A step towards a constructive proof of Zauner's conjecture

Gene S. Kopp

Purdue University (now) / Lousiana State University (Autumn 2022)

Codes and Expansions (CoDex) Seminar
May 24, 2022

Disclaimer

This talk announces results from five forthcoming preprints.

- [K and Lagarias] Class field theory for orders in number fields
- [K and Lagarias] SICs and orders in number fields
- [K] Stark class invariants as limits of a ratio of q-Pochhammer symbols
- [Appleby, Flammia, and K] Ghost SICs and the Wigner function
- [Appleby, Flammia, and K] A constructive approach to Zauner's conjecture via the Stark conjectures

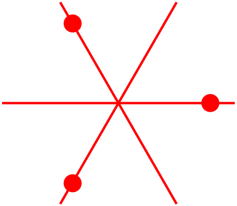
Titles, notation, and minor details may change.

Structure of this talk

- **Refining Zauner:** Historical and new refinements of Zauner's conjecture on the existance of SICs.
- **Ghostly constructions:** Indirect (conjectural/numerical) constructions of SICs/MEFFs via direct (conjectural/numerical) constructions of related "ghost" objects using number theory.
- **A challenge:** A new problem in frame theory (finding MEFFs), which you can work on without doing number theory!

Complex equiangular lines

You can draw three equiangular lines through the origin in $\mathbb{R}^2$:



Definition

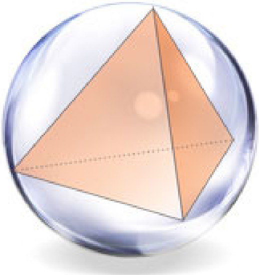
A finite set $S = \{\mathbb{C}v_1, \ldots, \mathbb{C}v_n\} \subset \mathbb{P}^{d-1}(\mathbb{C})$ with $\| v_j \| = 1$ is equiangular if $\big|\langle v_j, v_k\rangle\big| := \big|\overline{v}_j \cdot v_k\big| = \alpha$ for $j \neq k$.

In terms of the Hermitian projections onto the lines, equiangularity means $\mathrm{Tr}(\Pi_j \Pi_k) = \alpha^2$ for $j \neq k$.

Is it possible to find more than three equiangular lines in $\mathbb{C}^2$?

Complex equiangular lines

Yes! Take $S = \{[1 : \frac{1+i}{1+\sqrt{3}}], [1 : \frac{-1-i}{1+\sqrt{3}}], [\frac{1+i}{1+\sqrt{3}} : 1], [\frac{-1-i}{1+\sqrt{3}} : 1]\}$.



Proposition (Delsarte, Goethals, and Seidel; 1975)

Consider a set $S \subset \mathbb{P}^{d-1}(\mathbb{C})$ of n equiangular lines of common angle $\arccos(\alpha)$. Then, $n \leq d^2$. If $n = d^2$, then $\alpha = \frac{1}{\sqrt{d+1}}$.

SICs

Definition (SIC (symmetric informationally-complete positive operator-valued measure))

A SIC is a set $\{\Pi_1, \ldots, \Pi_{d^2}\} \subset M_{d\times d}(\mathbb{C})$ such that:

(1) $\Pi_j^2 = \Pi_j$

(2) $\mathrm{Tr}(\Pi_j \Pi_k) = \frac{1}{d+1}$ for $j \neq k$

(3) $\mathrm{rk}\, \Pi_j = 1$

(4) $\Pi_j^\dagger = \Pi_j$

A SIC is equivalent to:

- A maximal set of complex equiangular lines.
- A maximal complex equiangular tight frame (ETF).
- A minimal complex projective 2-design.

MEFFs

If we generalize from equiangular lines to equichordal subspaces, Delsarte, Goethals, and Seidel's upper bound of d^2 still holds.

Definition (MEFF (maximal equichordal fusion frames))

A rank r MEFF is a set $\{\Pi_1, \ldots, \Pi_{d^2}\} \subset M_{d\times d}(\mathbb{C})$ such that:

(1) $\Pi_j^2 = \Pi_j$

(2) $\operatorname{Tr}(\Pi_j \Pi_k) = \frac{r(dr-1)}{d^2-1}$ for $j \neq k$

(3) $\operatorname{rk} \Pi_j = r$

(4) $\Pi_j^\dagger = \Pi_j$

MEFFs are a special case of ECTFFs (equichordal tight fusion frames), which have also been called STFFs (symmetric tight fusion frames).

