Bounds on equiangular lines and on related spherical codes

Boris Bukh*

Abstract

An $L$-spherical code is a set of Euclidean unit vectors whose pairwise inner products belong to the set $L$. We show, for a fixed $\alpha, \beta > 0$, that the size of any $[-1, -\beta] \cup \{\alpha\}$-spherical code is at most linear in the dimension.

In particular, this bound applies to sets of lines such that every two are at a fixed angle to each other.

1 Introduction

Background A set of lines in $\mathbb{R}^d$ is called equiangular, if the angle between any two of them is the same. Equivalently, if $P$ is the set of unit direction vectors, the corresponding lines are equiangular with the angle $\arccos \alpha$ if $\langle v, v' \rangle \in \{-\alpha, \alpha\}$ for any two distinct vectors $v, v' \in P$. The second equivalent way of defining equiangular lines is via the Gram matrix. Let $M$ be the matrix whose columns are the direction vectors. Then $M^TM$ is a positive semidefinite matrix whose diagonal entries are 1’s, and each of whose off-diagonal entries is $-\alpha$ or $\alpha$. Conversely, any such matrix of size $m$ and rank $d$ gives rise to $m$ equiangular lines in $\mathbb{R}^d$.

The equiangular lines have been extensively studied following the works of van Lint and Seidel [9], and of Lemmens and Seidel [7]. Let $N(d)$ be the maximum number of equiangular lines in $\mathbb{R}^d$. Let $N_\alpha$ be the maximum number of equiangular lines with the angle $\arccos \alpha$. The values of $N(d)$ are known exactly for $d \leq 13$, for $d = 15$, for $21 \leq d \leq 41$ and for $d = 43$ [1, 5]. When $d$ is large, the only known upper bound on $N(d)$ is due to Gerzon (see [7, Theorem 3.5]) and asserts that

$$N(d) \leq d(d + 1)/2$$

with equality only if $d = 2, 3$ or $d + 2$ is a square of an odd integer.

A remarkable construction of de Caen[3] shows that $N(d) \geq \frac{2}{d}(d + 1)^2$ for $d$ of the form $d = 6 \cdot 4^i - 1$. A version of de Caen’s construction suitable for other values of $d$ has been given by Greaves, Koolen, Munemasa and Szöllősi [5]. See also the work of Jedwab and Wiebe [6] for an alternative construction of $\Theta(d^2)$ equiangular lines. In these constructions the inner product $\alpha$ tends to 0 as dimension grows.

Previously known bounds on $N_\alpha(d)$ The first bound is the so-called relative bound (see [9, Lemma 6.1] following [7, Theorem 3.6])

$$N_\alpha(d) \leq d \frac{1 - \alpha^2}{1 - r\alpha^2}$$

if $d < 1/\alpha^2$.

*Supported in part by U.S. taxpayers through NSF grant DMS-1301548.
While useful in small dimensions, it gives no information for a fixed $\alpha$ and large $d$. The second bound is
\[ N_\alpha(d) \leq 2d \] unless $1/\alpha$ is an odd integer [7, Theorem 3.4].
This bound can be further improved to $\frac{3}{2}(d+1)$ unless $\frac{1}{2\alpha} + \frac{1}{2}$ is an algebraic integer of degree 2, see [2, Subsection 2.3].
Finally, the values of $N_{1/3}(d)$ and $N_{1/5}(d)$ for a large $d$ have been completely determined:
\[ N_{1/3}(d) = 2d - 2 \quad \text{for } d \geq 15 \quad [7, \text{Theorem } 4.5], \]
\[ N_{1/5}(d) = \lfloor 3(d-1)/2 \rfloor \quad \text{for all sufficiently large } d \quad [8] \text{ and } [5, \text{Corollary } 6.6]. \]

New bound We will show that $N_\alpha(d)$ is linear for every $\alpha$. In fact, we will prove a result in greater generality. Following [4], we call a set of unit vectors $P$ an $L$-spherical code if $\langle v, v' \rangle \in L$ for every pair of distinct points $v, v' \in P$. In this language, a set of equiangular lines is a $\{-\alpha, \alpha\}$-spherical code. Let $N_L(d)$ be the maximum cardinality of an $L$-spherical code in $\mathbb{R}^d$.

