Open problems in finite frame theory: Packings in projective spaces

Dustin G. Mixon

Tight Frames and Approximation

February 20, 2018
Big picture

**Finite frame theory:** Application-driven arrangements of vectors

Recent problems solved with the help of AG:
- Phase retrieval injectivity threshold
- Finite-dimensional HRT conjecture
- Bilinear identifiability threshold
- Full spark unit norm tight frames

**This talk:** Can AG solve projective packing problems?

Vinzant, SampTA 2015
Cahill, M., Strawn, SIAM J. Appl. Algebra Geometry, 2017
A motivating application

Why the decline? Better home theaters, **easy access online**

---

L.E.K., Box Office Trends, 2015
Stobing, How Do Movies Leak Before They Come Out on DVD and Blu-Ray?, 2016
A motivating application

How to defeat media piracy?

Watermarks help, but these can be removed

**Want:** Robust personalized fingerprints to help identify culprits

image from hollywoodandfine.com/the-screen-image-deteriorates/
A motivating application

-unit fingerprints \( \{\varphi_i\}_{i \in [n]} \)

- The \( i \)th user is given \( s + \varphi_i \)

- Users \( K \subseteq [n] \) forge the signal:
  \[
  \hat{s} = \sum_{k \in K} \alpha_k (s + \varphi_k) + \epsilon
  \]

- Interrogate argmax
  \[
  \arg \max_{i \in [n]} |\langle \varphi_i, \hat{s} - s \rangle|\n  \]

Theorem

\[
\max_{i,j \in [n], i \neq j} |\langle \varphi_i, \varphi_j \rangle| \text{ small, } K, \epsilon \text{ small } \implies \text{ false positives unlikely}
\]

The problem

Find unit-norm vectors \( \{ \varphi_i \}_{i \in [n]} \subseteq \mathbb{F}^d \) that minimize coherence:

\[
\mu(\{ \varphi_i \}_{i \in [n]}) = \max_{i,j \in [n], i \neq j} |\langle \varphi_i, \varphi_j \rangle |
\]

i.e., \( n \) points in \( \mathbb{F}P^{d-1} \) that maximize the minimum distance

Applications

▶ digital fingerprinting
▶ multiple description coding
▶ compressed sensing
▶ quantum state estimation

cf. Tammes problem:

image from wearedesignbureau.com/projects/weird-science/

Common mallow pollen grain
Packing cheat sheet

**Step 1:** Prove lower bound on coherence
- Isometric embedding
- Semidefinite programming
- Tarski–Seidenberg projection

**Step 2:** Construct packing that meets bound
- Group actions
- Combinatorial design
- Non-convex optimization
Packing in $\mathbb{RP}^1$

$n = 2$  
$n = 3$  
$n = 4$  
$n = 5$

Easy proof of optimality:

- $\mathbb{RP}^1$ and $S^1$ are isometrically isomorphic
- pigeonhole $\Rightarrow$ equally spaced points are optimal
Packing in $\mathbb{RP}^2$

Case-by-case optimality proofs, most cases are open
Part I

The Welch bound
**Theorem (Welch bound)**

Suppose $n \geq d$. Then every $\{\varphi_i\}_{i \in [n]} \subseteq \mathbb{F}^d$ satisfies

$$\mu(\{\varphi_i\}_{i \in [n]}) \geq \sqrt{\frac{n-d}{d(n-1)}}.$$ 

**Proof:** Put $\Phi = [\varphi_1 \cdots \varphi_n] \in \mathbb{F}^{d \times n}$. Then

$$0 \leq \|\Phi \Phi^* - \frac{n}{d} I\|_F^2 = \|\Phi^* \Phi\|_F^2 - \frac{n^2}{d} \leq n + n(n-1)\mu(\Phi)^2 - \frac{n^2}{d}.$$ 

