PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 9, September 2009, Pages 2953–2957
S 0002-9939(09)09888-8
Article electronically published on April 3, 2009

A CONSTRUCTIVE BOUND ON KISSING NUMBERS

CHAOPING XING

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. In the present paper, by making use of the concatenation of $17^2 - 1 = 288$ points on the sphere of radius 4 in $\mathbb{R}^{16}$ and subcodes of algebraic geometry codes over $\mathbb{F}_{17^2}$, we improve the best-known constructive bound on kissing numbers by A. Vardy.

1. INTRODUCTION

One classical question in the geometry of numbers is how many nonoverlapping balls of the same radius in n-dimensional Euclidean space $\mathbb{R}^n$ can be arranged so that they all just touch, or "kiss", another ball of the same size. This problem is equivalent to packing points on a sphere (i.e., the surface of a ball [1]).

Let us give a precise definition of kissing numbers. The *kissing number* K_n (or *Newton number* after the originator of the problem) is defined to be the largest number of nonoverlapping balls in $\mathbb{R}^n$ so that they all just touch a given ball (all balls here have the same size). The exact values of K_n are known only for a few small dimensions n. This is equivalent to saying that K_n is the size of the largest set of points on a sphere in $\mathbb{R}^n$ of radius r such that any two distinct points in the set have distance at least r. This motivates us to define spherical codes.

A spherical code S in $\mathbb{R}^n$ is a set of points on a sphere $\mathcal{S}_n(r)$ of radius r and center $\mathbf{0}$ ($\mathbf{0}$ denotes the origin) in $\mathbb{R}^n$; i.e., S is a subset of

$$\mathcal{S}_n(r) := \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^n : \sqrt{\sum_{i=1}^{n} x_i^2} = r \right\}.$$

The distance of S is defined to be

$$d_E(S) := \inf\{d_E(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y},\ \mathbf{x}, \mathbf{y} \in S\},$$

where $d_E(\mathbf{x}, \mathbf{y})$ denotes the Euclidean distance of two points $\mathbf{x}$ and $\mathbf{y}$. Thus, the kissing number is equal to

$$K_n = \max\{|S| : S \subset \mathcal{S}_n(r),\ d_E(S) \geq r\}. \tag{1.1}$$

Remark 1.1. (i) Note that K_n is independent of the radius r.

(ii) Some authors always consider spherical codes in $\mathcal{S}_n(1)$ (e.g., see [1, p. 24]). We find that sometimes it is more convenient if the radius is not fixed.

Received by the editors October 20, 2008, and, in revised form, January 9, 2009.
2000 *Mathematics Subject Classification.* Primary 11H06, 11H31, 05B40, 94B75.
The author was supported by the Singapore MOE Tier 2 grant T208B2206 and the National Scientific Research Project 973 of China 2004CB318000.

If the distance of S is strictly less than or greater than radius r, then we can generalize the definition of kissing numbers in terms of angles.

Let ϕ be an angle with $0 < \phi < 90^o$ and let r, ρ satisfy $\sin(\phi/2) = \rho/(2r)$. Then the kissing number $K_n(\phi)$ is defined by

$$K_n(\phi) := \max\{|S| : \ S \subset \mathcal{S}_n(r), \ d_E(S) \geq \rho\}. \tag{1.2}$$

It is clear that $K_n = K_n(60^o)$.

By (1.2), a spherical code $S \subset \mathcal{S}_n(r)$ with distance at least ρ gives a lower bound

$$K_n(\phi) \geq |S| \tag{1.3}$$

with $\sin(\phi/2) = \rho/(2r)$.

In this paper, we are interested in the asymptotic behavior of $K_n(\phi)$; i.e., we want to look at how $K_n(\phi)$ varies when n tends to infinity for a fixed ϕ. We define the asymptotic quantity

$$k(\phi) := \limsup_{n\to\infty} \frac{\log_2(K_n(\phi))}{n}.$$

Kabatiansky and Levenshtein [3] show that one has, for $0 < \phi < 90^o$,

$$k(\phi) \lesssim \frac{1+\sin(\phi)}{2\sin(\phi)} \log_2\left(\frac{1+\sin(\phi)}{2\sin(\phi)}\right) - \frac{1-\sin(\phi)}{2\sin(\phi)} \log_2\left(\frac{1-\sin(\phi)}{2\sin(\phi)}\right),$$

