Equiangular lines over finite fields

Joseph W. Iverson

Department of Mathematics
Iowa State University
Ames, IA, USA

Open Problems in Algebraic Combinatorics
Online Workshop
May 4, 2021

Collaborators

Gary R.W. Greaves
Nanyang Technological University

John Jasper
South Dakota State University

Dustin G. Mixon
The Ohio State University

Outline

Context: Real and complex equiangular lines

Equiangular lines in orthogonal geometry

Equiangular lines in unitary geometry

Outline

Context: Real and complex equiangular lines

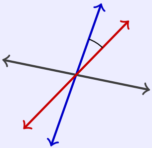
Equiangular lines in orthogonal geometry

Equiangular lines in unitary geometry

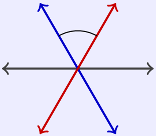
Line packing

Problem

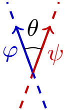
Pack n lines (1-dim subspaces) in $\mathbb{R}^d$ or $\mathbb{C}^d$ without sharp angles



Bad



Good



$\cos\theta = |\langle \varphi, \psi \rangle|$

- Given lines, choose unit norm reps

$$\Phi = \begin{bmatrix} | & & | \\ \varphi_1 & \cdots & \varphi_n \\ | & & | \end{bmatrix} \in \mathbb{C}^{d \times n}$$

- To avoid sharp angles, minimize **coherence**

$$\mu = \max_{i \neq j} |\langle \varphi_i, \varphi_j \rangle|$$

An application

Uniquely solve an underdetermined system

$$\begin{bmatrix} & \Phi & \end{bmatrix} \begin{bmatrix} \\ x \\ \\ \end{bmatrix} = \begin{bmatrix} y \end{bmatrix}$$

Image from `mylittledrummerboys.blogspot.com`

Donoho & Elad, Proc. Natl. Acad. Sci. USA, 2003

Candès, Romberg & Tao, IEEE Trans. Inform. Theory, 2006

An application

Uniquely solve an underdetermined system

$$\begin{bmatrix} & \Phi & \end{bmatrix} \begin{bmatrix} \\ x \\ \\ \end{bmatrix} = \begin{bmatrix} y \end{bmatrix}$$

Compressed sensing

$\Phi x = y$ has a unique **sparse** solution if

- x has a lot of zero entries, and
- the columns of Φ are "very different"

In fact, x can be found by a linear program

- Span lines with wide angles $\implies$ "very different"
- Better coherence $\implies$ fewer zeros required

Image from `mylittledrummerboys.blogspot.com`

Donoho & Elad, Proc. Natl. Acad. Sci. USA, 2003

Candès, Romberg & Tao, IEEE Trans. Inform. Theory, 2006

Recognizing optimal packings

Theorem (Welch bound)

Given n unit vectors spanning $\mathbb{R}^d$ or $\mathbb{C}^d$

$$\Phi = \begin{bmatrix} \varphi_1 & \cdots & \varphi_n \end{bmatrix} \in \mathbb{C}^{d\times n},$$

their coherence $\mu := \max_{i\neq j} |\langle \varphi_i, \varphi_j \rangle|$ satisfies

$$\mu \geq \sqrt{\frac{n-d}{d(n-1)}}.$$

Equality holds iff Φ is an **equiangular tight frame** (ETF):

- Equiangular: $|\langle \varphi_i, \varphi_j \rangle| = \mu$ for all $i \neq j$
- Tight frame: $\Phi\Phi^* = \mathrm{const} \cdot I$

Proof.

$0 \leq \|\Phi\Phi^* - \frac{n}{d} I_d\|_F^2 = \sum_{i,j\in[n]} |\langle \varphi_i, \varphi_j \rangle|^2 - \frac{n^2}{d} \leq (n^2-n)\mu^2 + n - \frac{n^2}{d}$

Welch, IEEE Trans. Inform. Theory, 1974

Image from calit2.net

Real and complex equiangular lines

Corollary (Relative bound)

Suppose $\mu^2 < \frac{1}{d}$ and there are n unit vectors

$$\Phi = \begin{bmatrix} \varphi_1 & \dots & \varphi_n \end{bmatrix}$$

in $\mathbb{R}^d$ or $\mathbb{C}^d$ such that $|\langle \varphi_i, \varphi_j \rangle| = \mu$ for every $i \neq j$. Then

$$n \leq \frac{d(1-\mu^2)}{1-d\mu^2}.$$

Equality holds if and only if Φ is an ETF.

J.J. Seidel

Lemmens and Seidel, J. Algebra, 1973

Image from "Geometry and Combinatorics", Academic Press, 1991

Real and complex equiangular lines

Theorem (Absolute/Gerzon bound)

If there are n unit vectors

$$\Phi = \begin{bmatrix} \varphi_1 & \dots & \varphi_n \end{bmatrix}$$

in $\mathbb{R}^d$ or $\mathbb{C}^d$ such that $|\langle \varphi_i, \varphi_j \rangle| = \mu$ is constant for $i \neq j$, then

$$n \leq \begin{cases} \binom{d+1}{2}, & \text{real case;} \\ d^2, & \text{complex case.} \end{cases}$$

If equality holds, then Φ is an ETF.

Michael Gerzon

Proof of bound.