Equality if and only if

- $|\langle \varphi_i, \varphi_j \rangle| = \text{const for } i \neq j$ “equiangular”
- $\Phi \Phi^* = \frac{n}{d} I$ “tight frame”

---

Tight frames

Overcomplete generalization of orthonormal bases:

\[
\begin{align*}
\begin{array}{c}
\text{Box} \\
\end{array} &= \begin{array}{c}
\text{Box} \\
\end{array} + \begin{array}{c}
\text{Box} \\
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{c}
\text{Box} \\
\end{array} &= \frac{2}{3} \left( \begin{array}{c}
\text{Box} \\
\end{array} + \begin{array}{c}
\text{Box} \\
\end{array} + \begin{array}{c}
\text{Box} \\
\end{array} \right)
\end{align*}
\]

Offers painless solution to least-squares problem \( y = \Phi^* x + \text{noise} \)

aka “eutactic stars”

---

Schläfli, Theorie der vielfachen Kontinuität, 1901
The real case is “easy”: Existence

**Strongly regular graph**
- every vertex has $k$ neighbors
- neighbors: $\lambda$ common neighbors
- otherwise: $\mu$ common neighbors

**Theorem**
Every real equiangular tight frame comes from a strongly regular graph.

Real ETFs $\leftrightarrow$ Brouwer’s table of SRGs

**Caveat:** Sometimes ETFs produce new SRGs (Tremain ETFs)

---
Waldron, Linear Algebra Appl., 2009  
The real case is “easy”: Non-existence

**Lemma**

Given a symmetric matrix with integer entries, if the eigenvalues have distinct multiplicities, then they are integer.

\[ \Lambda = \{0, \frac{n}{d}\} \quad \rightarrow \quad \Phi^* \Phi = I + \mu S \quad \leftarrow \quad \Lambda \subseteq 1 + \mu \mathbb{Z} \]

**Corollary**

Suppose \( n \neq d, 2d \). There exists an \( n \)-vector ETF in \( \mathbb{R}^d \) only if

\[ \sqrt{\frac{(n-d)(n-1)}{d}}, \quad \sqrt{\frac{d(n-1)}{n-d}} \in \mathbb{Z} \]

**Caveat:** Not sufficient by computer-assisted proof (76 in \( \mathbb{R}^{19} \))

Sustik, Tropp, Dhillon, Heath, Linear Algebra Appl., 2007
Azarija, Marc, arXiv:1509.05933
The complex case is hard

**Existence:** No analog to SRGs, so throw and see what sticks

- Group actions. abelian, Heisenberg–Weyl
- Generalize small examples. Steiner, Tremain, hyperovals
- Complexify real examples. DRACKNs, GQs, schemes
- Combinatorify algebraic examples. Kirkman

**Non-existence:** No analog to integrality conditions

**The Fickus Conjecture** (US$200/$100 prize for proof/disproof)

Consider $d, n - d$ and $n - 1$. There exists an $n$-vector ETF in $\mathbb{C}^d$ only if one of these quantities divides the product of the other two.

Holds for $(d, n) = (3, 8)$ by Gröbner basis calculation

---

Fickus, M., arXiv:1504.00253
M., Short Fat Matrices, 2015
Szöllősi, arXiv:1402.6429
Example: Abelian group action

The following are equivalent:

- $D$ is pseudorandom
- $|\hat{1}_D|^2 = \text{spike} + \text{const}$
- $D$ is a difference set

<table>
<thead>
<tr>
<th>$-$</th>
<th>1</th>
<th>2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Turyn, Pacific J. Math, 1965
Tao, Vu, Additive Combinatorics, 2006
Example: Abelian group action

$1_D$

$|\hat{1}_D|^2$

The following are equivalent:

- $D$ is pseudorandom
- $|\hat{1}_D|^2 = \text{spike} + \text{const}$
- $D$ is a difference set

\[
\begin{array}{c|cccc}
- & 1 & 2 & 4 \\
\hline
1 & 0 & 1 & 3 \\
2 & 6 & 0 & 2 \\
4 & 4 & 5 & 0 \\
\end{array}
\]

\[
\omega = e^{2\pi i/7}, \quad h = \text{diag}(\omega^1, \omega^2, \omega^4), \quad \mathbb{Z}/7\mathbb{Z} \cong \langle h \rangle \leq U(3)
\]

The orbit $\{g1\}_{g \in \langle h \rangle}$ is an ETF with $\langle g^k1, g^l1 \rangle = \hat{1}_D(l - k)$

Turyn, Pacific J. Math, 1965
Tao, Vu, Additive Combinatorics, 2006
Part II

Beyond the Welch bound
Welch revisited

Lift \( L: \mathbb{F}P^{d-1} \to \sqrt{1 - \frac{1}{d}} \cdot S^{D-1} \)

\[ \varphi \mapsto \varphi \varphi^* - \frac{1}{d} I \]

Then \( \langle L(\varphi), L(\psi) \rangle = |\langle \varphi, \psi \rangle|^2 - \frac{1}{d} \)

Theorem (Rankin’s simplex bound)
If \( n \leq D + 1 \), \( \{x_i\}_{i \in [n]} \subseteq S^{D-1} \) satisfies

\[ \max_{i,j \in [n], i \neq j} \langle x_i, x_j \rangle \geq -\frac{1}{n-1}. \]

Pull back Rankin \( \implies \) Welch bound

---

Conway, Hardin, Sloane, Experiment. Math., 1996
Bounds from lifting

**Theorem (Rankin’s orthoplex bound)**

If $n > D + 1$, $\{x_i\}_{i \in [n]} \subseteq S^{D-1}$ satisfies

$$\max_{i,j \in [n], i \neq j} \langle x_i, x_j \rangle \geq 0.$$ 

**Pull back Rankin:**

**Corollary**

If $n > D + 1$, $\{\varphi_i\}_{i \in [n]} \subseteq F^d$ satisfies

$$\mu(\{\varphi_i\}_{i \in [n]}) \geq \frac{1}{\sqrt{d}}.$$ 

Equality: $(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array})$, $\frac{1}{\sqrt{2}}(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array})$, $\frac{1}{\sqrt{2}}(\begin{array}{cc} 1 & 1 \\ i & -i \end{array})$

---

Conway, Hardin, Sloane, Experiment. Math., 1996
Builds from lifting

**Zonal kernel:** Any function $f : \mathbb{R} \to \mathbb{R}$ with lifting $L$ such that

$$\langle L(x), L(y) \rangle = f(|\langle x, y \rangle|^2) \quad \forall x, y \in \mathbb{F}_p^{d-1}$$

e.g., $f(t) = t - \frac{1}{d}$, $L(\varphi) = \varphi \varphi^* - \frac{1}{d} I$

**Lemma**

Let $f$ be a zonal kernel for $\mathbb{F}_p^{d-1}$ such that

$$f(1) = 1, \quad f(t) < -\frac{1}{n-1} \quad \forall t \in [0, B).$$

Then every $\{\varphi_i\}_{i \in [n]} \subseteq \mathbb{F}^d$ satisfies $\mu(\{\varphi_i\}_{i \in [n]}) \geq \sqrt{B}$.

**Proof:** Otherwise, contradict Rankin’s simplex bound. □

$f \in \text{cone(special polynomials)} \implies \text{Delsarte’s LP bound}$

---

Haas, Hammen, M., in preparation
Bounds from lifting

Important instances of Delsarte:

\( \deg(f) = 1: \) Delsarte \( \Rightarrow \) Welch

\( \deg(f) = 2: \) Delsarte \( \Rightarrow \) Levenstein

Theorem (Levenstein bound)