**Theorem 1.** For every fixed $\beta > 0$ there exists a constant $c_\beta$ such that for any $L$ of the form $L = [-1, -\beta] \cup \{\alpha\}$ we have $N_L(d) \leq c_\beta d$.

We make no effort to optimize the constant $c_\beta$ that arises from our proof, as it is huge. We speculate about the optimal bounds on $N_L(d)$ in section 3. We do not know if the constant $c_\beta$ must in fact depend on $\beta$.

The rest of the paper is organized as follows. In the next section we prove Theorem 1 and in the concluding section we discuss possible generalizations and strengthenings of Theorem 1.

## 2 Proof of Theorem 1

Proof sketch The idea behind the proof of Theorem 1 builds upon the argument of Lemmens and Seidel for $N_{1/3}(d)$. Before going into the details, we outline the argument.

Let $L = [-1, -\beta] \cup \{\alpha\}$, and let $P$ be an $L$-spherical code whose size we wish to bound. Define a graph $G$ on the vertex set $P$ by connecting $v$ and $v'$ by an edge if $\langle v, v' \rangle \in [-1, -\beta]$. In their treatment of $N_{1/3}(d)$ Lemmens and Seidel consider the largest clique in $G$, and carefully analyze how the rest of the graph attaches to that clique. In contrast, in our argument we consider the largest independent set $I$ of $G$, and show that almost every other vertex is incident to nearly all vertices of $I$. Iterating this argument inside the common neighborhood of $I$ we can build a large clique in $G$. As the clique size is bounded by a function of $\beta$, that establishes the theorem.

Proof details For the remainder of the section, $L$, $P$ and $G$ will be as defined as in the preceding proof sketch. The following two well-known lemmas bound the sizes of cliques and independent sets in $G$:

**Lemma 2.** Suppose $u_1, \ldots, u_n$ are $n$ vectors of norm at most 1 satisfying $\langle u_i, u_j \rangle \leq -\gamma$. Then $n \leq 1/\gamma + 1$.

*Proof.* This follows from $0 \leq \| \sum u_i \|^2 = \sum_{i,j} \langle u_i, u_j \rangle \leq n - \gamma n(n-1)$. \qed
Lemma 3.

i. Every independent set in $G$ is linearly independent. In particular, the graph $G$ contains no independent set on more than $d$ vertices.

ii. The graph $G$ contains no clique on more than $1/\beta + 1$ vertices.

Proof. i) Let $p_1, \ldots, p_n$ be the points of the independent set. Suppose that $\sum c_i p_i = 0$. Taking an inner product with $p_j$ we obtain $0 = (1 - \alpha)c_j + \alpha \sum c_i$ implying that all $c_i$’s are equal. The result follows since $(1 - \alpha) + n\alpha \neq 0$.

ii) This is a special case of the preceding lemma. \hfill \Box

In the next two lemmas we analyze how the vertices of $G$ attach to an independent set.

Lemma 4. Suppose that $M$ is a matrix with linearly independent column vectors $p_1, \ldots, p_n$. Suppose that $v, v' \in \text{span}\{p_1, \ldots, p_n\}$ are points satisfying $\langle p_i, v \rangle = s_i$ and $\langle p_i, v' \rangle = s'_i$ for some column vectors $s = (s_1, \ldots, s_n)^T$ and $s' = (s'_1, \ldots, s'_n)^T$. Then $\langle v, v' \rangle = s^T(M^TM)^{-1}s'$.