Weak Zauner

Conjecture (Zauner 1999)

There is at least one SIC in every dimension $d \geq 1$.

SICs are known in dimensions 1–53 and many other dimensions as large as $d = 1299$.

Numerical (probable) SICs are known in dimension 1–193 and various higher dimensions. Most exact and numerical solutions have been found by Grassl and Scott.

By studying known SICs, people (starting with Zauner himself) have formulated increasingly more precise refinements of this conjecture.

The Weyl-Heisenberg group

Let $\zeta = e^{\frac{2\pi i}{d}}$ and $\xi = -e^{\frac{\pi i}{d}}$. The Weyl-Heisenberg group (associated to $\mathbb{Z}/d\mathbb{Z}$) is the finite unitary matrix group

$$\mathrm{WH}(d) = \{\xi^k X^{p_1} Z^{p_2} : k, p_1, p_2 \in \mathbb{Z}\}, \text{ where}$$

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta & 0 & \cdots & 0 \\ 0 & 0 & \zeta^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{d-1} \end{pmatrix}.$$

A special set of coset representatives for WH(d) modulo its center is

$$D_{\mathbf{p}} = \xi^{p_1 p_2} X^{p_1} Z^{p_2}$$

for $\mathbf{p} = (p_1, p_2) \in (\mathbb{Z}/d\mathbb{Z})^2$.

Strong Zauner

Conjecture (Zauner 1999)

There is at least one SIC $\mathcal{S}$ in every dimension $d \geq 1$ satisfying the following properties:

(1) $\mathcal{S}$ is Weyl-Heisenberg covariant: $\mathcal{S} = \{D_{\mathbf{p}}^{-1}\Pi D_{\mathbf{p}}\}_{\mathbf{p}\in(\mathbb{Z}/d\mathbb{Z})^2}$ for some fiducial projector Π.

(2) $U_{\mathrm{Zau}}^{-1}\Pi U_{\mathrm{Zau}} = \Pi$ for the order three unitary Zauner matrix with entries

$$(U_{\mathrm{Zau}})_{k\ell} = \frac{1}{\sqrt{d}}\,\mathrm{e}\left(\frac{d-1}{24} + \frac{2k\ell + (d+1)\ell^2}{2d}\right).$$

Here, $\mathrm{e}(z) = e^{2\pi i z}$.

All but one of the known SICs satisfy (1) (up to unitary equivalence). Some WH SICs do not satsfy (2).

Equivalence of SICs

We can refine Zauner by specifying how many (Weyl-Heisenberg covariant) SICs there are each dimesion.

A SIC remains a SIC after a unitary “rotation” or an anti-unitary “reflection”—such transformations form the extended unitary group $\mathrm{EU}(d)$.
We consider two SICs $\{\Pi_j\}$ and $\{\Pi'_j\}$ to be equivalent if there is some $U \in \mathrm{EU}(d)$ such that $U^{-1}\Pi_j U = \Pi'_j$.

Proposition

WH SICs with fiducial projectors Π and Π' are equivalent if and only if $U^{-1}\Pi U = \Pi'$ for some $U \in \mathrm{PEC}(d)$, where

$$\mathrm{PEC}(d) = \{U \in \mathrm{EU}(d) : U^{-1}HU \in \mathrm{WH}(d) \text{ for all } H \in \mathrm{WH}(d)\}/\{\text{scalar}$$

is a finite group.

Counting SICs

Conjecture (K 2017)

Fix $d \neq 3$, and let $\Delta = (d+1)(d-3)$.Then,

$$|\text{WH-SIC}(d)/\operatorname{PEC}(d)| = |\mathcal{Q}(\Delta)/\operatorname{GL}_2(\mathbb{Z})|\,,$$

where $\mathcal{Q}(\Delta)/\operatorname{GL}_2(\mathbb{Z})$ is the set of twisted $\operatorname{GL}_2(\mathbb{Z})$-classes of binary quadratic forms of discriminant Δ.

The quantity $|\mathcal{Q}(\Delta)/\operatorname{GL}_2(\mathbb{Z})|$ is also...

- ...the number of $\operatorname{GL}_2(\mathbb{Z})$-conjugacy classes of elements of $\operatorname{SL}_2(\mathbb{Z})$ of trace $d-1$.
- ...a certain sum of class numbers of real quadratic rings.

