Bounds for spherical codes

Peter Keevash ∗ Benny Sudakov †

Abstract

A set $C$ of unit vectors in $\mathbb{R}^d$ is called an $L$-spherical code if $x \cdot y \in L$ for any distinct $x, y$ in $C$. Spherical codes have been extensively studied since their introduction in the 1970’s by Delsarte, Goethals and Seidel. In this note we prove a conjecture of Bukh on the maximum size of spherical codes. In particular, we show that for any set of $k$ fixed angles, one can choose at most $O(d^k)$ lines in $\mathbb{R}^d$ such that any pair of them forms one of these angles.

1 Introduction

A set of lines in $\mathbb{R}^d$ is called equiangular if the angles between any two of them are the same. The problem of estimating the size of the maximum family of equiangular lines has had a long history since being posed by van Lint and Seidel [9] in 1966. Soon after that, Delsarte, Goethals and Seidel [5] showed that for any set of $k$ angles, one can choose at most $O(d^{2k})$ lines in $\mathbb{R}^d$ such that every pair of them forms one of these angles. By choosing a unit direction vector on every line, the problem of lines with few angles has the following equivalent formulation. Given a set $L = \{a_1, \ldots, a_k\} \subseteq [-1,1]$, find the largest set $C$ of unit vectors in $\mathbb{R}^d$ such that $x \cdot y \in L$ for any distinct $x, y \in C$. (Here $x \cdot y = \sum_i x_i y_i$ is the standard inner product.) Hence the problem of lines with few angles is a special case of a more general question which we will discuss next.

Suppose $C$ is a set of unit vectors in $\mathbb{R}^d$ and $L \subseteq [-1,1]$. We say $C$ is an $L$-spherical code if $x \cdot y \in L$ for any distinct $x, y$ in $C$. We will prove the following theorem on the maximum size of certain spherical codes, which was conjectured by Bukh [1, Conjecture 9].

Theorem 1.1. For any $k \geq 0$ there is a function $f_k : (0,1) \to \mathbb{R}$ such that if $0 < \beta < 1$, $A \subseteq \mathbb{R}$ with $|A| = k$ and $C$ is an $L$-spherical code in $\mathbb{R}^d$ with $L = [-1,-\beta] \cup A$ then $|C| \leq f_k(\beta)d^k$.

In particular, for any set of $k$ fixed angles, one can choose at most $O(d^k)$ lines in $\mathbb{R}^d$ such that any pair of them forms one of these angles. This substantially improves the above-mentioned bound of Delsarte, Goethals and Seidel [5], in the case when the angles are fixed, i.e. do not depend on the dimension $d$. The case $k = 1$ was proved by Bukh [11] Theorem 1], who gave the first linear bound for the equiangular lines problem. One should note that the assumption that the angles are fixed is important. Otherwise, for example when $k = 1$, the linear upper bound is no longer valid, as there are constructions of quadratically many equiangular lines in $\mathbb{R}^d$ (see [4,7,8]).

∗Mathematical Institute, University of Oxford, Oxford, UK. keevash@maths.ox.ac.uk. Research supported in part by ERC Consolidator Grant 647678.
†Department of Mathematics, ETH, 8092 Zurich, Switzerland. benjamin.sudakov@math.ethz.ch. Research supported in part by SNSF grant 200021-149111.
2 Lemmas

In this section we present several lemmas which we will use in the proof of our main theorem. We start by recalling some well-known results. First we need the following bound on $L$-spherical codes, first proved in slightly stronger form by Delsarte, Goethals and Seidel [6]. At around the same time, Koornwinder [10] gave a short elegant proof using linear algebra (see also [2] Lemma 10).

Lemma 2.1. If $L \subseteq \mathbb{R}$ with $|L| = k$ and $C$ is an $L$-spherical code in $\mathbb{R}^d$ then $|C| \leq \binom{d+k}{k}$.

Next we need a well-known variant of Ramsey’s theorem, whose short proof we include for the convenience of the reader. Let $K_n$ denote the complete graph on $n$ vertices. Given an edge-colouring of $K_n$, we call an ordered pair $(X, Y)$ of disjoint subsets of vertices monochromatic if all edges in $X \cup Y$ incident to a vertex in $X$ have the same colour.

Lemma 2.2. Let $k, t, m, n$ be non-negative integers satisfying $n > k^{kt}m$ and let $f : E(K_n) \to [k]$ be an edge $k$-colouring of $K_n$. Then there is a monochromatic pair $(X, Y)$ such that $|X| = t$ and $|Y| = m$.

