On Kissing Numbers in Dimensions 32 to 128

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg, Germany

E. M. Rains and *N. J. A. Sloane*

AT&T Labs-Research
180 Park Avenue
Florham Park, NJ 07932-0971, USA

Submitted: April 9, 1998; Accepted: April 13, 1998

ABSTRACT

An elementary construction using binary codes gives new record kissing numbers in dimensions from 32 to 128.

1. Introduction

Let τ_n denote the maximal kissing number in dimension n, that is, the greatest number of n-dimensional spheres that can touch another sphere of the same size. Although asymptotic bounds on τ_n are known [5], little is known about explicit constructions, especially for $n > 32$. Up to now the best explicit constructions have come from lattice packings. The kissing number τ of the Barnes-Wall lattice[1] BW_n in dimension $n = 2^m$ is $\prod_{i=1}^{m}(2^i + 2)$, although for $m \geq 5$ this is weak (146,880, 9,694,080 and 1,260,230,400 in dimensions 32, 64 and 128, for example). In contrast, Quebbemann's lattice Q_{32} [14], [5, Chap. 8] has $\tau = 261{,}120$.

In recent years the kissing numbers of a few other lattices in dimensions > 32 have been determined. Nebe [10] shows that the Mordell-Weil lattice MW_{44} has $\tau = 2{,}708{,}112$. Nebe [11] shows that a 64-dimensional lattice constructed in [10] is extremal 3-modular, and so by modular form theory has $\tau = 138{,}458{,}880$. Bachoc and Nebe [1] give an 80-dimensional lattice with $\tau = 1{,}250{,}172{,}000$. Elkies [6] calculated the kissing number of his lattice MW_{128}: it is 218,044,170,240, over 170 times that of BW_{128}.

In the present note, we show that an elementary construction using binary codes gives better values than all of these. However, our packings are just local arrangements of spheres

[1] The subscript gives the dimension.

around the origin: we do not know if they can be modified to produce dense *infinite* packings.

2. The construction

Let $\mathcal{C}(n,d)$ (resp. $\mathcal{C}(n,d,w)$) denote a set of binary vectors of length n and Hamming distance $\geq d$ apart (resp. and with constant weight w). The maximal size of such a set is denoted by $A(n,d)$ (resp. $A(n,d,w)$) [2], [9].

One way to achieve the kissing number $\tau_8 = 240$ in eight dimensions is to take as centers of spheres the vectors of shape $\pm 1^8$, with a unique support (a code $\mathcal{C}(8,8,8)$!) and signs taken from a $\mathcal{C}(8,2)$, together with the vectors of shape $\pm 2^2 0^6$, where the supports are taken from a $\mathcal{C}(8,2,2)$ and the signs from a $\mathcal{C}(2,1)$. Taking all these codes to be as large as possible, we obtain a total of

$$A(8,8,8)A(8,2) + A(8,2,2)A(2,1) = 1 \cdot 2^7 + \binom{8}{2} 2^2 = 240$$

spheres touching the sphere at the origin.

Our construction generalizes this as follows. For a given dimension n, we choose a sequence of support sizes n_0, $n_1, \ldots, n_\mu$ satisfying

$$n \geq n_0 \geq 4n_1 \geq 4^2 n_2 \geq \cdots \geq 4^\mu n_\mu \geq 1 \ . \tag{1}$$

The ν^{th} set of centers that we use, for $0 \leq \nu \leq \mu$, consists of vectors of shape $\pm a_\nu^{n_\nu} 0^{n-n_\nu}$, where $a_\nu = \sqrt{n_0/n_\nu}$, the supports are taken from a $\mathcal{C}(n, n_\nu, n_\nu)$ and the signs from a $\mathcal{C}(n_\nu, \lceil \frac{n_\nu}{4} \rceil)$. With optimal codes, the total number of vectors is

$$\sum_{\nu=0}^{\mu} A(n, n_\nu, n_\nu) A\left(n_\nu, \left\lceil \frac{n_\nu}{4} \right\rceil\right) \ . \tag{2}$$

It is easy to check that all vectors have length $\sqrt{n_0}$, and that by (1) the distance between any two distinct vectors is $\geq \sqrt{n_0}$. It follows that (2) is a lower bound on τ_n.

