A Note on the Kissing Numbers of Superballs

Lanju Xu

Department of Mathematics,
Tsinghua University,
Beijing 100084, People's Republic of China
xulj03@mails.tsinghua.edu.cn

Abstract. The lower bounds for the translative kissing numbers of superballs are studied in this note. We improve the bound given by Larman and Zong. Furthermore, we give a constructive bound based on algebraic-geometry codes that also improves the bound by Larman and Zong in almost all cases.

1. Introduction

As usual, denote by K an n -dimensional convex body with boundary $\partial(K)$. The translative kissing number $N(K)$ of K is the largest number of nonoverlapping translates of K which can be brought into contact with K at its boundary. The lattice kissing number $N^*(K)$ of K is the similar number when the translates are taken from any lattice packing of K .

It is well known that $N^*(K) \leq N(K) \leq 3^n - 1$ for every n -dimensional convex body (see [7] and [4]). On the other hand, the best lower bounds of $N^*(K)$ and $N(K)$ for all n -dimensional convex bodies are central problems in the study of packings. They have been studied by many mathematicians. For more details refer to [1], [9], [3] and [12].

In this note we concentrate on a particular type of convex bodies, i.e. superballs. Let $\alpha \geq 1$ and denote by $\mathcal{B}_\alpha$ the n -dimensional superball

$$\left\{ \mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n : \left(\sum_{i=1}^n |x_i|^\alpha \right)^{1/\alpha} \leq 1 \right\}.$$

The Minkowski-metric given by $\mathcal{B}_\alpha$ can be represented as

$$\delta^{\mathcal{B}_\alpha}(\mathbf{x}, \mathbf{y}) := \left(\sum_{i=1}^n |x_i - y_i|^\alpha \right)^{1/\alpha}.$$

This is equivalent to saying that $N(\mathcal{B}_\alpha)$ is the size of the largest set C of points of $\partial(\mathcal{B}_\alpha)$, such that any two distinct points of C have Minkowski-metric at least 1, i.e.

$$N(\mathcal{B}_\alpha) = \max\{\text{card}\{C\}: C \subset \partial(\mathcal{B}_\alpha), \delta^{\mathcal{B}_\alpha}(C) \geq 1\}, \quad (1.1)$$

where

$$\delta^{\mathcal{B}_\alpha}(C) := \inf_{\substack{\mathbf{x}, \mathbf{y} \in C \\ \mathbf{x} \neq \mathbf{y}}} \delta^{\mathcal{B}_\alpha}(\mathbf{x}, \mathbf{y}).$$

In 1999 Larman and Zong [5] showed

$$\frac{1}{n} \log_2(N(\mathcal{B}_\alpha)) \geq 0.1072 \log_2 3 \approx 0.1699. \quad (1.2)$$

The purpose of this note is to improve the bound (1.2). We will show that the bound (1.2) can be improved for every $\alpha \geq 1$. In particular, we show that $(1/n) \log_2(N(\mathcal{B}_\alpha)) \geq 1 + o(1)$ as α tends to ∞ . Furthermore, we give a constructive bound based on algebraic-geometry codes, which also improves the bound (1.2).

In Section 2 we employ a similar method used to derive the Gilbert–Varshamov (G-V for short) bound in coding theory to improve the lower bound of the translative kissing number of superballs. In Section 3 we recall some results on coding theory and in Section 4 we give two constructive bounds from error-correcting codes which are of exponential and polynomial time, respectively. This idea has already been used by several researchers in investigating packing density [6], [8].

2. G-V Type Lower Bound

For a positive integer $m \leq n$, let

$$\mathcal{J}_n(m) = \left\{ \mathbf{u} = (u_1, \dots, u_n): \sum_{i=1}^n |u_i| = m, u_i \in \{0, \pm 1\} \ (1 \leq i \leq n) \right\}.$$

Then the cardinality of $\mathcal{J}_n(m)$ is $\binom{n}{m} 2^m$.

For a point $\mathbf{u} \in \mathcal{J}_n(m)$, define

$$\mathcal{B}_{\alpha,n}(\mathbf{u}, m) = \left\{ \mathbf{v} = (v_1, \dots, v_n) \in \mathcal{J}_n(m): \sum_{i=1}^n |v_i - u_i|^\alpha < m \right\}.$$

Let $B_{\alpha,n}(m)$ denote the cardinality of $\mathcal{B}_{\alpha,n}(\mathbf{u}, m)$. We have

$$B_{\alpha,n}(m) = \sum_{2t+2^a \cdot x < m} \binom{m}{t} \binom{n-m}{t} \binom{m-t}{x} 2^t,$$

which is independent of the center $\mathbf{u}$.