- $\left[\langle \varphi_i \varphi_i^*, \varphi_j \varphi_j^* \rangle_F \right]_{ij} = \left[|\langle \varphi_i, \varphi_j \rangle|^2 \right]_{ij} = \mu J + (1-\mu) I$ is invertible
- So $\{\varphi_j \varphi_j^*\}_{j \in [n]}$ is linearly independent in the real space of self-adjoint matrices

Lemmens and Seidel, J. Algebra, 1973

Image from `michaelgerzonphotos.org.uk/`

Major open problems

Problem (Relative bound)

For which (d, n) is there a real $d \times n$ ETF? Complex?

- Real case: ETFs are equivalent to SRGs with $k = 2\mu$, many necessary conditions, smallest open case is $\cancel{33 \times 66}$ 43×86
- Complex case: Many examples, but nonexistence is hard

Major open problems

Problem (Relative bound)

For which (d, n) is there a real $d \times n$ ETF? Complex?

- Real case: ETFs are equivalent to SRGs with $k = 2\mu$, many necessary conditions, smallest open case is $\cancel{33 \times 66}$ 43×86
- Complex case: Many examples, but nonexistence is hard

Problem (Real absolute bound)

For which d is there a real $d \times \binom{d+1}{2}$ ETF?

- Existence known only for $d = 2, 3, 7, 23$
- Necessary conditions: $d \leq 3$ or $d + 2$ is an odd square
- Next open case is $d = 79$

Major open problems

Problem (Complex absolute bound / Zauner's conjecture)

Prove that for every $d \geq 1$, there is a complex $d \times d^2$ ETF.

Gerhard Zauner

- Numerical evidence for $d \leq 151$ (then computers are slow)
- Known for only finitely many dimensions d (e.g. $d \leq 24$)
- 2021 EUR prize for proof in infinitely many dimensions
- Seems related to Stark conjectures and Hilbert's 12th problem

---

Zauner, PhD Thesis, U Vienna, 1999

Golden KCIK Award, `arXiv:2002.03233`

Appleby, Flammia, McConnell, Yard, Found. Phys., 2017

Kopp, Int. Math. Res. Not., 2019

Image from `gerhardzauner.at`

This talk

Our approach

Consider finite field versions of the above problems

- Orthogonal geometry $\approx$ finite $\mathbb{R}^d$
- Unitary geometry $\approx$ finite $\mathbb{C}^d$

What's coming:

- Basic definitions and results
- Interactions with real/complex cases
- Connections with algebraic combinatorics
- Gerzon equality in infinitely many dimensions for both orthogonal and unitary geometry

Outline

Context: Real and complex equiangular lines

Equiangular lines in orthogonal geometry

Equiangular lines in unitary geometry

Finite orthogonal geometry

Throughout this section, $q = p^k$ is an odd prime power.

Definition

An **orthogonal geometry** on $\mathbb{F}_q^d$ is given by a nondegenerate symmetric bilinear form $\langle \cdot, \cdot \rangle \colon \mathbb{F}_q^d \times \mathbb{F}_q^d \to \mathbb{F}_q$. That means for every x and y:

- $\langle x, y \rangle = \langle y, x \rangle$
- $\langle x, \cdot \rangle \colon \mathbb{F}_q^d \to \mathbb{F}_q$ is linear
- if $x \neq 0$, then $\langle x, \cdot \rangle \colon \mathbb{F}_q^d \to \mathbb{F}_q$ is not the zero mapping

Examples

- $\langle x, y \rangle = x^\top y$
- $M = M^\top \in \mathbb{F}_q^{d \times d}$ is invertible, and $\langle x, y \rangle = x^\top M y$
- Every example takes this form with $M = \left[\langle e_i, e_j \rangle\right]_{ij}$

Two kinds of orthogonal geometry

Notation:

- $\mathbb{F}_q^\times$ is the multiplicative group of units
- $\mathbb{F}_q^{\times 2} \leq \mathbb{F}_q^\times$ is the subgroup of quadratic residues (squares)

Two kinds of orthogonal geometry

Notation:

- $\mathbb{F}_q^\times$ is the multiplicative group of units
- $\mathbb{F}_q^{\times 2} \leq \mathbb{F}_q^\times$ is the subgroup of quadratic residues (squares)

Change of basis:

- If $\langle x, y \rangle = x^\top My$ and if $B \in \mathbb{F}_q^{d \times d}$ is invertible, then $\langle Bx, By \rangle = x^\top B^\top MBy$

Two kinds of orthogonal geometry

Notation:

- $\mathbb{F}_q^\times$ is the multiplicative group of units
- $\mathbb{F}_q^{\times 2} \leq \mathbb{F}_q^\times$ is the subgroup of quadratic residues (squares)

Change of basis:

- If $\langle x, y \rangle = x^\top M y$ and if $B \in \mathbb{F}_q^{d \times d}$ is invertible, then $\langle Bx, By \rangle = x^\top B^\top M B y$
- $\det(B^\top M B) = \det(M) \det(B)^2 \in \det(M) \, \mathbb{F}_q^{\times 2}$
- $\det(M) \, \mathbb{F}_q^{\times 2} \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$ is an invariant of $\langle \cdot, \cdot \rangle$

Two kinds of orthogonal geometry

Notation:

- $\mathbb{F}_q^\times$ is the multiplicative group of units
- $\mathbb{F}_q^{\times 2} \leq \mathbb{F}_q^\times$ is the subgroup of quadratic residues (squares)

Change of basis:

- If $\langle x, y\rangle = x^\top My$ and if $B \in \mathbb{F}_q^{d\times d}$ is invertible, then $\langle Bx, By\rangle = x^\top B^\top MBy$
- $\det(B^\top MB) = \det(M)\det(B)^2 \in \det(M)\,\mathbb{F}_q^{\times 2}$
- $\det(M)\,\mathbb{F}_q^{\times 2} \in \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ is an invariant of $\langle\cdot,\cdot\rangle$