Remarks

(1) Even if we do not know the exact values of $A(n,d,w)$ and $A(n,d)$ mentioned in (2), we can replace them by any available lower bounds, and still obtain a lower bound on the kissing number τ_n. There is some freedom in choosing the n_ν, which helps to compensate for our ignorance.

(2) A table of lower bounds on $A(n,d)$ has been given by Litsyn [7], extending the table in [9]. A table of lower bounds on $A(n,d,w)$ for $n \leq 28$ is given in [2], but for larger n little is known. A very incomplete table for $n > 28$ can be found in [15].

(3) The construction gives a set of points on a sphere with angular separation of 60°. It can obviously be modified to produce spherical codes with other angles.

3. Examples

We illustrate the construction by giving new records in dimensions 32, 36, 40, 44, 64, 80 and 128. For other examples see [12], and for further details about the codes see [7], [15].

n=32. We take $n_0 = 32$, $n_1 = 8$, $n_2 = 2$ and use $A(32,8) \geq 2^{17}$ from [3], $A(32,8,8) \geq 1117$ from the complement of a lexicographic code $\mathcal{C}(32,8,24)$ (cf. [4]), obtaining a kissing number of $A(32,32,32)A(32,8) + A(32,8,8)A(8,2) + A(32,2,2)A(2,1) \geq 1 \cdot 2^{17} + 1117 \cdot 2^7 + \binom{32}{2} \cdot 2^2 =$ 276,032.

n=36. Let the 36 coordinates be labeled (i,j), $0 \leq i,j \leq 5$, and let the symmetric group S_6 act by $(i,j) \to (i^\pi, j^{\sigma(\pi)})$, where $\pi \in S_6$ and σ is the outer automorphism of S_6. One can find a set of 17 orbits under the alternating group A_6, of sizes ranging from 45 to 360, whose union forms a constant weight code showing that $A(36,8,8) \geq 2385$. We take $n_0 = 32$, $n_1 = 8$, $n_2 = 2$ and obtain a kissing number of $A(36,32,32)A(32,8) + A(36,8,8)A(8,2) + A(36,2,2)A(2,1) \geq 1 \cdot 2^{17} + 2385 \cdot 2^7 + \binom{36}{2} \cdot 4 = 438{,}872$.

An alternative approach can be based on Warren D. Smith's discovery (personal communication, May 1997) that the 2754 minimal vectors of the self-dual length 18 distance 8 code over $\mathbb{F}_4$ [8] yields $\tau_{36} \geq 2754 \cdot 2^7 = 352{,}512$ by changing any even number of signs. By adjoining additional vectors with fractional coordinates R. H. Hardin and N. J. A. Sloane increased this to 386,570, which held the record until it was overtaken by the present construction. It is quite possible that with better clique-finding the $\mathbb{F}_4$ approach will regain the lead.

n=40. We take $n_0 = 40$, $n_1 = 8$, $n_2 = 2$, use a lexicographic code for $A(40,8,8)$, and obtain $A(40,40,40)A(40,10) + A(40,8,8)A(8,2) + A(40,2,2)A(2,1) \geq 1 \cdot 589824 + 3116 \cdot 2^7 + \binom{40}{2} \cdot 2^2 =$ 991,792.

n=44. $A(44,44,44)A(44,11) + A(44,8,8)A(8,2) + A(44,2,2)A(2,1) \geq 1 \cdot 2^{21} + 6622 \cdot 2^7 + \binom{44}{2} \cdot 4 = 2{,}948{,}552$.

n=48. In 48 dimensions the three known unimodular extremal unimodular lattices [5], [10] have kissing number 52,416,000. Our present construction gives less than half this value.

