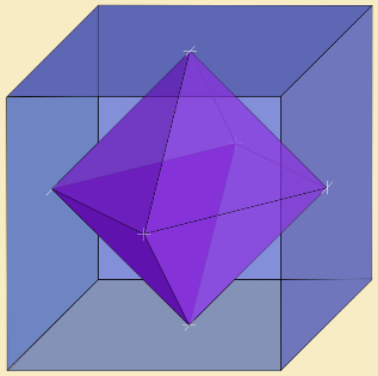
Tight 2-designs in complex projective spaces

Jon Yard
University of Waterloo
Institute for Quantum Computing
Department of Combinatorics & Optimization
Perimeter Institute for Theoretical Physics



Open Problems in Algebraic Combinatorics
May 3, 2021

Complex projective t-designs

The homogeneous degree-(t,t) polynomials $f \in \mathbb{C}[z,\bar{z}]_{t,t} = \mathbb{C}[z]_t \otimes \mathbb{C}[\bar{z}]_t$
define a space of functions on $\mathbb{CP}^{d-1}$:

$$\mathrm{Pol}_t\left(\mathbb{CP}^{d-1}\right) = \left\{ f([v]) = \frac{f\left(v, c(v)\right)}{\langle v, v\rangle^t} : f \in \mathbb{C}[z,\bar{z}]_{t,t} \right\}$$

Filtered algebra of polynomial functions is dense in $L^2\left(\mathbb{CP}^{d-1}\right)$:

$$\mathrm{Pol}\left(\mathbb{CP}^{d-1}\right) = \bigcup_{t\geq 0} \mathrm{Pol}_t\left(\mathbb{CP}^{d-1}\right) = \sum_{t\geq 0} \mathrm{Harm}_t(\mathbb{CP}^{d-1})$$

Where $\mathrm{Harm}_t(\mathbb{CP}^{d-1}) = \left\{ f \in \mathbb{C}[z,\bar{z}]_{t,t} : \sum_j \frac{d^2}{dz_j d\bar{z}_j} f(z,\bar{z}) = 0 \right\}$ is the harmonic polynomials

Definition: Given unit vectors $v_1, \ldots, v_n, \{[v_j]\} \subset \mathbb{CP}^{d-1}$ is a t-design if
$f([v_i]) = 0$ if for all $f \in \mathrm{Harm}_1\left(\mathbb{CP}^{d-1}\right) + \cdots + \mathrm{Harm}_t(\mathbb{CP}^{d-1})$

Linear programming bounds

How small can a 2-design be?

LP bound: If $\mathcal{D} \subset \mathbb{CP}^{d-1}$ is a 2-design, then $|\mathcal{D}| \geq \dim \mathrm{Pol}_1\left(\mathbb{CP}^{d-1}\right) = d^2$

A 2-design meeting this bound is therefore of minimal cardinality and called **tight**.

It is not hard to show in such a case that $\mathcal{D}$ is also a 1-distance set in this case, corresponding to a set of complex equiangular lines ("distance" = angle)

Generalizations:

- Higher t
- The other Compact Rank-One Symmetric Spaces (CROSSes) S^{d-1}, $\mathbb{RP}^{d-1}$, $\mathbb{HP}^{d-1}$, $\mathbb{OP}^2$

Complex equiangular lines

Suppose that $v_1, \ldots, v_n \in \mathbb{C}^d$ satisfy $\left|\langle v_i, v_j \rangle\right|^2 = \begin{cases} 1, i = j \\ \alpha, i \neq j \end{cases}$ for some $0 \leq \alpha < 1$.

Then $n \leq d^2$.

Proof: Let $P_i = v_i v_i^\dagger$ be the projection onto the complex line $\mathbb{C}v_i$ spanned by v_i.

Then $\det\left(\operatorname{Tr} P_i P_j\right) = \det\left|\langle v_i, v_j \rangle\right|^2 = \det\begin{pmatrix} 1 & \cdots & \alpha \\ \vdots & \ddots & \vdots \\ \alpha & \cdots & 1 \end{pmatrix} = (1-\alpha)^{n-1}(1+(n-1)\alpha) > 0.$

Therefore the P_i are linearly independent, so $n \leq \dim_{\mathbb{R}}(\mathrm{Herm}_d) = d^2$

(this is also an LP bound, cf. MUBs, which are 2-distance sets)

If $n = d^2$ is achieved, can show that $\alpha = \frac{1}{d+1}$.

