Complex Lines with Restricted Angles

Aidan Roy   Chris Godsil

Department of Combinatorics and Optimization
University of Waterloo

Ontario Combinatorics Workshop, 2005

The basic problem

For fixed angles A, find a maximal set of vectors in $\mathbb{C}^n$ such that

$$|\langle u, v\rangle| \in A.$$

- well-studied in $\Re^n$
- applications to communications sequences, quantum computing

Equiangular lines

Equiangular lines: Vectors $v_1, \ldots, v_l$ in $\mathbb{C}^n$ such that

$$\left|\langle v_i, v_j \rangle\right| = \begin{cases} 1, & i = j; \\ \alpha, & \text{otherwise.} \end{cases}$$

In $\mathbb{C}^2$ (with $\omega^3 = 1$):

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2}\omega \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2}\omega^2 \end{pmatrix}$$

Equiangular lines

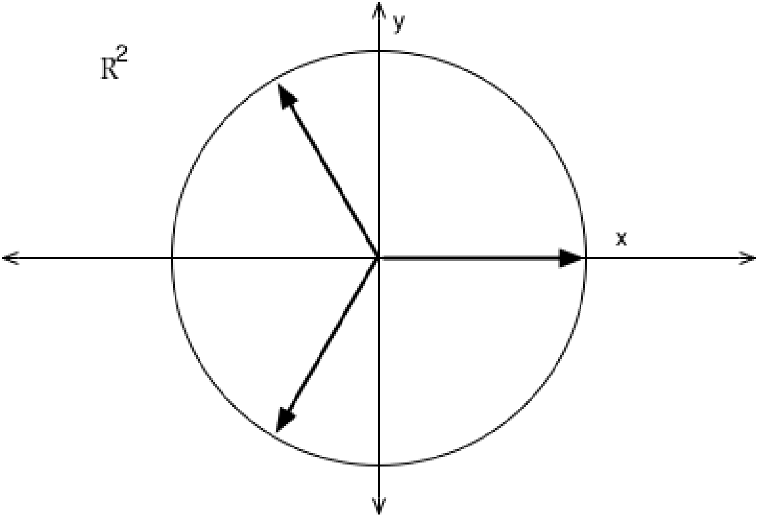
Equiangular lines: Vectors $v_1, \ldots, v_l$ in $\mathbb{C}^n$ such that

$$\left|\langle v_i, v_j \rangle\right| = \begin{cases} 1, & i = j; \\ \alpha, & \text{otherwise.} \end{cases}$$

In $\mathbb{C}^2$ (with $\omega^3 = 1$):

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2}\omega \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \sqrt{2}\omega^2 \end{pmatrix}$$

Equiangular lines



Mutually unbiased bases

Mutually unbiased bases: Bases $B_1, \ldots, B_b$ for $\mathbb{C}^n$ such that

$$|\langle u, v\rangle| = \begin{cases} 1, & u = v; \\ 0, & u \neq v, u, v \in B_i; \\ \alpha, & \text{otherwise.} \end{cases}$$

In $\mathbb{C}^2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

Mutually unbiased bases

Mutually unbiased bases: Bases $B_1, \ldots, B_b$ for $\mathbb{C}^n$ such that

$$|\langle u, v\rangle| = \begin{cases} 1, & u = v; \\ 0, & u \neq v, u, v \in B_i; \\ \alpha, & \text{otherwise.} \end{cases}$$

In $\mathbb{C}^2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

Flat vectors

Flat: every entry has the same absolute value.
$B_1, \ldots, B_b$ are mutually unbiased if and only if

- $B_i^* B_i = I$;
- $B_i^* B_j$ is flat ($i \neq j$).

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

Bounds for EAL's

If l is the largest number of equiangular lines in $\mathbb{C}^n$,

$$l \leq n^2.$$

- equality holds for $n \in \{2, 3, 4, 5, 6, 7, 8, 19\}$.
- evidence of equality for all n.