Proposition

Up to linear isometry, there exactly two kinds of orthogonal geometry on $\mathbb{F}_q^d$:

- *Square type:* $\det M \in \mathbb{F}_q^{\times 2}$ *(e.g. $\langle x, y\rangle = x^\top y$)*
- *Nonsquare type:* $\det M \notin \mathbb{F}_q^{\times 2}$

Equiangular systems and tight frames

Fix an orthogonal geometry on $\mathbb{F}_q^d$

Definition

For $a, b, c \in \mathbb{F}_q$, a sequence $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ is:

- a **frame** if it spans $\mathbb{F}_q^d$;

Equiangular systems and tight frames

Fix an orthogonal geometry on $\mathbb{F}_q^d$

Definition

For $a, b, c \in \mathbb{F}_q$, a sequence $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ is:

- a **frame** if it spans $\mathbb{F}_q^d$;
- a c-**tight frame** if it spans $\mathbb{F}_q^d$ and moreover

$$\sum_{j \in [n]} \langle \varphi_j, x \rangle \varphi_j = cx$$

  for every $x \in \mathbb{F}_q^d$;

Equiangular systems and tight frames

Fix an orthogonal geometry on $\mathbb{F}_q^d$

Definition

For $a, b, c \in \mathbb{F}_q$, a sequence $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ is:

- a **frame** if it spans $\mathbb{F}_q^d$;
- a c-**tight frame** if it spans $\mathbb{F}_q^d$ and moreover
$$\textstyle\sum_{j \in [n]} \langle \varphi_j, x \rangle \varphi_j = cx$$
for every $x \in \mathbb{F}_q^d$;
- an (a, b)-**equiangular system** if:
  (i) $\langle \varphi_i, \varphi_i \rangle = a$ for every $i \in [n]$, and
  (ii) $\langle \varphi_i, \varphi_j \rangle^2 = b$ for every $i \neq j$ in $[n]$;

Equiangular systems and tight frames

Fix an orthogonal geometry on $\mathbb{F}_q^d$

Definition

For $a, b, c \in \mathbb{F}_q$, a sequence $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ is:

- a **frame** if it spans $\mathbb{F}_q^d$;
- a c-**tight frame** if it spans $\mathbb{F}_q^d$ and moreover
$$\sum_{j\in[n]} \langle \varphi_j, x\rangle \varphi_j = cx$$
for every $x \in \mathbb{F}_q^d$;
- an (a, b)-**equiangular system** if:
  (i) $\langle \varphi_i, \varphi_i\rangle = a$ for every $i \in [n]$, and
  (ii) $\langle \varphi_i, \varphi_j\rangle^2 = b$ for every $i \neq j$ in $[n]$;
- an (a, b, c)-**equiangular tight frame** (ETF) if it is an (a, b)-equiangular system and a c-tight frame.

Differences from real case

Examples of differences with $p = 3$ and $\langle x, y \rangle = x^\top y$

Nonzero vectors can have "norm" 0:

- $x = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^\top$ has $\langle x, x \rangle = 0$

Differences from real case

Examples of differences with $p = 3$ and $\langle x, y \rangle = x^\top y$

Nonzero vectors can have "norm" 0:

- $x = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^\top$ has $\langle x, x \rangle = 0$

Tight frames can have constant 0:

- $\Phi = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ has $\Phi\Phi^\top = 0I$

Differences from real case

Examples of differences with $p = 3$ and $\langle x, y \rangle = x^\top y$

Nonzero vectors can have "norm" 0:

- $x = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^\top$ has $\langle x, x \rangle = 0$

Tight frames can have constant 0:

- $\Phi = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ has $\Phi\Phi^\top = 0I$

Spectral theorem fails:

- $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}^2 = 0$, so $\sigma(J_3) = \{0^2\}$ and J_3 is not diagonalizable

Example: $4 \times 10 = \binom{4+1}{2}$ ETF

$p = 3,\ M = \operatorname{diag}(1,1,1,2)$

$$\Phi = \begin{bmatrix} 1 & 2 & 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{F}_3^{4\times 10}$$

is an ETF with $(a,b,c) = (0,1,0)$ since $\operatorname{rank}\Phi = 4$, $\Phi\Phi^\top M = 0$,

$$\big[\langle \varphi_i, \varphi_j \rangle\big]_{ij} = \begin{bmatrix} 0 & - & + & + & - & - & + & + & + & + \\ - & 0 & - & + & + & + & - & + & + & + \\ + & - & 0 & - & + & + & + & - & + & + \\ + & + & - & 0 & - & + & + & + & - & + \\ - & + & + & - & 0 & + & + & + & + & - \\ - & + & + & + & + & 0 & + & - & - & + \\ + & - & + & + & + & + & 0 & + & - & - \\ + & + & - & + & + & - & + & 0 & + & - \\ + & + & + & - & + & - & - & + & 0 & + \\ + & + & + & + & - & + & - & - & + & 0 \end{bmatrix}$$