Conjecture (Zauner): This bound is achieved for every d.

Some equivalent formulations

- Maximal sets of equiangular lines in $\mathbb{C}^d$
- Maximal sets of equidistant points in $\mathbb{CP}^{d-1}$ (w.r.t. Fubini-Study metric)
- Maximal equiangular tight frames (here tight refers to $t = 1$)
- Minimal 2-designs in $\mathbb{CP}^{d-1}$
- Regular simplex inscribed into set of density matrices
- Isometric embedding of $\ell_2^d \hookrightarrow \ell_4^{d^2}$
- Maximal volume simplex embedded in convex set of density matrices
- SIC-POVMs

SIC-POVM = Symmetric Informationally Complete POVM

In quantum information theory, the projections onto d^2 equiangular lines in $\mathbb{C}^d$ give rise to an optimal quantum measurement known as a SIC-POVM:

Definition: A *SIC-POVM* on $\mathbb{C}^d$ is a set of d^2 rank-1 projections $P_j \in \mathrm{Herm}_d(\mathbb{C})$ that is

- (*Symmetric*) $\mathrm{Tr}\, P_i P_j = \begin{cases} 1, & i = j \\ \frac{1}{d+1}, & i \neq j \end{cases}$
- (*Informationally Complete*) $\mathbb{R}P_1 + \mathbb{R}P_2 + \cdots + \mathbb{R}P_{d^2} = \mathrm{Herm}_d(\mathbb{C})$

Then $\sum_j P_j/d = I_d$, so $\{P_j/d\}$ is POVM with simple reconstruction rule:

$$\rho \mapsto \left\{ p(j) = \mathrm{Tr}\, \rho \frac{P_j}{d} \right\} \to \sum_j \frac{dp(j)+1}{d+1} P_j = \sum_j \frac{\mathrm{Tr}\rho P_j + 1}{d+1} P_j = \rho$$

Minimal complex projective 2-designs

Definition: Rank-1 projections $P_1, \ldots P_n$ form a complex-projective 2-design if

$$\frac{1}{n}\sum_{j=1}^{n} P_j \otimes P_j = \frac{2}{d^2+d} P_{sym}$$

Easy Theorem: any 2-design in $\mathbb{CP}^{d-1}$ requires at least $n \geq d^2$ and if this bound is achieved, they must be equiangular.

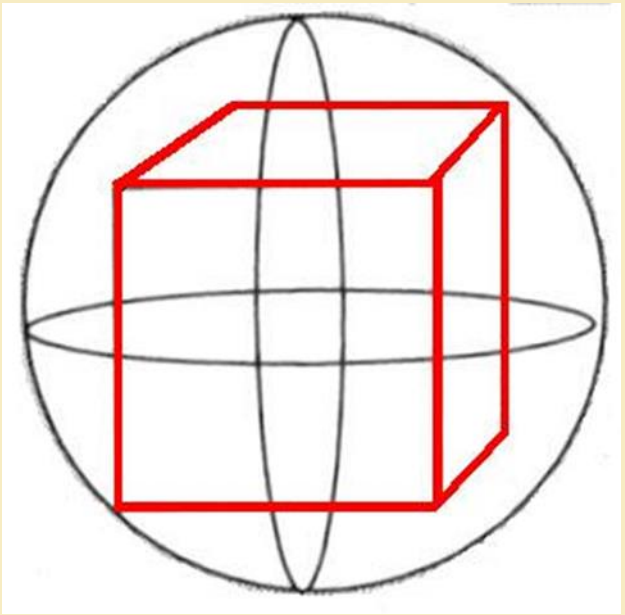
So SIC-POVMs are also *minimal* 2-designs.