(Delsarte, Goethals, Seidel '75)
(Hoggar '98; Zauner '99; Grassl '04, Appleby '04)
(Renes, Blume-Kohout, Scott, Caves '03)

Bounds for MUB's

If b is the largest number of mutually unbiased bases in $\mathbb{C}^n$,

$$b \leq n + 1.$$

- for prime powers: equality holds.
- for non prime-powers: $b \geq 3$.

(Delsarte, Goethals, Seidel '75)

(Alltop '80; Wootters & Fields '89)

A construction of EAL's

Theorem (1)

Let D be a difference set in an abelian group G. Then the characters of G, restricted to D and normalized, are a set of equiangular lines.

- Best possible for flat lines
- If $n - 1$ is a prime power, then $n^2 - n + 1$ EAL's exist in $\mathbb{C}^n$.

Example

- A difference set in $\mathbb{Z}_7$: $\{0, 1, 3\}$
- Characters of $\mathbb{Z}_7$ (with $\omega^7 = 1$):

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \omega^3 \\ \omega^4 \\ \omega^5 \\ \omega^6 \end{pmatrix} \begin{pmatrix} 1 \\ \omega^2 \\ \omega^4 \\ \omega^6 \\ \omega \\ \omega^3 \\ \omega^5 \end{pmatrix} \cdots$$

- Theorem 1 $\Rightarrow$ 7 equiangular lines in $\mathbb{C}^3$.

Proof of Theorem (1)

If χ_a and χ_b are characters of G,

$$\begin{aligned}\langle \chi_a|_D, \chi_b|_D\rangle &= \sum_{d \in D} \overline{\chi_a(d)}\chi_b(d) \\ &= \sum_{d \in D} \chi_{b-a}(d) \\ &:= \chi_{b-a}(D).\end{aligned}$$

Proof of Theorem (1)

For any non-trivial character χ,

$$\begin{aligned} |\chi(D)|^2 &= \chi(D)\overline{\chi(D)} \\ &= \chi(D)\chi(-D) \\ &= |D|\chi(0) + \chi(G - \{0\}) \\ &= |D| - 1. \end{aligned}$$

□

Relative difference sets

- **Relative difference set**: a set $R \subseteq G$ such that for some subgroup N,
$$\Delta R = G - N.$$
- **Semiregular**: $|R| = |N|$, $|G| = |R|^2$.

eg)

$$G = \mathbb{Z}_4, \quad R = \{0, 1\}, \quad N = \{0, 2\}$$

Relative difference sets

- **Relative difference set**: a set $R \subseteq G$ such that for some subgroup N,
$$\Delta R = G - N.$$
- **Semiregular**: $|R| = |N|$, $|G| = |R|^2$.

eg)

$$G = \mathbb{Z}_4, \;\; R = \{0, 1\}, \;\; N = \{0, 2\}$$

A construction of MUB's

Theorem (2)

Let R be a semiregular relative difference set in an abelian group G. Then the characters of G, restricted to R and normalized, are a set of mutually unbiased bases.

- If n is a prime power, there are $n+1$ MUB's in $\mathbb{C}^n$.
- All known maximal MUB's can be constructed this way.

Beyond difference sets

Theorem (3)

Let Γ be a graph that is

- *k-regular*
- *bipartite with $2d$ vertices*
- *an abelian group of automorphisms acts regularly on each colour class.*

Then there is a set of complex lines $\{v_1, \ldots, v_d\}$ in $\mathbb{C}^k$ such that for any i and j,

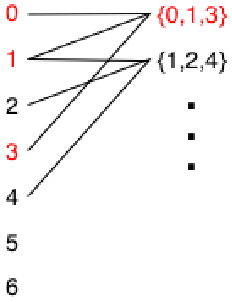
$$\left|\langle v_i, v_j \rangle\right| \in spec(\Gamma).$$

Difference sets → graphs

Difference set D ↔ Incidence structure $Dev(D)$ ↔ Incidence graph $(P, \mathcal{B})$

$\{0,1,3\} \subset \mathbb{Z}_7$

{0,1,3}
{1,2,4}
{2,3,5}
⋮



Future Work

- MUB's for non-prime powers, EAL's for $n > 8$
- Bipartite graphs with few eigenvalues
- Other proofs of upper bounds