Image from `wikimedia.org`

Example: $4 \times 10 = \binom{4+1}{2}$ ETF

$p = 3$, $M = \mathrm{diag}(1,1,1,2)$

$$\Phi = \begin{bmatrix} 1 & 2 & 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{F}_3^{4\times 10}$$

is an ETF with $(a,b,c) = (0,1,0)$ since $\operatorname{rank}\Phi = 4$, $\Phi\Phi^\top M = 0$,

$$\big[\langle \varphi_i, \varphi_j\rangle\big]_{ij} = \begin{bmatrix} 0 & - & + & + & - & - & + & + & + & + \\ - & 0 & - & + & + & + & - & + & + & + \\ + & - & 0 & - & + & + & + & - & + & + \\ + & + & - & 0 & - & + & + & + & - & + \\ - & + & + & - & 0 & + & + & + & + & - \\ - & + & + & + & + & 0 & + & - & - & + \\ + & - & + & + & + & + & 0 & + & - & - \\ + & + & - & + & + & - & + & 0 & + & - \\ + & + & + & - & + & - & - & + & 0 & + \\ + & + & + & + & - & + & - & - & + & 0 \end{bmatrix}$$

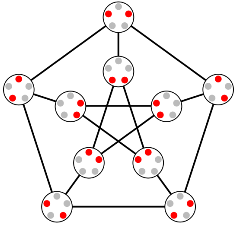


Image from `wikimedia.org`

Frames from Gram matrices

Suppose $\langle x, y \rangle = x^\top M y$.

If $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ spans, then it contains a basis, and a principal submatrix of $\left[\langle \varphi_i, \varphi_j \rangle\right]_{ij}$ is a Gram matrix for $\langle \cdot, \cdot \rangle$.

Frames from Gram matrices

Suppose $\langle x, y\rangle = x^\top My$.

If $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ spans, then it contains a basis, and a principal submatrix of $\left[\langle\varphi_i, \varphi_j\rangle\right]_{ij}$ is a Gram matrix for $\langle\cdot,\cdot\rangle$.

Theorem

Given $G \in \mathbb{F}_q^{n\times n}$, choose columns that form a basis for Col G*, and let G_b be the corresponding principal submatrix. There exists a spanning set $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_q^d$ such that $G = \left[\langle\varphi_i, \varphi_j\rangle\right]_{ij}$ iff:*

(i) $G^\top = G$,

(ii) $\operatorname{rank} G = d$,

(iii) $\det(G_b) \in \det(M)\,\mathbb{F}_q^{\times 2}$.

- Every symmetric matrix is a Gram matrix in **some** geometry

ETFs from Gram matrices

Corollary

Suppose $G \in \mathbb{F}_q^{n\times n}$ has $\operatorname{rank} G = d$. Then G is the Gram matrix of an (a,b,c)-ETF in an orthogonal geometry on $\mathbb{F}_q^d$ iff:

(i) $G = G^\top$,

(ii) $G_{ii} = a$ for every $i \in [n]$,

(iii) $(G_{ij})^2 = b$ for every $i \neq j$ in $[n]$,

(iv) $G^2 = cG$.

$$G = \begin{bmatrix} 0 & - & + & + & - & - & + & + & + & + \\ - & 0 & - & + & + & + & - & + & + & + \\ + & - & 0 & - & + & + & + & - & + & + \\ + & + & - & 0 & - & + & + & + & - & + \\ - & + & + & - & 0 & + & + & + & + & - \\ - & + & + & + & + & 0 & + & - & - & + \\ + & - & + & + & + & + & 0 & + & - & - \\ + & + & - & + & + & - & + & 0 & + & - \\ + & + & + & - & + & - & - & + & 0 & + \\ + & + & + & + & - & + & - & - & + & 0 \end{bmatrix}, \; G^2 = 0 \qquad \rightsquigarrow \qquad \Phi = \begin{bmatrix} 1 & 2 & 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 0 & 1 & 0 \end{bmatrix},$$

$$(a,b,c) = (0,1,0)$$

Overlap with the real case

Recall $q = p^k$ is an odd prime power.

Proposition

Suppose there is a real $d \times n$ ETF with $n > d + 1$, and either

(i) $n \neq 2d$ *and* $p \nmid \sqrt{\frac{d(n-1)}{n-d}}$*; or*

(ii) $n = 2d$ *and* $n - 1 \in \mathbb{F}_q^{\times 2}$*.*

Then there is a $d \times n$ ETF in an orthogonal geometry on $\mathbb{F}_q^d$.

Proposition

Suppose there is a $d \times n$ ETF in an orthogonal geometry on $\mathbb{F}_q^d$. If $p > 2n - 5$, then there is a real $d \times n$ ETF.

- Moral: Lots of overlap with the real case
- Caveat: Weird stuff in the cracks!

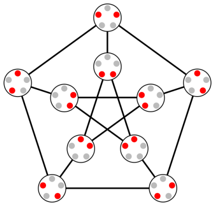
Strongly regular graphs

Definition

A (simple, undirected) graph is **strongly regular** if it is neither edgeless nor complete, and there are parameters k, λ, μ such that:

- every vertex has exactly k neighbors,
- every pair of adjacent vertices have exactly λ neighbors in common, and
- every pair of distinct nonadjacent vertices have exactly μ neighbors in common.

If there are v vertices, then we call it a (v, k, λ, μ)-SRG.