Proof. Consider a family of $kt$ vertices $v_1, \ldots, v_{kt}$ and sets $Y_1, \ldots, Y_{kt}$ constructed as follows. Fix $v_1$ arbitrarily and let $c(1) \in [k]$ be a majority colour among the edges $(v_1, u)$. Set $Y_1 = \{u : f(v_1, u) = c(1)\}$. By the pigeonhole principle, $|Y_1| \geq \lceil (n-1)/k \rceil \geq k^{kt-1}m$. In general, we fix any $v_{i+1}$ in $Y_i$, let $c(i + 1) \in [k]$ be a majority colour among the edges $(v_{j+1}, u)$ with $u \in Y_i$, and let $Y_{i+1} = \{u \in Y_i : f(v_{i+1}, u) = c(i + 1)\}$. Then $|Y_{i+1}| \geq \lceil |Y_i| / k \rceil \geq k^{kt-i-1}m$, and for every $1 \leq j \leq i$ the edges from $v_j$ to all vertices in $Y_{i+1}$ have colour $c(j)$. Since we have only $k$ colours, there is a colour $c \in [k]$ and $S \subseteq [kt]$ with $|S| = t$ so that $c(j) = c$ for all $j \in S$. Then $X = \{v_j : j \in S\}$ and $Y = Y_{kt}$ form a monochromatic pair of colour $c$, satisfying the assertion of the lemma. □

The following lemma is also well-known.

Lemma 2.3. If $L = [-1, -\beta]$ and $C$ is a $L$-spherical code then $|C| \leq \beta^{-1} + 1$.

Proof. Let $v = \sum_{x \in C} x$. Then, by definition of $L$-spherical code,

$$0 \leq \|v\|^2 = \sum_{x \in C} \|x\|^2 + \sum_{x \neq x' \in C} x \cdot x' \leq |C| - |C| (|C| - 1) \beta = |C| (1 - (|C| - 1) \beta).$$

Therefore $1 - (|C| - 1) \beta \geq 0$, implying $|C| \leq \beta^{-1} + 1$. □

We will also need the following simple corollary of Turán’s theorem, which can be obtained by greedily deleting vertices together with their neighbourhoods.

Lemma 2.4. Every graph on $n$ vertices with maximum degree $\Delta$ contains an independent set of size at least $\frac{n}{\Delta+1}$.

In the remainder of this section we will introduce our new tools for bounding spherical codes. Suppose $x \in \mathbb{R}^d$ and $U$ is a subspace of $\mathbb{R}^d$. We write $x_U$ for the projection of $x$ on $U$. Let $U^\perp$ be the orthogonal complement of $U$. Note that $x = x_U + x_{U^\perp}$. If $x_{U^\perp} \neq 0$ we write $p_U(x) = \|x_{U^\perp}\|^{-1} x_{U^\perp}$ for the normalized projection of $x$ on $U^\perp$. So $\|p_U(x)\| = 1$. If $U = \langle Y \rangle$ is spanned by the set of vectors $Y$ we also use $p_Y(x)$ to denote $p_U(x)$.
Lemma 2.5. Suppose \( \|x_1\| = \|x_2\| = \|y\| = 1 \) and each \( x_i \cdot y = c_i \) with \( |c_i| < 1 \). Then each \( p_y(x_i) = \frac{y - c_i y_i}{\sqrt{1 - c^2_i}} \) and \( p_y(x_1) \cdot p_y(x_2) = \frac{x_1 - x_2 - c_1 c_2}{\sqrt{(1 - c_1^2)(1 - c_2^2)}} \).

Proof. The projection of \( x_i \) on \( y \) is \( c_i y \), so the projection of \( x_i \) on \( y \) is \( x_i - c_i y \). As \( (x_i - c_i y) \cdot (x_i - c_i y) = 1 - c_i^2 \) and \( (x_1 - c_1 y) \cdot (x_2 - c_2 y) = x_1 \cdot x_2 - c_1 c_2 \) the lemma follows.