Proof. By passing to a subspace we may assume that $p_1, \ldots, p_n$, span $\mathbb{R}^n$, and so $M$ is invertible. As $s = M^Tv$ and $s' = M^Tv'$, we infer that $\langle v, v' \rangle = v^T v' = ((M^TM)^{-1}s)^T(M^TM)^{-1}s' = s^T(M^TM)^{-1}s'$. \hfill \Box

The following lemma is the geometric heart of the proof. In its special case $v = v'$, the lemma bounds degrees from certain vertices into an independent set. More precisely, let $I$ be a sufficiently large independent set. We will show later (in Lemma 6) that the vertices, the norm of whose projection on $\text{span } I$ exceeds $\alpha^{1/2}$, are few. The straightforward, but slightly messy calculations in the following lemma characterize the vertices with such projections in terms of their degree into $I$. The case $v \neq v'$ is not needed when $P$ comes from the set of equiangular lines, but is required to establish Theorem 1 in its full generality.

Lemma 5. Let $t = 1/\beta + 1$. There exists $n_0 = n_0(\beta)$ and $\varepsilon = \varepsilon(\beta)$ such that the following holds. Suppose that $p_1, \ldots, p_n$ is an independent set in $G$ of size $n$, and suppose that a points $p, p' \in P$ are adjacent to the same $m$ vertices among $p_1, \ldots, p_n$. Assume $0 < m < n - t$ and $n \geq n_0$. Write $p = v + u$ and $p' = v' + u'$ where $v, v' \in \text{span}\{p_1, \ldots, p_n\}$ and $u, u'$ are both orthogonal to $\text{span}\{p_1, \ldots, p_n\}$. Then $\langle v, v' \rangle \geq \alpha + \varepsilon$.

Proof. Since points $p_1, \ldots, p_n$ are linearly independent (by Lemma 3), the condition of the preceding lemma is fulfilled. We have $M^TM = \alpha J + (1 - \alpha)I$. One can verify that its inverse is given by

$$
(1 - \alpha)(M^TM)^{-1} = I - \phi J \quad \text{with} \quad \phi \overset{\text{def}}{=} \frac{\alpha}{1 + (n - 1)\alpha}. \quad (1)
$$

Note that $\phi \leq 1/n$ since $\alpha \leq 1$.

Without loss of generality, $p_1, \ldots, p_m$ are the $m$ vertices that $p$ and $p'$ are adjacent to. This means that $s \overset{\text{def}}{=} M^Tv$ and $s' \overset{\text{def}}{=} M^Tv'$ are of the form $s = (-\beta_1, \ldots, -\beta_m, \alpha, \ldots, \alpha)$ and $s' = (-\beta'_1, \ldots, -\beta'_m, \alpha, \ldots, \alpha)$ for some $\beta_1, \beta'_1, \ldots, \beta_m, \beta'_m \in [\beta, 1]$. From Lemma 4 and (1) it follows that

$$
(1 - \alpha)\langle v, v' \rangle = \alpha^2(n - m) + \sum \beta_i \beta'_i - \phi(\sum \beta)(\sum \beta''). \quad (2)
$$
We claim that, subject to the constraint $\beta_1, \beta_1', \ldots, \beta_m, \beta_m' \in [\beta, 1]$, the right side of (2) is minimized when all the $\beta_i$’s and all the $\beta_i'$’s are equal to $\beta$. Indeed, since $[\beta, 1]^{2m}$ is compact, the minimum is actually attained. Assume that $(\beta_1, \beta_1', \ldots, \beta_m, \beta_m')$ is the vector achieving the minimum, and let $j$ be the index for which $\beta_j'$ is the largest. Then the derivative of the right side of (2) with respect to $\beta_j'$ is $\beta_j' - \phi \sum \beta_i \geq \beta_j' - \frac{1}{n} \sum \beta_i > \beta_j - \frac{1}{m} \sum \beta_i \geq 0$. By the optimality assumption this implies that $\beta_j' = \beta$, and so $\beta_i' = \beta$ for all $i$. Similarly, $\beta_i = \beta$ for all $i$.