and for $0 < \phi < \phi^*$,

$$k(\phi) \lesssim -\frac{1}{2}\log_2(1-\cos(\phi)) - 0.0990, \tag{1.4}$$

where $\phi^* \approx 63^o$ is the root of the certain equation. In particular, when $\phi = 60^o$, (1.4) gives

$$k(60^0) \lesssim 0.401.$$

On the other hand, a lower bound on $k(\phi)$ is given in [6, 8] by

$$k(\phi) \geq -\log_2(\sin(\phi)). \tag{1.5}$$

This is an existence bound and cannot be constructed even in exponential time. In particular, we obtain

$$k(60^o) \geq -\log_2(\sin(60^o)) \approx 0.2075. \tag{1.6}$$

It is shown by A. Vardy (see [1]) that a sequence of spherical codes can be constructed in polynomial time and gives a lower bound

$$k(60^o) \geq \frac{2}{15} \approx 0.13333. \tag{1.7}$$

In this paper, we mainly focus on constructive lower bounds on $k(60^o)$. By employing algebraic geometry codes, we give an explicit construction of a spherical code sequence that gives a better constructive bound than (1.7).

Let us describe Vardy's method to get the bound (1.7) without detailed proof.

For an algebraic curve $\mathcal{X}$ over the finite field $\mathbb{F}_q$ of q elements, choose $n+1$ distinct $\mathbb{F}_q$-rational points $P_0, P_1, \ldots, P_n$ of $\mathcal{X}$. A one-point Goppa geometric code of length n over $\mathbb{F}_q$ is defined by

$$C_{\mathcal{X}}(mP_0; P_1, P_2, \ldots, P_n) := \{(f(P_1), f(P_2), \ldots, f(P_n)) : \ f \in \mathcal{L}(mP_0)\},$$

where $\mathcal{L}(mP_0)$ is the Riemann-Roch space defined by

$$\mathcal{L}(mP_0) := \{f \in \mathbb{F}_q(\mathcal{X})^* : \ \nu_{P_0}(f) \geq -m, \ \nu_P(f) \geq 0 \text{ for all } P \neq P_0\} \cup \{0\}.$$

The code $C_{\mathcal{X}}(mP_0; P_1, P_2, \ldots, P_n)$ has parameters $[n, k \geq m - g + 1, d \geq n - m]$. Moreover, this code can be explicitly constructed as long as the base curve $\mathcal{X}$ is explicitly given.

From [2], there is a family $\{\mathcal{X}\}$ of algebraic curves over $\mathbb{F}_{16^2}$ that can be explicitly constructed such that $N(\mathcal{X}) \to \infty$ and $N(\mathcal{X})/g(\mathcal{X}) \to 15$. For each curve $\mathcal{X}$ in this family, let $C_{\mathcal{X}}(mP_0; P_1, P_2, \ldots, P_n)$ be a one-point Goppa geometric code defined above with $n := N(\mathcal{X}) - 1$ and $m := \lfloor n/3 \rfloor$. Then the Hamming distance δ of the code is at least $n - m \geq 2n/3$.

The binary Preparata code of length 16 (see [4, p.99]) has parameters $(16, 2^8, 6)$. We change the $2^8 = 256$ codewords in this code into 256 points on the sphere $\mathcal{S}_{16}(4)$ of radius 4 in $\mathbb{R}^{16}$ by sending 1 to 1 and 0 to -1. Denote by S the set consisting of these 256 points on $\mathcal{S}_{16}(4)$. Then it is easy to see that $d_E(S) \geq \sqrt{4 \times 6} = \sqrt{24}$. Let χ be a bijection from $\mathbb{F}_{16^2}$ to S (such a bijection exists since these two sets have the same size). Then $(\chi(c_1), \ldots, \chi(c_n))$ is a point on the sphere $\mathcal{S}_{16n}(\sqrt{16n})$ for any codeword $(c_1, \ldots, c_n)$ of $C_{\mathcal{X}}(mP_0; P_1, P_2, \ldots, P_n)$. Thus, the set $\chi(C_{\mathcal{X}}(mP_0; P_1, P_2, \ldots, P_n))$ becomes a spherical code $S_{\mathcal{X}}$ on the sphere $\mathcal{S}_{16n}(\sqrt{16n})$ with $d_E(S_{\mathcal{X}}) \geq \sqrt{24\delta} \geq \sqrt{16n}$. Hence, we have

$$K_{16n} \geq |C_{\mathcal{X}}(mP_0; P_1, P_2, \ldots, P_n)| \geq (16^2)^{m-g(\mathcal{X})+1}.$$

The above lower bound gives the constructive bound (1.7) by letting $N(\mathcal{X}) \to \infty$.