Lemma 2.1. *If M is a positive integer satisfying*

$$M \cdot B_{\alpha,n}(m) < \binom{n}{m} 2^m,$$

then there exists a subset C of $\partial(\mathcal{B}_\alpha)$ such that $|C| \geq M + 1$ and $\delta^{\mathcal{B}_\alpha}(C) \geq 1$.

Proof. First choose an arbitrary point $\mathbf{c}_1$ from $\mathcal{J}_n(m)$. Pick up a point $\mathbf{c}_2$ from $\mathcal{J}_n(m) \setminus \mathcal{B}_{\alpha,n}(\mathbf{c}_1, m)$, then pick up a point $\mathbf{c}_3$ from $\mathcal{J}_n(m) \setminus (\mathcal{B}_{\alpha,n}(\mathbf{c}_1, m) \cup \mathcal{B}_{\alpha,n}(\mathbf{c}_2, m))$.

Continuing in this fashion, we can get a subset $C := \{(1/m^{1/\alpha})\mathbf{c}_1, \dots, (1/m^{1/\alpha})\mathbf{c}_{M+1}\}$ of $\partial(\mathcal{B}_\alpha)$ such that

$$\mathbf{c}_i \in \mathcal{J}_n(m) \setminus \left(\bigcup_{j=1}^{i-1} \mathcal{B}_{\alpha,n}(\mathbf{c}_j, m) \right)$$

for any $2 \leq i \leq M+1$. This is because the set $\mathcal{J}_n(m) \setminus (\bigcup_{j=1}^{i-1} \mathcal{B}_{\alpha,n}(\mathbf{c}_j, m))$ is not empty due to the fact that

$$\left| \mathcal{J}_n(m) \setminus \left(\bigcup_{j=1}^{i-1} \mathcal{B}_{\alpha,n}(\mathbf{c}_j, m) \right) \right| \geq \binom{n}{m} 2^m - M \cdot B_{\alpha,n}(m) > 0.$$

From the above procedure, it is easy to get $\delta^{\mathcal{B}_\alpha}(C) \geq 1$. This finishes the proof. $\square$

For $0 \leq \sigma < 1$, we define the q -ary entropy function H_q by setting $H_q(0) = 0$ and

$$H_q(\sigma) := \sigma \log_q(q-1) - \sigma \log_q \sigma - (1-\sigma) \log_q(1-\sigma)$$

for $0 < \sigma < 1$. By Stirling's formula, we have

Lemma 2.2. *For a real $0 \leq \sigma \leq 1$, we have*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log_2 \binom{n}{\lfloor \sigma n \rfloor} = H_2(\sigma).$$

Theorem 2.3. *We have*

$$\frac{1}{n} \log_2(N(\mathcal{B}_\alpha)) \geq \max_{0 < \sigma < 1} \min_{0 \leq y \leq \min\{\sigma/2, 1-\sigma\}} f(\sigma, y), \quad (2.1)$$

where

$$f(\sigma, y) = (\sigma - y) \left(1 - H_2 \left(\frac{\sigma - 2y}{2^\alpha(\sigma - y)} \right) \right) + H_2(\sigma) - \sigma H_2 \left(\frac{y}{\sigma} \right) - (1 - \sigma) H_2 \left(\frac{y}{1 - \sigma} \right).$$

Proof. By Lemma 2.1 and (1.1), we have

$$N(\mathcal{B}_\alpha) \geq \max_{0 < m \leq n} \frac{\binom{n}{m} 2^m}{B_{\alpha,n}(m)} + 1,$$

where

$$B_{\alpha,n}(m) = \sum_{2t + 2^\alpha \cdot x < m} \binom{m}{t} \binom{n-m}{t} \binom{m-t}{x} 2^t.$$