We thus deduce that

$$(1 - \alpha)\langle v, v' \rangle \geq \alpha^2(n - m) + \beta^2m - \phi((n - m)\alpha - \beta^2).$$

Let $R(m, n)$ denote the right side of preceding inequality. Let $t^* \defeq \frac{(1 - \alpha)(\alpha - \beta)}{\alpha + \beta}$. We have

$$t^* = \frac{(1 - \alpha)(\alpha - \beta)}{\alpha + \beta} < \frac{1 - \alpha}{\alpha + \beta} < \frac{1}{\beta} = t - 1.$$  

Thus to prove the lemma, it is enough to show that $R(m, n) \geq (1 - \alpha)\alpha + \varepsilon$ whenever $1 \leq m \leq n - t^* - 1$ and $n \geq n_0$ for suitable $n_0$ and $\varepsilon$.

The expression $R(m, n)$ is a quadratic polynomial in $m$. A simple calculation shows that it satisfies $R(m, n) = R(n - t^* - m, n)$, and in particular that the maximum of $R(m, n)$ for a fixed $n$ is at the point $m_{\text{max}} \defeq (n - t^*)/2$, which is inside the interval $[1, n - t^* - 1]$. Furthermore, at the boundary points of the interval we have

$$R(1, n) = R(n - t^* - 1, n) = \alpha(1 - \alpha) + (\alpha + \beta)^2 - \frac{\alpha(1 + \beta)^2}{1 + \alpha(n - 1)}.$$  

Let $n_0 = 1 + 8/\beta^2$. Since $\frac{\alpha(1 + \beta)^2}{1 + \alpha(n - 1)} < \frac{4}{n - 1}$, it follows that $R(m, n) \geq R(1, n) > \alpha(1 - \alpha) + \frac{1}{2}(\alpha + \beta)^2$ whenever $1 \leq m \leq n - t^* - 1$ and $n \geq n_0$. In particular $\langle v, v' \rangle > \alpha + \varepsilon$ holds under the same conditions, where $\varepsilon = \frac{1}{2}\beta^2$.

\[ \square \]

**Lemma 6.** Suppose $p_1, \ldots, p_n$ is an independent set in $G$. Suppose $p^{(1)}, \ldots, p^{(m)} \in P$ are points of the form $p^{(i)} = v^{(i)} + u^{(i)}$ with $v^{(i)} \in \text{span}\{p_1, \ldots, p_n\}$ and $u^{(i)} \perp \text{span}\{p_1, \ldots, p_n\}$ and $\langle v^{(i)}, v^{(j)} \rangle > \alpha + \varepsilon$ for all $i, j$. Then $m \leq 1/\varepsilon + 1$.

**Proof.** From $\langle p^{(i)}, p^{(j)} \rangle = \langle v^{(i)}, v^{(j)} \rangle + \langle u^{(i)}, u^{(j)} \rangle$ and $\langle p^{(i)}, p^{(j)} \rangle \in [-1, -\beta] \cup \{\alpha\}$, we deduce that $\langle u^{(i)}, u^{(j)} \rangle < -\varepsilon$. The result then follows from Lemma 2. \[ \square \]

The combinatorial part of the argument is contained in the next result.

**Lemma 7.** Suppose $\delta > 0$ is given. Then there exists $M(\beta, \delta)$ such that the following holds. Let $U \subset P$ be arbitrary. Suppose $I$ is a maximum-size independent subset of $U$. Then there is a subset $U' \subset U \setminus I$ of size $|U'| \geq |U| - M|I|$ such that every vertex of $U'$ is adjacent to at least $(1 - \delta)|I|$ vertices of $I$.

**Proof.** Let $t, \varepsilon$ and $n_0$ be as in Lemma 5, and put $n = \max(n_0, [1/\delta])$. Denote by $R$ the least integer such that every graph on $R$ vertices contains either an independent set of size $n + 1$ or a clique of size at least $1/\beta + 2$ (such an $R$ exists by Ramsey’s theorem). Let

$$M = \max(R, (1/\varepsilon + 1)2^n),$$  

$$N = |I|.$$  

4
If $|U| < M$, then $|U| - M|I|$ is negative, and the lemma is vacuous. So, assume $|U| \geq M$. In particular, $|U| \geq R$, and since by Lemma 3 the set $U$ contains no clique of size greater $1/\beta + 1$, we conclude that $N \geq n + 1$.