In this paper, we extend the above method by A. Vardy and obtain the following result.

Theorem 1.2. *We have a constructive bound*

$$k(60^o) \geq \frac{1}{16}\left(\left(\frac{1}{3} - \frac{1}{16}\right)\log_2\left(17^2\right) + \log_2\left(1 - \frac{1}{17^2}\right)\right) \approx 0.138065. \tag{1.8}$$

2. Proof of Theorem 1.2

Lemma 2.1. *Let $\mathcal{X}$ be an algebraic curve over $\mathbb{F}_q$ with $n+1$ distinct $\mathbb{F}_q$-rational points $P_0, P_1, \ldots, P_n$. Let g be the genus of $\mathcal{X}$. If m is an integer satisfying $m > 2g + 2$, then*

$$\left|\mathcal{L}(mP_0) \setminus \bigcup_{i=1}^{n} \mathcal{L}(mP_0 - P_i)\right| \geq q^{m-g+1}\left(1 - \frac{1}{q}\right)^n - n2^n q^{g+1}. \tag{2.1}$$

Proof. Let $\ell = 2\lfloor m/2 - g \rfloor + 1 \leq m - 2g + 1$. By the inclusion and exclusion principle, we have

$$\begin{aligned}
\left|\bigcup_{i=1}^{n} \mathcal{L}(mP_0 - P_i)\right| &= \sum_{k=1}^{n}(-1)^{k+1} \sum_{i_1,\ldots,i_k} \left|\bigcap_{j=1}^{k} \mathcal{L}(mP_0 - P_{i_j})\right| \\
&= \sum_{k=1}^{n}(-1)^{k+1} \sum_{i_1,\ldots,i_k} \left|\mathcal{L}\left(mP_0 - \sum_{j=1}^{k} P_{i_j}\right)\right| \\
&\leq \sum_{k=1}^{\ell}(-1)^{k+1} \sum_{i_1,\ldots,i_k} \left|\mathcal{L}\left(mP_0 - \sum_{j=1}^{k} P_{i_j}\right)\right| \\
&= \sum_{k=1}^{\ell}(-1)^{k+1}\binom{n}{k} q^{m-k-g+1} \text{ (by Riemann–Roch Theorem).}
\end{aligned}$$

Hence, we have

$$\begin{aligned}\left|\mathcal{L}(mP_0) \setminus \bigcup_{i=1}^{n} \mathcal{L}(mP_0 - P_i)\right| &\geq q^{m-g+1} - \sum_{k=1}^{\ell} (-1)^{k+1} \binom{n}{k} q^{m-k-g+1} \\ &= q^{m-g+1}\left(1 - \frac{1}{q}\right)^n + \sum_{k=\ell+1}^{n} (-1)^{k+1} \binom{n}{k} q^{m-k-g+1} \\ &\geq q^{m-g+1}\left(1 - \frac{1}{q}\right)^n - n2^n q^{m-\ell-g} \\ &\geq q^{m-g+1}\left(1 - \frac{1}{q}\right)^n - n2^n q^{g+1}.\end{aligned}$$

Note that in the above inequalities we used the facts that $\binom{n}{k} \leq 2^n$ and $2g - 1 \leq m - \ell \leq 2g + 1$. □

Remark 2.2. If the curve $\mathcal{X}$ is explicitly given, then both $\mathcal{L}(mP_0)$ and $\mathcal{L}(mP_0 - P_i)$ can be explicitly constructed in polynomial time. Thus, the set $\mathcal{L}(mP_0) \setminus \bigcup_{i=1}^{n} \mathcal{L}(mP_0 - P_i)$ can be explicitly constructed as well.