The term $\binom{m-t}{x}$ increases as x increases if $2t + 2^a \cdot x < m$. Put $m = \lfloor \sigma n \rfloor$ and $t = \lfloor yn \rfloor$. Then

$$\begin{aligned} \limsup_{n \rightarrow \infty} \frac{\log_2 B_{\alpha,n}(m)}{n} &= \lim_{n \rightarrow \infty} \frac{1}{n} \log_2 \left(\sum_{2t+2^a \cdot x < m} \binom{m}{t} \binom{n-m}{t} \binom{m-t}{x} 2^t \right) \\ &\leq \lim_{n \rightarrow \infty} \frac{1}{n} \log_2 \left(\binom{\lfloor \sigma n \rfloor}{\lfloor yn \rfloor} \binom{n - \lfloor \sigma n \rfloor}{\lfloor yn \rfloor} \binom{\lfloor \sigma n \rfloor - \lfloor yn \rfloor}{\lfloor (\sigma - 2y)n/2^a \rfloor} 2^{\lfloor yn \rfloor} \right) \\ &\leq \sigma H_2\left(\frac{y}{\sigma}\right) + (1 - \sigma) H_2\left(\frac{y}{1 - \sigma}\right) \\ &\quad + (\sigma - y) H_2\left(\frac{\sigma - 2y}{2^a(\sigma - y)}\right) + y. \end{aligned}$$

We have

$$\frac{1}{n} \log_2(N(\mathcal{B}_\alpha)) \geq \max_{0 < \sigma < 1} \left\{ \sigma + H_2(\sigma) - \limsup_{n \rightarrow \infty} \frac{\log_2 B_{\alpha,n}(m)}{n} \right\}.$$

The desired result follows. $\square$

The lower bound is not expressed in a simple form. However its computation is a finite problem and can easily be handled by a computer. Here we just list some results for some small integers α .

Corollary 2.4.

$$\begin{aligned} \frac{1}{n} \log_2(N(\mathcal{B}_1)) &\geq 0.1772, & \frac{1}{n} \log_2(N(\mathcal{B}_2)) &\geq 0.2058, \\ \frac{1}{n} \log_2(N(\mathcal{B}_3)) &\geq 0.4505, & \frac{1}{n} \log_2(N(\mathcal{B}_4)) &\geq 0.6627. \end{aligned}$$

From the above numerical results, we can see that our bound (2.1) is better than the one given in (1.2).

3. Error-Correcting Codes

There is a remarkable connection between packings and codes [1], [6]. Let us recall some important results about codes.

Let $\mathbb{F}_q$ be the finite field with q elements. A q -ary code (n, K, d) is a K -element subset of $\mathbb{F}_q^n$ for which the Hamming distance is at least d . If the q -ary code forms a subspace of $\mathbb{F}_q^n$, we call it a linear code, denoted by $[n, k, d]$, where $k = \log_q K$.

Let $A(n, d)$ be the maximal possible value of K among q -ary codes (n, K, d) . We define

$$a(\delta) := \limsup_{n \rightarrow \infty} \frac{\log_q A(n, \delta n)}{n}.$$

Then the lower G-V bound is given by

$$a_q(\delta) \geq 1 - H_q(\delta), \quad 0 \leq \delta \leq \frac{q-1}{q}. \quad (3.1)$$

The lower bound can be sharpened for $q = p^{2m} \geq 49$ using algebraic geometry. Here is a simple construction due to Goppa [2].

Let $\mathcal{X}$ be a smooth projective absolute irreducible curve over $\mathbb{F}_q$ of genus g . Let $P_1, P_2, \dots, P_n$ be n distinct rational points of $\mathcal{X}$. Choose a divisor G with $g \leq \deg G < n$ and

$$\text{Supp}(G) \cap \{P_1, P_2, \dots, P_n\} = \emptyset.$$

Let $\mathcal{L}(G) := \{f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} : \text{div}(f) + G \geq 0\} \cup \{0\}$. Consider the map

$$\varphi: \mathcal{L}(G) \rightarrow \mathbb{F}_q^n, \quad f \mapsto (f(P_1), f(P_2), \dots, f(P_n)).$$