Suppose \( n \geq d \). Then every \( \{ \varphi_i \}_{i \in [n]} \subseteq \mathbb{F}^d \) satisfies

\[
\mu(\{ \varphi_i \}_{i \in [n]}) \geq \sqrt{\frac{n(\frac{1}{m+1}) - d(\frac{1}{md+1})}{(n-d)(\frac{1}{md+1})}}, \quad 2m = [\mathbb{F} : \mathbb{R}].
\]

Equality: 2-designs with \( |\langle \varphi_i, \varphi_j \rangle| \in \{0, \mu\} \) (cf. tight \( \Leftrightarrow \) 1-design)

Few packings known, all exhibit interesting symmetries (e.g., \( E_8 \))

---


Haas, Hammen, M., in preparation
How close? Welch is within a constant factor of optimal

How to remove the remaining gaps?
  ▶ Three-point generalization of Delsarte (still not tight)
  ▶ Tarski–Seidenberg projection (tight, but slow)

---

Sloane, Packings in Grassmannian Spaces, neilsloane.com/grass/
Cohn, Woo, J. Am. Math. Soc., 2012
Fickus, Jasper, M., arXiv:1707.01858
Tarski–Seidenberg projection

Tight bound $\iff$ minimizing over a **semialgebraic** set:

$$\left\{ (G, x) : \ \text{rank } G = d, \ \text{diag } G = 1, \ G \succeq 0, \ \mu(G)^2 \leq x \right\}$$

Idea: Project onto $x$ coordinate and minimize

**Tarski–Seidenberg Theorem**

The projection of a semialgebraic set is semialgebraic.

Algorithm: cylindrical algebraic decomposition (Mathematica)

Runtime is **double exponential** in number of variables

Bochnak, Coste, Roy, Real Algebraic Geometry, 1998
Tarski–Seidenberg projection

Half the variables in real case. Can we get fewer?

- **contact graph**: $i \leftrightarrow j$ whenever $|\langle \varphi_i, \varphi_j \rangle| = \mu$
- **$d$-secure graph**: There’s no way to reach the empty graph by iteratively deleting vertices of degree $< d$

Lemma

The contact graph of an optimal packing is $d$-secure.

Proof:

- If not $d$-secure, reach the empty graph by deleting $\{j_k\}_{k \in [n]}$
- Slightly move each $\varphi_{jk}$ toward $(\{\varphi_i\}_{i \in N(j_k)})^\perp$
- Iterating through $k$ decreases $\mu$
**Tarski–Seidenberg projection**

$d$-secure says more when $n$ is small, so take $n = d + 2$

**Lemma**

There are two minimal $d$-secure graphs of order $d + 2$:

- $K_{d+1} \cup \nu$
- complement of a maximum matching

Therefore, every optimal Gram matrix has one of two forms:

\[
\begin{bmatrix}
1 & \pm \mu & \pm \mu & x_1 \\
\pm \mu & 1 & \pm \mu & x_2 \\
\pm \mu & \pm \mu & 1 & x_3 \\
x_1 & x_2 & x_3 & 1
\end{bmatrix}
\]

or

\[
\begin{bmatrix}
1 & x_1 & \pm \mu & \pm \mu \\
x_1 & 1 & \pm \mu & \pm \mu \\
\pm \mu & \pm \mu & 1 & x_2 \\
\pm \mu & \pm \mu & x_2 & 1
\end{bmatrix}
\]

Given fixed sign pattern, each form has $\leq n$ variables

---

Fickus, Jasper, M., arXiv:1707.01858
Tarski–Seidenberg projection

Theorem
Every \( \{\varphi_i\}_{i \in [6]} \subseteq \mathbb{R}^4 \) satisfies
\[
\mu(\{\varphi_i\}_{i \in [6]}) \geq \frac{1}{3},
\]
and equality is achieved in Sloane’s online database.

Proof:
- Apply CAD to project onto \( \mu \) coordinate, take minimum
- Minimize over both forms and all sign patterns
- To avoid CAD queries, solve first form using its spectrum, reduce to 14 inequivalent sign patterns for the second form □

Open: \( (d, n) = (5, 7) \). How to speed up CAD?