Ray class groups and ray class fields

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $\mathfrak{m}$ be a ideal in $\mathcal{O}_K$, and let Σ be a subset of the real embeddings of K.

Definition (Weber 1897, Takagi 1920, Hasse 1926; ray class group modulo $(\mathfrak{m}, \Sigma)$)

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K) = \frac{\{\text{fractional ideals of } \mathcal{O}_K \text{ coprime to } \mathfrak{m}\}}{\{a\mathcal{O}_K \text{ s.t. } a \equiv 1 \pmod{\mathfrak{m}} \text{ and } \rho(a) > 0 \text{ for } \rho \in \Sigma\}}$$

Class field theory associates to $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)$ a ray class field $H_{\mathfrak{m},\Sigma}$, an abelian extension of K with Galois group $\mathrm{Gal}(H_{\mathfrak{m},\Sigma}/K) \cong \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)$. Varying $\mathfrak{m}$ and Σ, the ray class fields are cofinal among all abelian extensions of K.

Ray class groups and ray class fields of orders

Let K be a number field and $\mathcal{O}$ any order (full rank subring) of K. Let $\mathfrak{m}$ be a ideal in $\mathcal{O}$, and let Σ be a subset of the real embeddings of K.

Definition (Lagarias and K 2022+; ray class group of $\mathcal{O}$ modulo $(\mathfrak{m}, \Sigma)$)

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\{\text{invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}}{\{a\mathcal{O} \text{ s.t. } a \equiv 1 \pmod{\mathfrak{m}} \text{ and } \rho(a) > 0 \text{ for } \rho \in \Sigma\}}$$

We associate to $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ a ray class field (of an order) $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$, an abelian extension of K with Galois group $\mathrm{Gal}(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K) \cong \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$. This notion interpolates between ray class fields and “ring class fields.”

Fields of definition of SICs

Conjecture (Appleby, Flammia, McConnell, and Yard 2016; K and Lagarias 2022+)

Fix $d \neq 3$, and let $\Delta = (d+1)(d-3) = f^2\Delta_0$ with Δ_0 a fundamental discriminant. There is a bijective map

$$\begin{aligned} \mathcal{Q}(\Delta)/\operatorname{GL}_2(\mathbb{Z}) &\to \text{WH-SIC}(d)/\operatorname{PEC}(d) \\ [Q] &\mapsto \{D_{\mathbf{p}}^{-1}\Pi_Q D_{\mathbf{p}}\}_{\mathbf{p}\in(\mathbb{Z}/d\mathbb{Z})^2} \end{aligned}$$

having the following properties:

- If $Q(x,y) = \frac{f}{f'}(ax^2+bxy+cy^2)$ with $\gcd(a,b,c)=1$ and $f'|f$, then the entries of Π are in the ray class field $H^{\mathcal{O}}_{d\mathcal{O},\{\rho_1\}}$, where $\mathcal{O} = \mathbb{Z}\left[f'\frac{\Delta_0+\sqrt{\Delta_0}}{2}\right]$.
- The Π_Q associated to a fixed f' are Galois conjugate to each other.

Hilbert's 12th problem and explicit class field theory

Hilbert's 12th problem asks for an explicit construction of abelian extensions of number fields using special values of transcendental functions.

The abelian extensions of $\mathbb{Q}$ are generated by the values of $\mathrm{e}(z) = e^{2\pi iz}$ at rational numbers.

Those of an imaginary quadratic field K are generated by "complex multiplication (CM) values" of modular functions.

Both have geometric interpretations: Torsion points on the circle (for $\mathbb{Q}$) and on a CM elliptic curve (for K).

SICs hint at as-yet unknown geometry governing explict CFT for real quadratic fields, but only give a restricted set of class fields...

so we look at MEFFs!