Then the image of φ , which is called an algebraic-geometry code, is a q -ary linear code of length n , dimension $k \geq \deg G - g + 1$, and distance $d \geq n - \deg G$. Modular curves [10] give the Tsfasman–Vlăduț–Zink (TVZ for short) lower bound for squares q :

$$a_q(\delta) \geq 1 - \delta - (\sqrt{q} - 1)^{-1}. \quad (3.2)$$

We also need the following method of combining codes (concatenation). For a linear $[n, k, d]$ code C_0 over $\mathbb{F}_q$, and for a linear $[N, K, D]$ code C_1 over $\mathbb{F}_{q^k}$, there exists an $[nN, kK, dD]$ code C over $\mathbb{F}_q$ constructed as follows:

$$\mathbb{F}_q^{kK} \simeq \mathbb{F}_q^K \xrightarrow{C_1} \mathbb{F}_{q^k}^N \simeq (\mathbb{F}_q^k)^N \xrightarrow{(C_0, \dots, C_0)} \mathbb{F}_q^{nN}.$$

We concatenate a binary $[m, m, 1]$ -linear code with a sequence of algebraic-geometry codes over $\mathbb{F}_{2^m}$ achieving the TVZ bound and a binary $[m, m-1, 2]$ -linear code with a sequence of algebraic-geometry codes over $\mathbb{F}_{2^{m-1}}$ achieving the TVZ bound, respectively (see [11]). Then we have

Lemma 3.1.

(i) If m is even, then

$$a_2(\delta) \geq 1 - \frac{1}{2^{m/2} - 1} - m\delta. \quad (3.3)$$

(ii) If m is odd, then

$$a_2(\delta) \geq \left(1 - \frac{1}{2^{(m-1)/2} - 1} - \frac{m}{2}\delta\right) \frac{m-1}{m}. \quad (3.4)$$

Moreover, the bounds (3.3) and (3.4) are constructive in polynomial time.

4. Lower Bounds from Binary Codes

A binary (n, M, d) code C is a subset of $\mathbb{F}_2^n$ for which the Hamming distance is at least d . Regard $\mathbb{F}_2^n$ as lying in $\mathbb{R}^n$ by making the identification $\mathbb{F}_2 = \{+1, -1\}$. Then the set

$$\frac{1}{n^{1/\alpha}} C := \left\{ \frac{1}{n^{1/\alpha}} \mathbf{c} : \mathbf{c} \in C \right\}$$

is a subset of $\partial(\mathcal{B}_\alpha)$ with

$$\delta^{\mathcal{B}_\alpha} \left(\frac{1}{n^{1/\alpha}} C \right) \geq 2 \times \left(\frac{d}{n} \right)^{1/\alpha}. \quad (4.1)$$

If we require that $d \geq \lceil n/2^\alpha \rceil$, then (4.1) implies that $\delta^{\mathcal{B}_\alpha}((1/n^{1/\alpha})C) \geq 1$. Thus, we have

Lemma 4.1. *A binary (n, M, d) -code with $d \geq \lceil n/2^\alpha \rceil$ gives a lower bound*

$$N(\mathcal{B}_\alpha) \geq M.$$

In this section we give two lower bounds from binary codes, one from binary codes achieving the G-V bound and the other from algebraic-geometry codes. Furthermore, the lower bounds from algebraic-geometry codes are constructive in polynomial time.

By combining Lemma 4.1 and (3.1), we can immediately get the following result:

Theorem 4.2. *One has*

$$\frac{1}{n} \log_2(N(\mathcal{B}_\alpha)) \geq 1 - H_2 \left(\frac{1}{2^\alpha} \right). \quad (4.2)$$

By computation from the bound (4.2) as α taken some small integers and infinity, we get

Corollary 4.3.

$$(i) \quad \begin{aligned} \frac{1}{n} \log_2(N(\mathcal{B}_1)) &\geq 0, & \frac{1}{n} \log_2(N(\mathcal{B}_2)) &\geq 0.1887, \\ \frac{1}{n} \log_2(N(\mathcal{B}_3)) &\geq 0.4564, & \frac{1}{n} \log_2(N(\mathcal{B}_4)) &\geq 0.6627, \\ \frac{1}{n} \log_2(N(\mathcal{B}_5)) &\geq 0.7993, & \frac{1}{n} \log_2(N(\mathcal{B}_6)) &\geq 0.8838, \\ \frac{1}{n} \log_2(N(\mathcal{B}_7)) &\geq 0.9340, & \frac{1}{n} \log_2(N(\mathcal{B}_8)) &\geq 0.9631. \end{aligned}$$

$$(ii) \quad (1/n) \log_2(N(\mathcal{B}_\alpha)) \geq 1 + o(1) \text{ as } \alpha \text{ tends to infinity.}$$

Next, we derive another lower bound from algebraic-geometry codes. By combining Lemma 3.1 and (3.1), we can also get the following results:

Theorem 4.4.

$$(i) \quad \frac{1}{n} \log_2(N(\mathcal{B}_\alpha)) \geq \max_{2|m, m \geq 2} \left\{ 1 - \frac{1}{2^{m/2} - 1} - \frac{m}{2^\alpha} \right\}. \quad (4.3)$$

$$(ii) \quad \frac{1}{n} \log_2(N(\mathcal{B}_\alpha)) \geq \max_{2|(m-1), m \geq 3} \left\{ \left(1 - \frac{1}{2^{(m-1)/2} - 1} - \frac{m}{2^{1+\alpha}} \right) \frac{m-1}{m} \right\}. \quad (4.4)$$

Moreover, the bounds (4.3) and (4.4) are constructive in polynomial time.

From simple computations, we also have the following results:

Corollary 4.5.

$$\begin{aligned}
 \text{(i)} \quad & \frac{1}{n} \log_2(N(\mathcal{B}_1)) \geq 0, & \frac{1}{n} \log_2(N(\mathcal{B}_2)) &\geq 0.33333, \\
 & \frac{1}{n} \log_2(N(\mathcal{B}_3)) \geq 0.359694, & \frac{1}{n} \log_2(N(\mathcal{B}_4)) &\geq 0.57963, \\
 & \frac{1}{n} \log_2(N(\mathcal{B}_5)) \geq 0.723515, & \frac{1}{n} \log_2(N(\mathcal{B}_6)) &\geq 0.816609, \\
 & \frac{1}{n} \log_2(N(\mathcal{B}_7)) \geq 0.890377, & \frac{1}{n} \log_2(N(\mathcal{B}_8)) &\geq 0.937438.
 \end{aligned}$$

$$\text{(ii)} \quad (1/n) \log_2(N(\mathcal{B}_\alpha)) \geq 1 + o(1) \text{ as } \alpha \text{ tends to infinity.}$$

From the above numerical results, we can see the lower bounds given in (4.3) and (4.4) are slightly worse than the bound (4.2), but still better than the bound (1.2) except for $\alpha = 1$. Moreover, they can be constructed in polynomial time.

Acknowledgment

I am grateful to C. P. Xing for his help and guidance.

References

1. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattice and Groups*, Springer-Verlag, New York, 1999 (third edition).
2. V. D. Goppa, Codes on algebraic curves, *Dokl. Akad. Nauk SSSR* **259**(6) (1981), 1289–1290; *Soviet Math. Dokl.*, **24** (1981), 170–172.
3. B. Grünbaum, On a conjecture of H. Hadwiger, *Pacific J. Math.*, **11** (1961), 215–219.
4. H. Hadwiger, Über Treffanzahlen bei translationsgleichen Eikörpern, *Arch. Math.*, **8** (1957), 212–213.
5. D. G. Larman and C. Zong, On the kissing numbers of some special convex bodies, *Discrete Comput. Geom.*, **21** (1999), 233–242.
6. S. N. Litsyn and M. A. Tsfasman, Constructive high-dimensional sphere packings, *Duke Math. J.*, **54** (1987), 147–161.
7. H. Minkowski, *Geometrie der Zahlen*, Leipzig, Berlin, 1896, 1910; New York, Chelsea, 1953.
8. J. A. Rush and N. J. A. Sloane, An improvement to the Minkowski–Hlawka bound for packing superballs, *Mathematika*, **34** (1987), 8–18.
9. H. P. F. Swinnerton-Dyer, Extremal lattices of convex bodies, *Math. Proc. Cambridge Philos. Soc.*, **49** (1953), 161–162.
10. M. A. Tsfasman, S. G. Vlăduț and T. Zink, Modular curves, Shimura curves, and Goppa codes better than the Varshamov–Gilbert bound, *Math. Nachr.*, **104** (1982), 13–28.
11. S. G. Vlăduț, G. L. Katsman and M. A. Tsfasman, Modular curves and codes with polynomial construction complexity, *Problemy Peredachi Informatsii*, **20**(1) (1984), 3–15; *Probl. Inform. Transm.*, **20**(1) (1984).
12. C. Zong, The kissing numbers of tetrahedra, *Discrete Comput. Geom.*, **15** (1996), 239–252.

Received August 16, 2005, and in revised form January 10, 2006, and April 2, 2006.
Online publication February 28, 2007.