Petersen graph:
$v = 10,\ k = 3,$
$\lambda = 0,\ \mu = 1$

SRG notation

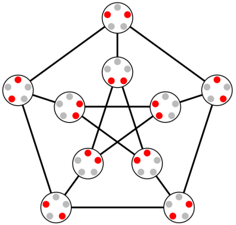
Given a (v, k, λ, μ)-SRG:

- The $\{0, 1\}$-adjacency matrix A has $\sigma(A) =: \{k^1, r^f, s^g\}$, where $r > 0 > s$
- Each of r, s, f, g is a function of (v, k, λ, μ)

SRG notation

Given a (v, k, λ, μ)-SRG:

- The $\{0,1\}$-adjacency matrix A has $\sigma(A) =: \{k^1, r^f, s^g\}$, where $r > 0 > s$
- Each of r, s, f, g is a function of (v, k, λ, μ)
- The **Seidel adjacency matrix** $\Sigma := J - 2A - I$ has $\sigma(\Sigma) = \{(v-2k-1)^1, (-2r-1)^f, (-2s-1)^g\}$
- $\Sigma_{ij} = \begin{cases} -1, & \text{if } i \sim j; \\ 1, & \text{if } i \nsim j \text{ and } i \neq j; \\ 0, & \text{if } i = j \end{cases}$



$$\begin{bmatrix} 0&1&0&0&1&1&0&0&0&0 \\ 1&0&1&0&0&0&1&0&0&0 \\ 0&1&0&1&0&0&0&1&0&0 \\ 0&0&1&0&1&0&0&0&1&0 \\ 1&0&0&1&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&1&1&0 \\ 0&1&0&0&0&0&0&0&1&1 \\ 0&0&1&0&0&1&0&0&0&1 \\ 0&0&0&1&0&1&1&0&0&0 \\ 0&0&0&0&1&0&1&1&0&0 \end{bmatrix}$$

A

$$\begin{bmatrix} 0&-&+&+&-&-&+&+&+&+ \\ -&0&-&+&+&+&-&+&+&+ \\ +&-&0&-&+&+&+&-&+&+ \\ +&+&-&0&-&+&+&+&-&+ \\ -&+&+&-&0&+&+&+&+&- \\ -&+&+&+&+&0&+&-&-&+ \\ +&-&+&+&+&+&0&+&-&- \\ +&+&-&+&+&-&+&0&+&- \\ +&+&+&-&+&-&-&+&0&+ \\ +&+&+&+&-&+&-&-&+&0 \end{bmatrix}$$

Σ

SRGs and ETFs

Notation: For $M \in \mathbb{Z}^{n\times n}$, $\overline{M} \in \mathbb{F}_p^{n\times n}$ is its image mod p

Theorem

Given an SRG with $f \neq g$, define $G := \Sigma + (2r+1)I$ and $d := \operatorname{rank}_p \overline{G}$. If p divides $v - 4k + 2\lambda + 2\mu$, then $\overline{G}$ is the Gram matrix of a $(2r+1, 1, 2r-2s)$-ETF with size $d \times v$ in an orthogonal geometry on $\mathbb{F}_p^d$. Furthermore:

(a) *If $r \not\equiv_p s$ and $v - 2k + 2r \not\equiv_p 0$, then $d = g + 1$.*

(b) *If $r \not\equiv_p s$ and $v - 2k + 2r \equiv_p 0$, then $d = g$.*

(c) *If $r \equiv_p s$, then $d \leq \min\{f+1, g+1\}$.*

(d) *Let p^m be the largest power of p that divides v. If p^{m+1} divides $v - 2k + 2r$, then $d \leq g$.*

More SRGs and ETFs

Theorem

Given an SRG with $f \neq g$, define $d := \operatorname{rank}_p \overline{\Sigma + (2r+1)I}$, $n := v + 1$, and

$$G := \begin{bmatrix} 2r+1 & \mathbf{1}_v^\top \\ \mathbf{1}_v & \Sigma + (2r+1)I \end{bmatrix} \in \mathbb{Z}^{n \times n},$$

If p divides both $k - 2\mu$ and $v - 3k + 2\lambda + 1$, then $\overline{G} \in \mathbb{F}_p^{n \times n}$ is the Gram matrix of a $(2r+1, 1, 2r-2s)$-ETF with size $d \times n$ in an orthogonal geometry on $\mathbb{F}_p^d$. Furthermore:

(a) *If $r \not\equiv_p s$, then $d = g + 1$.*

(b) *If $r \equiv_p s$, then $d \leq \min\{f+1, g+1\}$.*

SRGs from ETFs

Corollary

A (v, k, λ, μ)-SRG comes from a finite field ETF unless **both** *of*

$$|v - 4k + 2\lambda + 2\mu| \qquad \textit{and} \qquad \gcd(k - 2\mu, v - 3k + 2\lambda + 1)$$

are powers of 2.

- Brouwer's table of feasible SRG parameters: 211 known complementary pairs of parameters with $v \leq 1300$
- All but 9 pairs (95%) come from finite field ETFs:

v	k	λ	μ
21	10	3	6
40	12	2	4
57	24	11	9

v	k	λ	μ
70	27	12	9
112	30	2	10
120	42	8	18

v	k	λ	μ
220	84	38	28
280	117	44	52
512	196	60	84

$(a, 1, c)$-ETFs from SRGs

p	d	n	a	c
3	**4**	**10**	**0**	**0**
3	9	25	0	1
3	9	37	0	1
3	10	37	0	0
3	**10**	**55**	**0**	**0**
3	12	36	1	0
3	12	49	0	1
3	12	67	0	1
3	**13**	**91**	**0**	**0**
3	14	36	1	0
3	14	45	1	0
3	15	64	0	1
3	15	106	0	1
3	16	82	0	0
3	**16**	**136**	**0**	**0**
3	18	81	1	0
3	18	100	0	1
3	18	154	0	1
3	19	49	1	1
3	19	65	1	2
3	19	81	1	0
3	19	105	1	0
3	**19**	**190**	**0**	**0**
3	20	46	0	0
3	20	57	1	0
3	21	81	1	0
3	21	121	0	1
3	21	162	1	0
3	21	211	0	1
3	22	50	1	2
3	22	65	1	2
3	22	77	1	2