Main conjecture for MEFFs (abstract form)

Conjecture (Appleby, Flammia, and K 2022+)

Fix $d \in \mathbb{N}$ and $0 < r < d$, $r \neq \frac{d\pm1}{2}$. Suppose $n = \frac{d^2-1}{r(d-r)} \in \mathbb{Z}$, and let $\Delta = n(n-4) = f^2\Delta_0$ with Δ_0 a fundamental discriminant. There is a bijective map

$$\mathcal{Q}(\Delta)/\operatorname{GL}_2(\mathbb{Z}) \to \text{WH-MEFF}(d,r)/\operatorname{PEC}(d)$$
$$[Q] \mapsto \{D_{\mathbf{p}}^{-1}\Pi_Q D_{\mathbf{p}}\}_{\mathbf{p}\in(\mathbb{Z}/d\mathbb{Z})^2}$$

having the following properties:

- If $Q(x,y) = \frac{f}{f'}(ax^2 + bxy + cy^2)$ with $\gcd(a,b,c) = 1$ and $f'|f$, then the entries of Π are in the ray class field $H^{\mathcal{O}}_{d\mathcal{O},\{\rho_1\}}$, where $\mathcal{O} = \mathbb{Z}\left[f'\frac{\Delta_0+\sqrt{\Delta_0}}{2}\right]$.
- The Π_Q associated to a fixed f' are Galois conjugate to each other.

Ghost SICs/MEFFs

Definition (Ghost MEFF)

A rank r ghost MEFF is a set $\{\Phi_1, \ldots, \Phi_{d^2}\} \subset M_{d\times d}(\mathbb{C})$ such that:

(1) $\Phi_j^2 = \Phi_j$

(2) $\mathrm{Tr}(\Phi_j\Phi_k) = \frac{r(dr-1)}{d^2-1}$ for $j \neq k$

(3) $\mathrm{rk}\,\Phi_j = r$

(4) $\Phi_j^\dagger = U_P\Phi_j$ (Parity-Hermitian) where

$$U_P = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

A rank 1 ghost MEFF is a ghost SIC.

Theorem (Appleby, Flammia, K, 2022+)

Assume the class field hypothesis: that the fiducial projectors of WH SICs have entries in $\mathbb{Q}(\sqrt{\Delta})^{\mathrm{ab}}$ with $\Delta = (d+1)(d-3)$. Then, there is a (non-canonical) one-to-one bijection between WH SICs and WH ghost SICs, given by a choice of Galois automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})^{\mathrm{ab}}/\mathbb{Q})$ such that $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$.

A straightforward analogue of this theoerm likely holds for WH MEFFs and WH ghost MEFFs.

The Shintani-Faddeev modular cocycle

Theorem (K 2022+)

Let $\mathbf{r} = (r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2$, and let

$$\varpi_{\mathbf{r}}(\tau) = \prod_{k=0}^{\infty} (1 - \mathrm{e}((k + p_1)\tau + p_2)) \text{ for } \mathrm{Re}(\tau) > 0.$$

$$\text{For } A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(N) = \left\{A \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\right\},$$

there exists a meromorphic function $\mathfrak{w}^{\mathbf{r}}_A(\tau)$ on the larger domain $\mathbb{C} \setminus \{\tau \in \mathbb{R} : c\tau + d \leq 0\}$ with the property that

$$\varpi_{\mathbf{r}}\left(\frac{a\tau + b}{c\tau + d}\right) = \mathfrak{w}^{\mathbf{r}}_A(\tau)\varpi_{\mathbf{r}}(\tau).$$

Definition (K 2022+)

The map $A \mapsto \mathfrak{w}^{\mathbf{r}}_A(\tau)$ is the Shintani-Faddeev modular cocycle.

Main conjecture for (ghost) MEFFs (constructive form)

Conjecture (Appleby, Flammia, and K 2022+)

Let $d, r \in \mathbb{N}$ with $0 < r < d$. Suppose that $n = \frac{d^2-1}{r(d-r)} \in \mathbb{Z}$, and let $\Delta = n(n-4)$. Let $Q(x, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}(\Delta)$, β a root of $Q(\beta, 1) = 0$. Let $B = \begin{pmatrix} \frac{1}{2}(-b+n-2) & -c \\ a & \frac{1}{2}(b-n+2) \end{pmatrix}$, and take the smallest positive power $A = B^k \in \Gamma(d)$. For $\mathbf{p} \in \mathbb{Z}^2/d\mathbb{Z}^2$, set

$$\nu_{\mathbf{p}} = \begin{cases} r, & \text{if } p_1 = p_2 = 0; \\ -n^{-1/2}\zeta_{24}^{\mu(A)}\, \mathrm{e}\left(\frac{r(d^2-1)Q(-p_2,p_1)}{2d}\right) \text{ש}_A^{d^{-1}\mathbf{p}}(\beta)\,, & \text{otherwise.} \end{cases}$$

($\mu(A) =$ Meyer-Rademacher invariant.) Let $\nu'_{\mathbf{p}} = \nu_{(rp_1,p_2)}$. Then,

$$\Phi = \frac{1}{d} \sum_{\mathbf{p}\in(\mathbb{Z}/d\mathbb{Z})^2} \nu'_{\mathbf{p}} D_{\mathbf{p}}$$

is a fiducial idempotent matrix of a rank r WH ghost MEFF.