Given a subspace \( U \) we can calculate \( p_U(x) \) using the following version of the Gram-Schmidt algorithm. Suppose that \( \{y_1, \ldots, y_k\} \) is a basis for \( U \). Write \( y_{k+1} = x \). Define vectors \( y_j^i \) by \( y_j^0 = y_j \) for \( j \in [k + 1] \) and \( y_j^i = p_{y_{i-1}}(y_j^{i-1}) \) for \( 1 \leq i < j \leq k + 1 \). It is easy to check by induction that for every \( j \) the vectors \( y_1^0, y_1^1, \ldots, y_j^{j-1} \) are orthogonal. Also \( y_j^{j-1} \) is a unit vector for \( j > 1 \). Therefore \( p_U(x) = y_{k+1}^k \).

Lemma 2.6. Suppose \( X \cup Y \) is a set of unit vectors in \( \mathbb{R}^d \) such that \( x \cdot y = y \cdot y' = c \) with \( |c| < 1 \) for all \( x \in X \) and distinct \( y, y' \) in \( Y \). Let \( U = \langle Y \rangle \) and \( k = |Y| \). Then for any \( x, x' \) in \( X \) we have \( p_U(x) \cdot p_U(x') = g_k(x \cdot x') \), where

\[
g_k(a) := 1 - (1-c)^{-1}(1-(c^{-1}+k)^{-1})(1-a) = (1-c)^{-1}[a-c+(c^{-1}+k)^{-1}(1-a)].
\]

Remark. Note that \( g_0(a) = a \), \( g_k(c) = (c^{-1}+k)^{-1} \) and \( g_k(a) \) is decreasing in \( k \). Also \( g_k \to \frac{c^2}{1-c} \) when \( k \) tends to infinity.

Proof. We write \( Y = \{y_1, \ldots, y_k\} \), \( y_{k+1} = x \), \( y_{k+2} = x' \) and calculate \( p_U(x) = y_{k+1}^k \) and \( p_U(x') = y_{k+2}^k \) using the algorithm and notation introduced before the lemma. It is easy to see that vectors in \( Y \) are linearly independent, since the matrix of pairwise inner products of these vectors has full rank. Let \( c_i^{-1} = i + c^{-1} \). We show by induction for \( 0 \leq i \leq k \) that \( y_{j}^i \cdot y_{j'}^i = c_i \) for all distinct \( j, j' > i \), with the possible exception of \( \{j, j'\} = \{k + 1, k + 2\} \). Indeed, this holds by hypothesis when \( i = 0 \). When \( 0 < i \leq k \), by induction \( y_{i-1}^i \cdot y_{i-1}^i = y_{i-1}^i \cdot y_{i-1}^i = c_{i-1} \). Therefore by Lemma 2.5

\[
y_{j}^i \cdot y_{j'}^i = p_{y_{i-1}}((y_{j}^{i-1} \cdot y_{j'}^{i-1}) \cdot p_{y_{i-1}}(y_{j}^{i-1})) = (1-c_{i-1}^2)^{-1}(y_{j}^{i-1} \cdot y_{j'}^{i-1} - c_{i-1}^2) \quad (1)
\]

If \( \{j, j'\} \neq \{k + 1, k + 2\} \), then \( y_{j}^i \cdot y_{j'}^i = c_{i-1} \) as well. The induction step follows, as

\[
(y_{j}^{i-1} \cdot y_{j'}^{i-1})^{-1} = (1-c_{i-1}^2)(c_{i-1} - c_{i-1}^2)^{-1} = 1 + c_{i-1}^{-1} = i + c^{-1} = c_{i}^{-1}.
\]

Writing \( r_i = y_{k+1}^i \cdot y_{k+2}^i - 1 \) we have \( r_{i+1} = (1-c_i^2)^{-1}r_i \) by (1), so

\[
p_U(x) \cdot p_U(x') = 1 + r_k = 1 - \lambda(1-x \cdot x'),
\]

where \( \lambda = \prod_{i=0}^{k-1}(1-c_i^2)^{-1} \). To compute \( \lambda \) consider the case \( x \cdot x' = c \). Then by the above discussion \( 1 - \lambda(1-c) = p_U(x) \cdot p_U(x') = c_k = (c^{-1}+k)^{-1} \), so \( \lambda = (1-c)^{-1}(1-(c^{-1}+k)^{-1}) \). □
3 Proof of the main result

In this section we prove Theorem 1.1. We argue by induction on \(k\). The base case is \(k = 0\), when \(L = [-1, -\beta]\), and we can take \(f_0(\beta) = \beta^{-1} + 1\) by Lemma 2.3. Henceforth we suppose \(k > 0\). We can assume \(d \geq d_0 = (2k)^{2k\beta^{-1}}\). Indeed, if we can prove the theorem under this assumption, then for \(d < d_0\) we can use the upper bound for \(\mathbb{R}^{d_0}\) (since it contains \(\mathbb{R}^d\)). Then we can deduce the bound for the general case by multiplying \(f_k(\beta)\) (obtained for the case \(d \geq d_0\)) by a factor \(d_0^2 = (2k)^{2k\beta^{-1}}\).