Arrange the elements of $I$ on a circle, and consider all $N$ circular intervals containing $n$ vertices of $I$. Let $S_1, S_2, \ldots, S_N$ be these intervals, in order.

We declare a vertex $p \in U \setminus I$ to be $i$-bad if it is adjacent to between $1$ and $n - t^*$ vertices of $S_i$. For a set $T \subset S_i$, we call an $i$-bad vertex $p$ to be of type $T$ if $T$ is precisely the set of neighbors of $p$ in the set $S_i$. Let $B_{i,T}$ be the set of all $i$-bad vertices of type $T$, and let $B_i = \bigcup_T B_{i,T}$ be the set of all $i$-bad vertices. By Lemmas 5 and 6 we have $|B_{i,T}| \leq 1/v + 1$ for every $T$, and so

$$|B_i| \leq (1/v + 1)(2^n - 1).$$

Let $B = \bigcup B_i$ be the set of bad vertices. Hence, $|B| \leq N(1/v + 1)(2^n - 1)$, and $|B \cup I| \leq MN$.

Consider a vertex $p \in U \setminus I$ that is good, i.e., $p \notin B$. Since $I$ is a maximal independent set, $p$ is adjacent to at least one vertex of $I$. Say $p$ is adjacent to a vertex of $S_i$ for some $i$. Since $p$ is good, $p$ must in fact be adjacent to at least $n - t$ vertices of $S_i$. As $S_i$ shares $n - 1$ vertices with both $S_{i-1}$ and $S_{i+1}$, we are impelled to conclude that $p$ must be adjacent to some of the vertices of $S_{i-1}$ and of $S_{i+1}$. Repeating this argument we conclude that $p$ is non-adjacent to at most $t$ elements from among any interval of length $n$. In particular, $p$ is adjacent to at least $N(1 - t/n)$ vertices of $I$. As $p$ is an arbitrary good vertex and $t/n \leq \delta$, the lemma follows.

We are now ready to complete the proof of Theorem 1. Indeed, with foresight we set

$$B = [1/\beta + 1],$$

$$\delta = 1/(B + 1)^2.$$

and let $M$ be as in the proceeding lemma. Put $U_0 = P$ and let $I_0$ be a maximal independent set in $U_0$. By the preceding lemma, there exists $U_1 \subset U_0 \setminus I_0$ such that every vertex of $U_1$ is adjacent to $(1 - \delta)|I_0|$ vertices of $I_0$ and $|U_1| \geq |U_0| - M|I_0|$. In view of Lemma 3, $|U_1| \geq |U_0| - Md$. Let $I_1$ be a maximal independent set in $U_1$. Repeating this argument, we obtain a nested sequence of sets $U_0 \supset U_1 \supset \ldots$ and a corresponding sequence of independent sets $I_0, I_1, \ldots$ such that

i. $|U_i| \geq |U_{i-1}| - Md$ for each $i = 1, 2, \ldots$,

ii. For $r < s$, each vertex in $I_s$ is adjacent to at least $(1 - \delta)|I_r|$ vertices of $I_r$.

We claim that $|P| \leq BMd$, which would be enough to complete the proof of Theorem 1. Indeed, suppose for the sake of contradiction that $|P| > BMd$. Then $I_0, \ldots, I_B$ are non-empty. Pick vertices $v_0, \ldots, v_B$ uniformly at random from $I_0, \ldots, I_B$ respectively. Since, for every $i \neq j$, the pair $v_i, v_j$ is an edge with probability at least $1 - \delta$, it follows that $v_0, \ldots, v_B$ is a clique with probability at least $1 - (B+1)/2 \delta > 0$. In particular, $G$ then contains a clique of size $B + 1 > \beta/2 + 1$, contrary to Lemma 3. The contradiction shows that $|P| \leq BMd$, completing the proof of Theorem 1.
3 Open problems