The real multiplication (RM) values of the Shintani-Faddeev cocycle appearing in the conjecture are related to special values of (derivatives of) L-functions. The Stark conjectures predict that these values live in abelian extensions of $\mathbb{Q}(\sqrt{\Delta})$.

Theorem (Appleby, Flammia, and K 2022+)

Assume the Twisted Convolution Vanishing Conjecture, a particular family of identities for the RM values. Then the conjecture on the previous slide is true.

Under the further assumption of Tate's refinement of the real quadratic rank 1 Stark conjecture, the strong form of Zauner's conjecture holds.

Necromancy: Algorithmically generating SICs and MEFFs

- A ghost SIC/MEFF is generated to medium precision using *L*-functions.
- This precision is then boosted with Newton's method.
- A portion of the exact overlaps $\nu_{\mathbf{p}}$ are computed in a power basis using lattice basis reduction. (Computing them all will yeild an exact SIC/MEFF.)
- A Galois automorphism sending $\sqrt{\Delta} \mapsto -\sqrt{\Delta}$ is applied.
- The full numerical SIC/MEFF is reconstructed using low rank matrix reconstruction.

Some new computations: All 4 predicted WH SICs in dimension $d = 100$ (numerically); the first nontrivial example of a higher rank MEFF with $(d, r) = (11, 3)$.

Recall the definition of MEFFs from earlier in the talk.

Definition (MEFF (maximal equichordal fusion frames))

A rank r MEFF is a set $\{\Pi_1, \dots, \Pi_{d^2}\} \subset M_{d\times d}(\mathbb{C})$ such that:

(1) $\Pi_j^2 = \Pi_j$

(2) $\mathrm{Tr}(\Pi_j \Pi_k) = \frac{r(dr-1)}{d^2-1}$ for $j \neq k$

(3) $\mathrm{rk}\, \Pi_j = r$

(4) $\Pi_j^\dagger = \Pi_j$

Known families of MEFFs

Unlike SICs, MEFFs are known to exist in arbitrarily large dimension.

Proposition (Appleby, Bengtsson, Flammia, and Goyeneche 2019; Constrution of Wigner MEFFs)

For any $d \in \mathbb{N}$, the matrices

$$\Pi^{\pm} = \frac{1}{2}(I \pm U_P)$$

are fiducial projectors for WH MEFFs of rank $\frac{d\pm 1}{2}$.

As with SICs in dimension $d = 3$, there is expected to be a continuous family of WH MEFFs of rank $r = \frac{d\pm 1}{2}$, with the Wigner MEFF generalizing the Hasse SIC.

“Known” families of MEFFs

As per our main conjecture, we also “know” about WH MEFFs with parameters (d, r) whenever $n = \frac{d^2-1}{r(d-r)}$ is an integer (but can’t prove our construction works).

For $1 < r < \frac{d-1}{2}$, this happens when $(d, r) \in \{(11, 3), (19, 4), (29, 5), (29, 8), (41, 6), (55, 7), (71, 8), (71, 15), (76, 21), (89, 9), (109, 10), (131, 11), (139, 24), (155, 12), (181, 13), (199, 55), \ldots\}$.

There are infinitely many pairs for each ratio n but only finitely many of each rank r.

A challenge: Search for non-WH MEFFs

The Hoggar SIC is group covariant for the group $\mathrm{WH}(2) \otimes \mathrm{WH}(2) \otimes \mathrm{WH}(2)$, and it is currently the only known MEFF that isn't covariant for $\mathrm{WH}(d)$ for some d.

But (to my knowledge) no one has looked!

I encourage you to look for MEFFs that are covariant for other tensor products of Weyl-Heisenberg groups or for other groups.

Thank you!

Thank you for listening! Any questions?