Suppose \(C = \{x_1, \ldots, x_n\}\) is an \(L\)-spherical code in \(\mathbb{R}^d\), where \(L = [-1, -\beta] \cup \{a_1, \ldots, a_k\}\), with \(a_1 < \cdots < a_k\). We define graphs \(G_0, \ldots, G_k\) on \([n]\) where \((i, j) \in G_\ell \iff x_i \cdot x_j = a_\ell\) for \(\ell \in [k]\) and \((i, j) \in G_0 \iff x_i \cdot x_j \in [-1, -\beta]\).

Consider the case \(a_k < \beta^2/2\). We claim that \(G_0\) has maximum degree \(\Delta \leq 2\beta^{-2} + 1\). Indeed, consider \(y \in [n]\) and \(J \subseteq [n]\) such that \((y, j) \in G_0\) for all \(j \in J\). For any \(j, j'\) in \(J\) we have \(x_y \cdot x_j, x_y \cdot x_{j'} \leq -\beta\). Hence, by Lemma 2.3 we have

\[
p_{x_y}(x_j) \cdot p_{x_y}(x_{j'}) = \frac{x_j \cdot x_{j'} - (x_y \cdot x_j)(x_y \cdot x_{j'})}{1 - (x_y \cdot x_j)^2} \leq \frac{a_k - \beta^2}{1 - (x_y \cdot x_{j'})^2} < -\beta^2/2.
\]

Thus \(|J| \leq 2\beta^{-2} + 1\) by Lemma 2.3 as claimed. By Lemma 2.4 \(G_0\) has an independent set \(S\) of size \(n/(2\beta^{-2} + 2)\). Then \(\{x_j : j \in S\}\) is an \(\{a_1, \ldots, a_k\}\)-spherical code, so \(|S| \leq d_k + 1 \leq 2d_k\) by Lemma 2.1. Choosing \(f_k(\beta) > 4\beta^{-2} + 4\), we see that the theorem holds in this case. Henceforth we suppose \(a_k \geq \beta^2/2\).

Next consider the case that there is \(\ell \geq 2\) such that \(a_{\ell-1} < a_{\ell}^2/2\). Choosing the maximum such \(\ell\) we have

\[
a_{\ell-1}^2/2 = 2(a_{\ell-1}/2)^2 \geq 2(a_{\ell}/2)^2 \geq \ldots \geq 2(a_k/2)^{2k-\ell+1} \geq \beta' := (\beta/2)^{2k}.
\]

Note that by induction \(\cup_{i=0}^{\ell-1} G_i\) contains no clique of order \(f_{\ell-1}(\beta)d^{\ell-1}\), so by Lemma 2.4 its complement has maximum degree at least \(n' = n/(2f_{\ell-1}(\beta)d^{\ell-1})\). Consider \(y \in [n]\) and \(J \subseteq [n]\) with \(|J| = n'\) such that \((y, j) \notin \cup_{i=0}^{\ell-1} G_i\) for all \(j \in J\). By the pigeonhole principle, there is a subset \(J' \subseteq J\) and an index \(\ell \leq s \leq k\) such that \((y, j) \in G_s\) for all \(j \in J'\).

For any \((j, j') \in \cup_{i=0}^{s-1} G_i [J']\), by Lemma 2.3 we have

\[
p_{x_y}(x_j) \cdot p_{x_y}(x_{j'}) = \frac{x_j \cdot x_{j'} - a_s^2}{1 - a_s^2} \leq a_s^2/2 - a_s^2 < -a_s^2/2 \leq -\beta'.
\]

Now \(\{x_y(x_j) : j \in J'\}\) is an \(L'\)-spherical code, where \(L' = [-1, -\beta'] \cup \{a_\ell', \ldots, a_k'\}\), with \(a_i' = a_i - a_s^2\) for \(i \geq \ell\). By induction hypothesis, we have \(|J'| \leq f_{k-\ell+1}(\beta')d^{k-\ell+1}\), so choosing \(f_k(\beta) > 2k f_{\ell-1}(\beta) f_{k-\ell+1}(\beta')\) the theorem holds in this case.