- I know of only one asymptotic lower bound on $N_L$. It is a version of [5, Proposition 5.12] that is also implicit in the bound for $N_{1/2}(d)$ in [7]. Denote by $I_n$ the identity matrix of size $n$, and by $J_n$ the all-one matrix of size $n$. Then the matrix $M = (r - 1)I_{rt} - (J_r - I_r) \otimes I_t$ is a positive semidefinite matrix of nullity $t$, it has $(r - 1)$’s on the diagonal, and its off-diagonal entries are 0 and $-1$. Hence, $\frac{1}{r-1+\tau}(M + \tau J_{rt})$ is a Gram matrix of a $\{-\frac{1-\tau}{r-1+\tau}, \frac{\tau}{r-1+\tau}\}$-code in $\mathbb{R}^{(r-1)t+1}$ of size $rt$. So, $N_L(d) \geq \frac{r}{r-1}d + O(1)$ for $L = \{-\frac{1-\tau}{r-1+\tau}, \frac{\tau}{r-1+\tau}\}$. For $\tau = 1/2$, this yields a family of equiangular lines. The results in [7, 8, 5] suggest that this bound is sharp.

Conjecture 8. The number of equiangular lines with a given angle is $N_{1/(2r-1)}(d) = \frac{r}{r-1}d + O(1)$ as $d$ tends to infinity.

In contrast, one can show that the bound implicit in the proof of Theorem 1 is $2^{O(1/\beta^2)}d$.

- Informally, it is natural to think of Theorem 1 as a juxtaposition of two trivial results from Lemma 3: $N_{[-1,-\beta]}(d) = O(1)$ and $N_{\{\alpha\}}(d) = O(d)$. Since $N_{\{\alpha_1,\ldots,\alpha_k\}}(d) = O(d^k)$ for any real numbers $\alpha_1,\ldots,\alpha_k$ (see [2, Proposition 1]) this motivates the following conjecture.

Conjecture 9. Suppose $\alpha_1,\ldots,\alpha_k$ are any $k$ real numbers, and $L = [-1,-\beta] \cup \{\alpha_1,\ldots,\alpha_k\}$. Then $N_L(d) \leq c_{\beta,k}d^k$.

It is conceivable that in this case even $N_L(d) \leq c_{\beta}N_{\{\alpha_1,\ldots,\alpha_k\}}(d)$ might be true.

- I cannot rule out the possibility that for a fixed $\alpha$ the size of any $[-1,0] \cup \{\alpha\}$-code is at most linear in the dimension.

Acknowledgments. I am grateful to James Cummings, Hao Huang and Humberto Naves for inspirational discussions. I am thankful to Joseph Briggs for careful reading, and for finding a mistake in an earlier version of this paper.

References

[1] Alexander Barg and Wei-Hsuan Yu. New bounds for equiangular lines. In Discrete geometry and algebraic combinatorics, volume 625 of Contemp. Math., pages 111–121. Amer. Math. Soc., Providence, RI, 2014. arXiv:1311.3219.

[2] Boris Bukh. Ranks of matrices with few distinct entries. arXiv:1508.00145, 2015.

[3] D. de Caen. Large equiangular sets of lines in Euclidean space. Electron. J. Combin., 7:Research Paper 55, 3 pp. (electronic), 2000. http://www.combinatorics.org/Volume_7/Abstracts/v7i1r55.html.

[4] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. Geometriae Dedicata, 6(3):363–388, 1977.
[5] Gary Greaves, Jacobus H. Koolen, Akihiro Munemasa, and Ferenc Szöllösi. Equiangular lines in Euclidean spaces. arXiv:1403.2155, January 2015.

[6] Jonathan Jedwab and Amy Wiebe. Large sets of complex and real equiangular lines. J. Combin. Theory Ser. A, 134:98–102, 2015. arXiv:1501.05395.

[7] P. W. H. Lemmens and J. J. Seidel. Equiangular lines. J. Algebra, 24:494–512, 1973.

[8] A. Neumaier. Graph representations, two-distance sets, and equiangular lines. Linear Algebra Appl., 114/115:141–156, 1989.

[9] J. H. van Lint and J. J. Seidel. Equilateral point sets in elliptic geometry. Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math., 28:335–348, 1966.