimum kissing numbers

Noga Alon [*]

Abstract

For each proper power of 4, n, we describe a simple explicit construction of a finite collection of pairwise disjoint open unit balls in R^n in which each ball touches more than $2^{\sqrt{n}}$ others.

A *packing* of balls in the Euclidean space is a finite or infinite collection of pairwise disjoint open unit balls in R^n. It is called a *lattice packing* if the centers of the balls form a lattice in R^n. The *minimum kissing number* of a packing is the minimum number of balls touching a given one. Note that for a lattice packing this is simply the number of balls touching any given one, since every ball touches the same number of others. The problem of existence and construction of lattice packings with high kissing numbers received a considerable amount of attention, and there are several known constructions that show that the kissing number of a lattice packing of balls in R^n may be at least $n^{\Omega(\log n)} = 2^{\Omega(\log^2 n)}$. See [3], [4], [2], [6], and [5]. The problem of constructing finite packings with a large minimum kissing number received much less attention. In this short note we consider this problem and construct finite packings in R^n with much higher kissing numbers than those of the known lattice packings. For each (proper) power of 4, n the kissing number of our packing in R^n exceeds $2^{\sqrt{n}}$. To do so, we construct, for each integer $k \geq 2$, a linear, binary, error correcting code of length $n = 4^k$, dimension $k(2^{k-1}+1)$ and minimum distance $n/4$ in which the number of words of minimum Hamming weight is

$$(2^k - 1)\binom{2^k}{2^{k-1}} > 2^{2^k} = 2^{\sqrt{n}}.$$

It is easy to check that the finite collection of balls of radius $\sqrt{n}/4$ centered at all the vectors of this linear code (considered as real vectors) forms a finite packing of balls whose minimum kissing number is

$$(2^k - 1)\binom{2^k}{2^{k-1}} > 2^{2^k} = 2^{\sqrt{n}}.$$

Our construction is a concatenation code which is a variant of one of the constructions in [1]. Here are the details. Let $F = GF(2^k)$ be the finite field with 2^k elements, where each member of F is represented by a binary vector of length k. Construct the generating matrix A of a linear code over $GF(2)$ as follows. A has $k(2^{k-1}+1)$ rows and 4^k columns. Let $v_1, \ldots, v_k$ be a basis of

[*] Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il.

$GF(2^k)$ over $GF(2)$. The rows of A are indexed by pairs (i,j) with $0 \leq i \leq 2^{k-1}$ and $1 \leq j \leq k$. The columns are indexed by pairs (x,y) where x and y are in F. Now $A((i,j),(x,y))$ is defined as $< v_j x^i, y >$, where here the product $v_j x^i$ is computed in F and $<,>$ denotes the inner product modulo 2 of vectors of length k. Consider a linear combination of rows of A. This is a binary vector that has in column (x,y) the value

$$< \sum_{i=0}^{2^{k-1}} \sum_{j=1}^{k} \epsilon_{i,j} v_j x^i, y > .$$

Note that the sum

$$\sum_{i=0}^{2^{k-1}} \sum_{j=1}^{k} \epsilon_{i,j} v_j x^i$$

is simply a polynomial of degree at most 2^{k-1} over F, and therefore it is zero for at most 2^{k-1} different values of x in F. If it is not zero for some x then as y varies exactly half of the elements y give a 0 inner product with it and exactly half give a 1 product. Thus the Hamming weight is determined by the number of zeros (in F) of the polynomial. There are only $2^{k-1}+1$ distinct weights and the minimum weight is obtained from polynomials with 2^{k-1} roots. The number of such polynomials is precisely

$$(2^k - 1)\binom{2^k}{2^{k-1}},$$

where the $2^k - 1$ factor comes from the fact that the polynomials are not necessarily monic, and the binomial coefficient is the number of ways to choose the roots of the polynomial. This proves the desired result and hence supplies the desired packings as well. Note that by letting y in the construction above vary over $F - \{0\}$ instead of F we get a related code of length $n = 4^k - 2^k$ and the same dimension and weight distribution as the above one. Note also that by changing the upper bound for i in the definition of the generating matrix A from 2^{k-1} to an arbitrary parameter $h(< 2^k)$ we get other codes with interesting parameters. A similar construction works, of course, for fields of other characteristics.

It would be interesting to decide if there is a linear binary code of length n in which the number of words of minimum Hamming weight is $2^{\Omega(n)}$. It would also be interesting to decide if there is a lattice packing in R^n whose kissing number is $2^{\Omega(n)}$. We strongly suspect that such codes and such lattice packings do exist.

Acknowledgment I would like to thank N. Sloane for pointing out an error in a previous version of this note and for helpful comments.

References

[1] N. Alon, O. Goldreich, J. Hastad and R. Peralta, *Simple constructions of almost k-wise independent random variables*, Proc. 31^{st} IEEE FOCS, St. Louis, Missouri, IEEE (1990), 544-553. See also: Random Structures and Algorithms 3 (1992), 289-304.

[2] E. S. Barnes and N. J. A. Sloane, *New lattice packings of spheres*, Canadian J. Math. 35 (1983), 30-41.

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

[4] A. Bos, J. H. Conway and N. J. A. Sloane, *Further lattice packings in high dimensions*, Mathematika 29 (1982), 171-180.

[5] J. H. Conway and N. J. A. Sloane, **Sphere packings, lattices and groups**, Springer Verlag, 1988.

[6] J. Leech, *Some sphere packings in higher space*, Canadian J. Math. 16 (1984), 657-682.