p	d	n	a	c
3	22	100	1	1
3	22	145	0	0
3	22	243	1	0
3	22	253	0	0
3	**22**	**253**	**1**	**1**
3	22	276	1	0
3	24	117	1	0
3	24	169	0	1
3	24	277	0	1
3	25	101	1	2
3	**25**	**325**	**0**	**0**
5	9	26	0	0
5	10	45	2	4
5	11	56	2	2
5	12	26	0	0
5	**12**	**78**	**2**	**3**
5	13	49	2	1
5	15	65	2	4
5	15	105	2	4
5	16	81	2	2
5	16	121	2	2
5	**17**	**153**	**2**	**3**
5	19	126	0	0
5	20	56	0	2
5	20	81	0	2
5	20	190	2	4
5	21	51	0	0
5	21	176	0	0
5	21	211	2	2
5	**22**	**253**	**2**	**3**
5	23	101	0	0

p	d	n	a	c
5	23	144	2	1
5	24	101	0	0
5	25	81	0	2
5	25	101	0	2
5	25	170	2	4
5	25	300	2	4
7	12	66	3	6
7	13	79	3	1
7	**14**	**105**	**3**	**5**
7	16	50	0	0
7	17	81	3	4
7	19	101	3	6
7	19	171	3	6
7	20	121	3	1
7	20	191	3	1
7	21	77	2	5
7	21	231	3	5
7	24	50	0	0
7	24	100	2	6
11	16	120	3	6
11	17	137	3	8
11	**18**	**171**	**3**	**1**
11	25	169	3	4
13	18	153	3	6
13	19	172	3	8
13	**20**	**210**	**3**	**12**
17	22	231	3	6
17	23	254	3	8
17	**24**	**300**	**3**	**12**
19	24	276	3	6
19	25	301	3	8

Necessary conditions for SRGs

If the SRG exists, then so does the $(a, 1, c)$-ETF

v	k	λ	p	d	n	a	c
69	48	32	13	24	69	5	3
85	54	33	7	35	85	0	4
85	70	57	5	35	86	0	4
85	70	57	13	35	85	5	1
88	27	6	5	32	88	2	3
99	**14**	**1**	**5**	**45**	**100**	**2**	**4**
100	33	8	3	34	101	1	2
111	30	5	19	36	111	7	1
112	36	10	3	48	112	0	2
115	18	1	3	46	115	1	1
115	18	1	17	45	115	7	16
120	34	8	7	52	121	2	6
120	84	58	3	57	121	0	2
121	36	7	3	37	121	1	1
121	36	7	5	36	121	2	2
121	48	17	3	48	121	0	1
133	32	6	3	57	133	0	2
133	32	6	11	56	133	9	9
133	88	57	3	57	133	0	1
133	88	57	5	56	133	4	2
133	108	87	5	57	133	2	3
133	108	87	11	56	133	7	7
136	105	80	3	52	137	1	2
136	105	80	11	52	136	7	9
162	21	0	5	57	163	2	3
162	21	0	7	56	162	0	4
162	92	46	7	24	163	5	1
162	112	76	13	64	162	9	11
162	138	117	7	70	162	0	4
162	138	117	17	70	163	7	1
169	42	5	3	43	170	1	2
169	42	5	5	43	169	2	1
169	42	5	7	42	169	0	5
169	56	15	3	57	169	0	2
169	56	15	5	56	169	4	1
169	70	27	3	70	169	2	2
175	108	63	13	43	175	7	4
176	25	0	3	55	176	1	2

v	k	λ	p	d	n	a	c
176	25	0	7	56	176	0	6
176	25	0	17	56	177	7	3
176	70	24	5	56	177	4	3
183	52	11	5	61	184	4	1
183	52	11	29	60	183	9	26
189	128	82	11	29	189	5	3
189	140	103	5	91	189	1	4
190	144	108	5	76	191	4	4
196	39	2	3	49	197	1	2
196	39	2	7	49	197	0	5
196	39	2	31	48	196	7	26
196	45	4	3	46	196	1	1
196	75	26	3	76	197	2	1
196	114	59	5	25	196	0	2
204	28	2	13	84	204	9	7
204	140	94	3	69	205	0	1
205	68	15	3	40	205	1	1
205	68	15	5	40	205	2	4
208	45	8	5	91	209	1	4
209	156	115	5	76	209	4	1
209	156	115	7	77	210	2	5
209	156	115	11	77	209	9	4
210	33	0	5	55	210	2	4
210	33	0	7	56	211	0	3
210	76	26	5	96	211	3	3
210	132	82	3	100	211	1	1
216	129	72	13	44	217	7	10
216	172	136	5	86	216	4	4
217	128	72	3	63	217	0	2
220	72	22	3	100	220	1	1
225	48	3	7	49	225	0	2
225	64	13	7	64	225	2	2
225	128	64	5	25	226	0	3
231	160	110	5	111	231	3	3
232	33	2	3	87	232	0	1
232	33	2	19	88	232	9	3
232	33	2	23	88	233	9	22
232	63	14	3	88	233	2	1

Bounds on equiangular lines

Problem (Relative bound)

Given an orthogonal geometry on $\mathbb{F}_q^d$ and $a, b \in \mathbb{F}_q$, find an upper bound for the size of an (a, b)-equiangular system.