Fickus, Jasper, M., arXiv:1707.01858
Sloane, Packings in Grassmannian Spaces, neilsloane.com/grass/
Part III

Zauner’s Conjecture
Maximal equiangular tight frames

Welch vs. Orthoplex: $n$-vector ETF in $\mathbb{C}^d$ requires $n \leq d^2$

ETF with $n = d^2$ is called maximal or SIC-POVM

Cornerstone object in theory of Quantum Bayesianism

---

**Zauner’s Conjecture**

For each $d \geq 2$, $\mathbb{C}^d$ admits a maximal ETF (with very specific structure).

Known to hold for finitely many $d$

---

Fuchs, Schack, Found. Phys., 2011


Recent progress on Zauner’s conjecture

**Heisenberg–Weyl group** $H$ generated by $T, M \in \mathcal{U}(\mathbb{C}^{\mathbb{Z}/d\mathbb{Z}})$

$$T \delta_j = \delta_{j+1}, \quad M \delta_j = e^{2\pi ij/d} \delta_j \quad (j \in \mathbb{Z}/d\mathbb{Z})$$

Then $\{U \varphi\}_{U \in H} = d^2$ vectors $\times$ all $d$th roots of unity

**Theorem**

Every $\varphi \in \mathbb{C}^{\mathbb{Z}/d\mathbb{Z}}$ satisfies

$$\left\lvert \sum_{j,k \in \mathbb{Z}/d\mathbb{Z}} \left( \sum_{l \in \mathbb{Z}/d\mathbb{Z}} \varphi(l) \varphi(j+l) \varphi(k+l) \varphi(j+k+l) \right) \right\rvert^2 \geq \frac{2}{d+1}$$

with equality precisely when $\{U \varphi\}_{U \in H}$ produces a maximal ETF.

Minimize LHS (non-convex!) $\Rightarrow$ numerical solutions for $d \leq 151$

---

Fuchs, Hoang, Stacey, arXiv:1703.07901
solutions available at www.physics.umb.edu/Research/QBism/solutions.html
Recent progress on Zauner’s conjecture

We want $\varphi \in \mathbb{C}^{\mathbb{Z}/d\mathbb{Z}}$ such that

$$\sum_{l \in \mathbb{Z}/d\mathbb{Z}} \varphi(l) \varphi(j + l) \varphi(k + l) \varphi(j + k + l) = \frac{\delta_0(j) + \delta_0(k)}{d+1}$$

Compute Gröbner basis and find real solutions (provided $d$ is small)

**Observation/Conjecture**

Entries of $\varphi \varphi^*$ lie in an abelian extension of $\mathbb{Q}(\sqrt{(d - 3)(d + 1)})$.

Chien’s program to find larger seed vectors:

1. Take a numerically approximated ETF seed vector
2. Locally optimize to obtain $\sim 10^4$ digits of precision
3. Apply conjecture to guess analytic expression
4. Verify success by symbolic computation

Appleby, Yadsan-Appleby, Zauner, Quantum Inf. Comput., 2013
Appleby, Chien, Flammia, Waldron, arXiv:1703.05981
Recent progress on Zauner’s conjecture

Coordinates are expressible by radicals, but not nicely:

Is there a shorter description?

M., Short Fat Matrices, 2017
Should we abandon Heisenberg–Weyl?

Hoggar’s ETF: Spin \((-1 + 2i, 1, 1, 1, 1, 1, 1, 1, 1)\) with HW over \((\mathbb{Z}/2\mathbb{Z})^3\)

Theorem

HW over \((\mathbb{Z}/2\mathbb{Z})^k\) produces a maximal ETF only if \(k \in \{1, 3\}\).

HW over other abelian groups? Numerics not promising

SmallGroups: When a group works, it gives a rotated HW ETF

Theorem

For \(d > 3\) prime, if any group produces a maximal ETF in \(\mathbb{C}^d\), then HW produces a rotated version of the same ETF.