Now suppose that there is no \(\ell > 1\) such that \(a_{\ell-1} < a_{\ell}^2/2\). We must have \(a_1 > 0\). Let \(t = 1/\beta'\). We apply Lemma 2.2 to find an index \(r\) and a disjoint pair of sets \((T, M)\) with \(|T| = t\) and \(|M| = m \geq (k + 1)^{-(k+1)t}n\), such that all vertices in \(T\) are adjacent to each other and to all vertices in \(M\) by edges of \(G_r\). Note that \(r > 0\), as \(G_0\) has no clique of size \(t\) by Lemma 2.3. For \(j \in M\) we write \(x_j' = x_j \cdot y\). By Lemma 2.6 for any \((j, j') \in G_i [M]\) with \(i \geq 1\) we have \(x_j' \cdot x_{j'} = a_i' := g_i^{ar}(a_i)\). Also, if \((j, j') \in G_0 [N]\) we have \(x_j' \cdot x_{j'} = g_i^{ar}(x_j \cdot x_{j'}) \leq g_i^{ar}(-\beta) \leq -\beta\). Thus \(\{x_j' : j \in M\}\) is an \(L'\)-spherical code in \(\mathbb{R}^{d-t}\), where \(L' = [-1, -\beta] \cup \{a_1', \ldots, a_k'\}\).
We can assume $a'_k \geq \beta^2/2$, otherwise choosing $f_k(\beta) > (k+1)^{(k+1)t}(4\beta^{-2} + 4)$ we are done by the first case considered above. Since $a'_r = (a_{r-1} + t)^{-1} < \beta'$, the computation in (2) implies that there is $\ell > 1$ such that $a_{\ell-1} < a_{\ell}/2$. Choosing $f_k(\beta) > (k+1)^{(k+1)t}2k f_{\ell-1}(\beta) f_{k-\ell+1}(\beta')$ we are done by the second case considered above. □

4 Concluding remarks

One can use our proof to derive an explicit bound for $f_k(\beta)$. Indeed, it can be easily shown that it is enough to take $f_k(\beta)$ to be $2^{\beta-o(k^2)}$. We omit the details, as we believe that this bound is very far from optimal. Moreover, one cannot expect a bound better than exponential in $\beta^{-1}$ using our methods or those of Bukh [1]. On the other hand, we do not know any example ruling out the possibility that $f_k(\beta)$ could be independent of $\beta$ if $k > 0$ and $A$ is fixed (Bukh [1] also makes this remark for $k = 1$). One place to look for an improvement is in the application of Ramsey’s theorem, as one would expect much better bounds for Ramsey-type questions for graphs defined by geometric constraints (see [3] and its references for examples of this phenomenon).

References

[1] B. Bukh, Bounds on equiangular lines and on related spherical codes, preprint, arXiv:1508.00136.
[2] B. Bukh, Ranks of matrices with few distinct entries, preprint, arXiv:1508.00145.
[3] D. Conlon, J. Fox, J. Pach, B. Sudakov and A. Suk, Ramsey-type results for semi-algebraic relations, *Transactions Amer. Math. Soc.* 366 (2014), 5043–5065.
[4] D. de Caen, Large equiangular sets of lines in Euclidean space, *Electronic J. Combin.* 7 (2000), Paper 55.
[5] P. Delsarte, J. Goethals and J. Seidel, Bounds for systems of lines, and Jacobi polynomials, *Philips Research Reports* 30 (1975), 91–105.
[6] P. Delsarte, J. Goethals and J. Seidel, Spherical codes and designs, *Geometriae Dedicata* 6 (1977), 363–388.
[7] G. Greaves, J. Koolen, A. Munemasa and F. Szöllősi, Equiangular lines in Euclidean spaces, preprint, arXiv:1403.2155.
[8] J. Jedwab and A. Wiebe, Large sets of complex and real equiangular lines, *J. Combin. Theory A* 134 (2015), 98–102.
[9] J. H. van Lint and J. J. Seidel, Equilateral point sets in elliptic geometry, *Nederl. Akad. Wetensch. Proc. Ser. A* 69=Indag. Math. 28 (1966), 335–348.
[10] T. Koornwinder, A note on the absolute bound for systems of lines, *Nederl. Akad. Wetensch. Proc. Ser. A* 79=Indag. Math. 38 (1976), 152–153.