- Efficient bound may disprove SRGs
- Is there a $(2, 1)$-equiangular system with 100 vectors in an orthogonal geometry on $\mathbb{F}_5^{45}$?
- If not, then Conway's 99-graph DNE

Bounds on equiangular lines

Problem (Relative bound)

Given an orthogonal geometry on $\mathbb{F}_q^d$ and $a, b \in \mathbb{F}_q$, find an upper bound for the size of an (a, b)-equiangular system.

- Efficient bound may disprove SRGs
- Is there a $(2, 1)$-equiangular system with 100 vectors in an orthogonal geometry on $\mathbb{F}_5^{45}$?
- If not, then Conway's 99-graph DNE

Theorem (Gerzon; Greaves, JI, Jasper, Mixon)

If $a^2 \neq b$ and there is an (a, b)-equiangular system Φ of n vectors in an orthogonal geometry on $\mathbb{F}_q^d$, then $n \leq \binom{d+1}{2}$. If equality holds, then Φ is an ETF.

- $a^2 \neq b$ avoids trivialities like an entire isotropic subspace

Attaining Gerzon's bound

Theorem (Greaves, JI, Jasper, Mixon)

For every integer $d > 1$ and every odd prime p that divides $d - 7$, there exists a $(3, 1, 12)$-ETF of $n = \binom{d+1}{2}$ vectors in an orthogonal geometry on $\mathbb{F}_p^d$. In particular, Gerzon's bound is attained in some d-dimensional orthogonal geometry provided $|d - 7| \neq 2^k$.

- Complement of the triangular graph $T(d+1)$, i.e., Kneser graph $K(d+1, 2)$
- Add some identity to the Seidel matrix
- Take it mod p
- Factor the Gram matrix

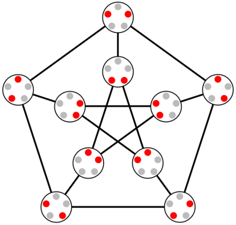


Image from wikimedia.org

Not attaining Gerzon's bound

Recall: We win with Gerzon if $|d-7| \neq 2^k$

Theorem (Greaves, JI, Jasper, Mixon)

For any choice of odd prime power q, there does not exist an ETF of $n = 15 = \binom{5+1}{2}$ vectors in any orthogonal geometry on $\mathbb{F}_q^5$. In particular, Gerzon's bound is not attained in any 5-dimensional finite orthogonal geometry over a field of odd characteristic.

- Real 5×15 ETF DNE
- Overlap with real case: $p \leq 25$
- Field stuff: $q = p \in \{3, 5, 7, 19\}$
- Witt extension theorem: Computationally efficient way to bound a clique number in graph of vectors with the right angle
- $p = 5$ is a weirdo, comes down to rank condition

Outline

Context: Real and complex equiangular lines

Equiangular lines in orthogonal geometry

Equiangular lines in unitary geometry

Unitary geometry

Throughout this section, q is a prime power (possibly even)

"Complex conjugation" on $\mathbb{F}_{q^2}$: $x \mapsto x^q$

- Order-2 field automorphism
- Fixes $\mathbb{F}_q \le \mathbb{F}_{q^2}$

Unitary geometry

We give $\mathbb{F}_{q^2}^d$ the Hermitian form $\langle x, y \rangle := \sum_{i \in [d]} x_i^q y_i =: x^* y$.

For every $x, y \in \mathbb{F}_{q^2}^d$:

- $\langle x, y \rangle = \langle y, x \rangle^q$
- $\langle x, \cdot \rangle \colon \mathbb{F}_{q^2}^d \to \mathbb{F}_{q^2}^d$ is linear
- if $x \neq 0$, then $\langle x, \cdot \rangle \colon \mathbb{F}_{q^2}^d \to \mathbb{F}_{q^2}^d$ is not the zero mapping

This is the unique Hermitian form (up to isometric isomorphism).

Equiangular systems and tight frames

Definition

For $a, b, c \in \mathbb{F}_q$, a sequence $\varphi_1, \ldots, \varphi_n \in \mathbb{F}_{q^2}^d$ is:

- a **frame** if it spans $\mathbb{F}_{q^2}^d$;
- a c-**tight frame** if it spans $\mathbb{F}_{q^2}^d$ and moreover
  $$\sum_{j\in[n]} \langle \varphi_j, x\rangle \varphi_j = cx$$
  for every $x \in \mathbb{F}_{q^2}^d$;
- an (a, b)-**equiangular system** if:
  (i) $\langle \varphi_i, \varphi_i \rangle = a$ for every $i \in [n]$, and
  (ii) $\langle \varphi_i, \varphi_j \rangle^{q+1} = b$ for every $i \neq j$ in $[n]$;
- an (a, b, c)-**equiangular tight frame** (ETF) if it is an (a, b)-equiangular system and a c-tight frame.

Some examples

Example

Any ETF in an orthogonal geometry on $\mathbb{F}_q^d$ gives one of the same size in unitary geometry on $\mathbb{F}_{q^2}^d$.