______________________________

Godsil, Roy, European J. Combin., 2009
How to avoid being explicit?

I've been thinking about the equiangular lines (or SIC-POVM) conjecture, and my conclusion is that the best means of attack would be through some kind of fixed point theorem -- I'm thinking specifically of geometric fixed point theorems, like Brouwer's. So my (rather vague) questions are:

1) Is there some good survey article or classification for fixed point theorems?
2) Are there fixed-point theorems which are related to actions of groups on geometric spaces?
3) Has anybody tried this idea?

Added: In response to Joe's comment below, let me note that while the motivation is from quantum information theory, the equiangular lines conjecture is a purely classical geometry problem (see my comment below). The conjecture is really intriguing: numerical constructions of sets of equiangular lines have been found up to dimension 67, at which point the computer time required exceeded the patience of the investigators. However, only a handful of these numerical solutions have been shown to be rigorously correct by finding corresponding algebraic numbers. See this recent paper.

---

Shor, mathoverflow.net/questions/30894/fixed-point-theorems-and-equiangular-lines
How to avoid being explicit?

Relax to biangular tight frames

Consider $K = \langle T, e^{2\pi i/d} \cdot I \rangle \leq H$

Suppose there exist $\alpha, \beta \geq 0$ such that

$$|\langle \varphi, U\varphi \rangle| = \begin{cases} 
\alpha & \text{if } U \in K \setminus Z(H) \\
\beta & \text{if } U \in H \setminus K 
\end{cases}$$

Plot of all such $\varphi = (1, x + iy)$:
How to avoid being explicit?

Relax to \textbf{biangular} tight frames

Consider $K = \langle T, e^{2\pi i/d} \cdot I \rangle \leq H$

Suppose there exist $\alpha, \beta \geq 0$ such that

$$|\langle \varphi, U\varphi \rangle| = \begin{cases} \alpha & \text{if } U \in K \setminus Z(H) \\ \beta & \text{if } U \in H \setminus K \end{cases}$$

Plot of all such $\varphi = (1, x + iy)$:

\textbf{Surprise}: An ETF exists by the intermediate value theorem!

Does this generalize?
Provable relaxations?

Relaxation 1
Does there exist \((u_0, \ldots, u_{d-1}), (v_0, \ldots, v_{d-1}) \in \mathbb{C}^{\mathbb{Z}/d\mathbb{Z}}\) such that

\[
\sum_{l \in \mathbb{Z}/d\mathbb{Z}} u_l v_{j+l} v_{k+l} u_{j+k+l} = \frac{\delta_0(j) + \delta_0(k)}{d+1} \quad \forall j, k \in \mathbb{Z}/d\mathbb{Z}
\]

Relaxation 2
What is the smallest \(r\) for which there exists \(Z \succeq 0\) over \(\mathbb{C}^{\mathbb{Z}/d\mathbb{Z}}\) of rank \(r\) such that

\[
\sum_{l \in \mathbb{Z}/d\mathbb{Z}} Z_{l,j+l} Z_{j+k+l,k+l} = \frac{\delta_0(j) + \delta_0(k)}{d+1} \quad \forall j, k \in \mathbb{Z}/d\mathbb{Z}
\]
Open problems

- The Fickus conjecture
- Better coherence bounds
- Fast Tarski–Seidenberg projection
- Zauner’s conjecture
- Relaxations of Zauner’s conjecture
Questions?

Tables of the existence of equiangular tight frames
M. Fickus, D. G. Mixon
arXiv:1504.00253

The Levenstein bound for packings in projective spaces
J. I. Haas IV, N. Hammen, D. G. Mixon
SPIE 2017, to appear

Packings in real projective spaces
M. Fickus, J. Jasper, D. G. Mixon
arXiv:1707.01858

Also, google **short fat matrices** for my research blog