n=64. The words of weight 16 in an extended cyclic code $\mathcal{C}(64,16)$ of size 2^{28} from [13] show that $A(64,16,16) \geq 30{,}828$. In this way we obtain a kissing number of 331,737,984.

n=80. By taking 4 orbits under $L_2(79)$ we obtain $A(80,16,16) \geq 143{,}780$. We take $n_0 = 64$, $n_1 = 16$, $n_2 = 4$, $n_3 = 1$ and obtain $\tau \geq 1{,}368{,}532{,}064$.

n=128. This is the most dramatic improvement, so we give a little more detail. Our construction uses:

$$\begin{array}{lcl}
A(128,128,128)A(128,32) \text{ vectors } \pm 1^{128}: & \geq & 1 \cdot 2^{43} \\
A(128,32,32)A(32,8) \text{ vectors } \pm 2^{32}0^{96}: & \geq & 512064 \cdot 2^{17} \\
A(128,8,8)A(8,2) \text{ vectors } \pm 4^{8}0^{120}: & \geq & 2704592 \cdot 2^{7} \\
A(128,2,2)A(2,1) \text{ vectors } \pm 8^{2}0^{126}: & \geq & \underline{\binom{128}{2} \cdot 4} \\
\text{for a total of} & & 8{,}863{,}556{,}495{,}104
\end{array}$$

Here $A(128,32) \geq 2^{43}$ comes from a BCH code [9, p. 267], $A(128,32,32) \geq 512064$ from a union of two orbits under $L_2(127)$, $A(32,8) \geq 2^{17}$ from [3], and $A(128,8,8) \geq 2704592$ is obtained by shortening a $\mathcal{C}(129,8,8)$ of size 2883408 formed from the union of 11 orbits of size 262128 under $L_2(128)$. The result is more than 40 times that of the Mordell-Weil lattice.

We do not expect any of these new records to survive for long, since our lower bounds for $A(n,d)$ and $A(n,d,w)$ are very weak. However, it is interesting that such a simple construction gives such dramatic improvements over the kissing numbers of the best lattices known.

References

[1] C. Bachoc and G. Nebe, *Extremal lattices of minimum 8 related to the Mathieu group* M_{22}, J. reine angew. Math. **494** (1998), 129–140.

[2] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, *A new table of constant weight codes*, IEEE Trans. Inform. Theory **36** (1990), 1334–1380.

[3] Y. Cheng and N. J. A. Sloane, *Codes from symmetry groups and a [32,17,8] code*, SIAM J. Disc. Math. **2** (1989), 28–37 .

[4] J. H. Conway and N. J. A. Sloane, *Lexicographic codes: error-correcting codes from game theory*, IEEE Trans. Inform. Theory **32** (1986), 337–348

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 3rd edition, 1998.

[6] N. D. Elkies, personal communication, 1998.

[7] S. Litsyn, *An updated table of the best binary codes known*, in W. C. Huffman and R. A. Brualdi, editors, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998, to appear.

[8] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane and H. N. Ward, *Self-dual codes over GF(4)*, J. Combin. Theory, Series **A**, **25** (1978), 288-318.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[10] G. Nebe, *Some cyclo-quaternionic lattices*, J. Alg. **199** (1998), 472–498.

[11] G. Nebe, *A method of computing the minimum of certain lattices*, preprint.

[12] G. Nebe and N. J. A. Sloane, *Table of the highest kissing numbers presently known*, published electronically at http://www.research.att.com/~njas/lattices/kiss.html.

[13] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, MIT Press, Cambridge, MA, 2nd ed., 1972

[14] H.-G. Quebbemann, *Lattices with theta-functions for* $G(\sqrt{2})$ *and linear codes*, J. Alg. **105** (1987), 443–450

[15] E. M. Rains and N. J. A. Sloane, *A table of lower bounds on constant weight codes*, published electronically at http://www.research.att.com/~njas/codes/Andw/.