Example

$q = 2$, $\zeta \in \mathbb{F}_{2^2}^\times$ is primitive.
There is a 6×27 ETF with parameters $(a, b, c) = (0, 1, 1)$:

$$\Phi = \begin{bmatrix} 1 & \zeta & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \zeta & \zeta & \zeta & \zeta & \zeta & \zeta & \zeta \\ \zeta & \zeta & \zeta & \zeta & \zeta & \zeta & \zeta & \zeta & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \zeta & \zeta & \zeta^2 & \zeta^2 & 0 & 0 & 0 & 0 & 1 & \zeta & \zeta^2 \\ 0 & 0 & 1 & 1 & 1 & \zeta & \zeta^2 & \zeta^2 & 1 & 1 & \zeta & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 & 0 & 0 & \zeta & \zeta & \zeta & \zeta & \zeta \\ 0 & 0 & 1 & \zeta & \zeta & 0 & 1 & \zeta^2 & \zeta & \zeta^2 & 0 & 1 & 1 & \zeta & 0 & \zeta & 0 & \zeta & 0 & \zeta & 1 & \zeta & 0 & \zeta^2 & \zeta & \zeta & \zeta \\ 0 & 0 & \zeta & \zeta & 1 & 0 & \zeta^2 & 1 & \zeta^2 & \zeta & 0 & \zeta & 1 & 1 & \zeta & 0 & \zeta & 0 & \zeta & 0 & \zeta & 1 & \zeta^2 & 0 & \zeta & \zeta & \zeta \end{bmatrix}$$

Its automorphism group is doubly transitive. (No doubly transitive complex ETF of this size exists.)

Projecting complex ETFs

Theorem (Greaves, JI, Jasper, Mixon)

Suppose there is a $d \times n$ complex ETF.

(a) *There is a $d \times n$ complex ETF with algebraic entries.*

(b) *For infinitely many pairwise coprime q, there is a $d \times n$ ETF in a unitary geometry on $\mathbb{F}_{q^2}^d$.*

- (a) is an application of Tarski–Seidenberg
- (b) is an application of Frobenius density theorem

Problem

Does the converse of (b) hold?

Gerzon's bound in unitary geometry

Theorem

If $a^2 \neq b$ and there is an (a, b)-equiangular system Φ of n vectors in a unitary geometry on $\mathbb{F}_{q^2}^d$, then $n \leq d^2$. If equality holds, then Φ is an ETF.

Problem

For which (q, d) is Gerzon's bound saturated?

- Zauner: For every d, there exists q
- Harder than Zauner to solve completely
- Easier to make progress

Time-frequency shifts

Assume $d_1, \ldots, d_m$ **all divide** $q+1$**.** Let $G = \prod_{k=1}^m \mathbb{Z}/d_k\mathbb{Z}$.

$\mathbb{F}_{q^2}^G \cong \mathbb{F}_{q^2}^{|G|}$ consists of functions $\varphi\colon G \to \mathbb{F}_{q^2}$.

For each k, fix a generator $\omega_k \in \mathbb{F}_{q^2}^\times$ for the subgroup of size d_k

Definition

For $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m) \in G$ and $\varphi \in \mathbb{F}_{q^2}^G$,

$$(T_y\varphi)(x) := \varphi(x-y) \qquad \text{and} \qquad (M_y\varphi)(x) := \prod_{k=1}^m \omega_k^{x_k y_k} \cdot \varphi(x).$$

Then $T_y, M_y \colon \mathbb{F}_{q^2}^G \to \mathbb{F}_{q^2}^G$ are isometric isomorphisms.

Proposition

For any nonzero $\varphi \in \mathbb{F}_{q^2}^G$, $\{T_x M_y \varphi\}_{x,y\in G}$ *is a tight frame for* $\mathbb{F}_{q^2}^G$.

Attaining Gerzon's bound

Theorem (Greaves, JI, Jasper, Mixon)

Take $q = 3$, m odd, and $d_k = 2$ for $1 \le k \le m$, so $G = (\mathbb{Z}/2\mathbb{Z})^m$. Let $\zeta \in \mathbb{F}_{3^2}$ be primitive, and define $\varphi \in \mathbb{F}_{3^2}^G$ by

$$\varphi(x) = \begin{cases} -1 - \zeta^2, & \text{if } x = 0; \\ 1, & \text{otherwise.} \end{cases}$$

Then $\Phi = \{T_x M_y \varphi\}_{x,y \in G}$ is a $(0,1,0)$-ETF of size $2^m \times 2^{2m}$. In particular, Gerzon's bound is attained in a unitary geometry on $\mathbb{F}_{3^2}^d$ whenever $d = 2^{2k+1}$.

- "TF" is free
- "E" is a direct calculation

Limited connections with complex case

Recall: Gerzon's bound is attained in a unitary geometry on $\mathbb{F}_{3^2}^d$ whenever $d = 2^{2k+1}$

- $d = 2, 8$ lift to complex ETFs that attain Gerzon's bound
  - $d = 2$: Tetrahedron in Bloch sphere
  - $d = 8$: Hoggar's 64 lines in $\mathbb{C}^8$
- $d = 32$ does not appear to lift to a complex ETF
- Godsil and Roy: Time-frequency shifts over $\mathbb{Z}_2^m$ generate an ETF only if $m \in \{1, 3\}$.

Godsil and Roy, European J. Combin., 2009

Some more problems

Problem

Generalize (doubly transitive) complex 3×9 to an infinite family over a finite field.

Problem

Is there a combinatorial description of ETFs in finite unitary geometry?

Problem

Find necessary conditions (e.g. integrality constraints) for ETF existence in unitary geometry.

Questions?

Frames over finite fields: Basic theory and equiangular lines in unitary geometry
G.R.W. Greaves, J.W. Iverson, J. Jasper, D.G. Mixon
arXiv:2012.12977

Frames over finite fields: Equiangular lines in orthogonal geometry
G.R.W. Greaves, J.W. Iverson, J. Jasper, D.G. Mixon
arXiv:2012.13642

Image from `sideshowtoy.com`