Proof of Theorem 1.2. Let $\{\mathcal{X}\}$ be a family of curves over $\mathbb{F}_{17^2}$ that is explicitly given in [2] such that $N(\mathcal{X}) \to \infty$ and $N(\mathcal{X})/g(\mathcal{X}) \to 16$. For each curve $\mathcal{X}$ in this family, consider a code over $\mathbb{F}_{17^2} \setminus \{0\}$ defined by

$$C_{\mathcal{X}} := \left\{ (f(P_1), f(P_2), \ldots, f(P_n)) : \ f \in \mathcal{L}(mP_0) \setminus \bigcup_{i=1}^{n} \mathcal{L}(mP_0 - P_i) \right\},$$

where $n = N(\mathcal{X}) - 1$, $m = \lfloor n/3 \rfloor$ and $P_0, P_1, \ldots, P_n$ are $n + 1$ distinct $\mathbb{F}_q$-rational points on $\mathcal{X}$. Then it is easy to see that $(f(P_1), f(P_2), \ldots, f(P_n)) \neq (g(P_1), g(P_2), \ldots, g(P_n))$ for two distinct functions f, g in $\mathcal{L}(mP_0)$ since $m < n$ (see [7, 5]). Moreover, the Hamming distance of $C_{\mathcal{X}}$ is at least $n - m \geq 2n/3$.

From the previous section, we know that there is a spherical code S on the sphere $\mathcal{S}_{16}(4)$ with $|S| = 2^8 = 256$ and $d_E(S) \geq \sqrt{24}$ such that all coordinates in each codeword are equal to 1 or -1. We now add 32 points $(\pm 4, 0, \ldots, 0), (0, \pm 4, 0, \ldots, 0), \ldots, (0, \ldots, 0, \pm 4)$ on $\mathcal{S}_{16}(4)$ to the set S to get a spherical code S'. Then it is easy to see that $S' \subset \mathcal{S}_{16}(4)$, $|S'| = |S| + 32 = 17^2 - 1$ and $d_E(S') = \sqrt{24}$. Through a bijection τ from $\mathbb{F}_{17^2} \setminus \{0\}$ to S', the set $\tau(C_{\mathcal{X}})$ is a spherical code on $\mathcal{S}_{16n}(\sqrt{16n})$. Moreover, we have

$$d_E(\tau(C_{\mathcal{X}})) \geq \sqrt{24(n-m)} \geq \sqrt{16n}.$$

Hence, we have

$$K_{16n} \geq |C_{\mathcal{X}}| \geq q^{m-g+1}\left(1 - \frac{1}{q}\right)^n - n2^n q^{g+1} \tag{2.2}$$

with $q = 17^2$.

Considering the limit $\limsup_{n\to\infty} \log_2(K_{16n})/(16n)$ for K_{16n} from the inequality (2.2), we obtain the desired result. □

References

[1] J. H. Conway and N. J. A. Sloane, "Sphere Packings, Lattices and Groups", Springer-Verlag, New York, 1999 (Third Edition). MR1662447 (2000b:11077)

[2] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfel′d-Vlăduţ bound,* Invent. Math., **121** (1995), 211-222. MR1345289 (96d:11074)

[3] G. A. Kabatianskiĭ and V. I. Levenšteĭn, *Bounds for packings on the sphere and in space,* Problemy Peredachi Informatsii **14**, No. 1 (1978), 3-25. MR0514023 (58:24018)

[4] S. Ling and C. P. Xing, "Coding Theory. A First Course", Cambridge University Press, Cambridge, 2004. MR2048591 (2005c:94001)

[5] H. Niederreiter and C. P. Xing, "Rational Points on Curves over Finite Fields: Theory and Applications", London Math. Soc. Lecture Note Series **285**, Cambridge University Press, Cambridge, 2001. MR1837382 (2002h:11055)

[6] C. E. Shannon, *Probability of error for optimal codes in a Gaussian channel,* Bell System Technical Journal, **38** (1959), 611-656. MR0103137 (21:1920)

[7] M. A. Tsfasman and S. G. Vlăduţ, "Algebraic-Geometric Codes", Kluwer, Dordrecht, 1991. MR1186841 (93i:94023)

[8] A. D. Wyner, *Capabilities of bounded discrepancy decoding,* Bell System Technical Journal, **44** (1965), 1061-1122. MR0180417 (31:4652)

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore

E-mail address: xingcp@ntu.edu.sg