Example: $d = 2$

$$\{\text{rank} - 1 \text{ projections on } \mathbb{C}^2\} = \mathbb{CP}^1 \simeq S^2$$

$$\frac{1}{2}\left(I + \frac{\pm X \pm Y \pm Z}{\sqrt{3}}\right)$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Orbits of Pauli group mod center acting by conjugation $(\mathbb{Z}/2)^2 \simeq \langle X, Z \rangle$/center

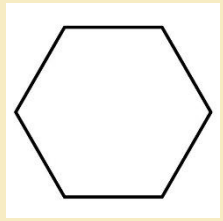
Each projector is eigenstate of order-3 subgroup of
qubit Clifford group = $N_{\mathrm{PU}_2}(\langle X, Z \rangle)$ = octahedral group $\simeq (\mathbb{Z}/2)^2 \rtimes \mathrm{SL}_2(2)$

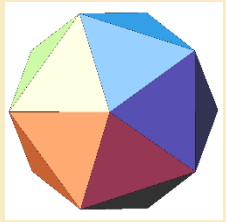
c.f. real equiangular lines - $\mathbb{RP}^{d-1}$

Over $\mathbb{R}$, analogous bound $n \leq \dim_{\mathbb{R}}(\mathrm{Sym_d}) = \frac{d^2+d}{2}$ rarely tight.

Tight $\Rightarrow \alpha = \frac{1}{\sqrt{d+2}} = \frac{1}{2m+1}$ if $d \geq 4$ (Gerzon).

d	2	3	4	5	6	$7-14$	$\cdots$	$23-41$	$\cdots$
n	**3**	**6**	6	10	16	**28**	$\cdots$	**276**	$\cdots$
$\frac{d^2+d}{2}$	**3**	**6**	10	15	21	**28** $-$ 105	$\cdots$	**276** $-$ 861	$\cdots$





$\mathbf{56}_{E_7}$ $\subset \Lambda_{24}$

Correspond to strongly regular graphs → explicit constructions

SIC-POVMs from finite Heisenberg group

$$1 \to U(1) \to \langle U(1), X, Z \rangle \to (\mathbb{Z}/d)^2 \to 0$$

where $X = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & \\ & & 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & & & \\ & \zeta_d & & \\ & & \ddots & \\ & & & \zeta_d^{d-1} \end{pmatrix}$.

Fixing a section $\Delta_j = (-\zeta_{2d})^{j_1 j_2} X^{j_1} Z^{j_2}$, $\Delta_j^\dagger = \Delta_{-j}$, $\Delta_j \Delta_k = (-\zeta_{2d})^{j_2 k_1 - j_1 k_2} \Delta_{j+k}$,
get projective representation $j \mapsto \Delta_j$ of $(\mathbb{Z}/d)^2$.
Call $v_0 \in \mathbb{C}^d$ a **fiducial vector** if (the projections onto) the $v_j = \Delta_j v_0$ form a SIC-POVM.

Zauner's weak conjecture: SIC-POVMs exist for every d
Zauner's strong conjecture: Fiducial vectors exist in every $\mathbb{C}^d$
So far, only 1 SIC-POVM known that is not a Heisenberg orbit (Hoggar – 3-qubit Pauli)

All Heisenberg SIC-POVMs in d=3

$$|\psi\rangle = |0\rangle + e^{i\theta}|2\rangle$$

$$\theta \in [0,2\pi)$$

Only case where there are infinitely many.

$d = 7$ example

There are 336 Heisenberg SIC-POVMs in $\mathbb{C}^7$. One is generated by

$$\left(\frac{j}{7}\right) = (0,1,1,-1,1,-1,-1) = \begin{cases} 0 & j = 0 \\ 1 & j \in (\mathbb{F}_7^\times)^2 \\ -1 & j \notin (\mathbb{F}_7^\times)^2 \end{cases}$$

$$|\psi\rangle = \sum_{j=0}^{6} \left(\frac{\sqrt{2\sqrt{2}-1}-1-\sqrt{2}}{2}\right)^{\left(\frac{j}{7}\right)} |j\rangle = |0\rangle - \frac{1+\sqrt{2}}{2}|\chi_1\rangle + \frac{\sqrt{2\sqrt{2}-1}}{2}|\chi_{-1}\rangle$$

$$|\chi_\pm\rangle = (0,1,1,\pm 1,1,\pm 1,\pm 1)^T$$

[Appleby ’07, Scott-Grassl ‘09, Y]

Similar example exists in dimension 19 (but it doesn’t generalize ☹).

The relevant number field $\mathbb{Q}\left(\sqrt{2\sqrt{2}-1}, \zeta_7\right)$ has **nonabelian** Galois group.

Algebraic numbers

```
Out[6]= Root[14 - 72 #1 + 25 #1^2 - 144 #1^3 - 88 #1^4 - 8 #1^5 + 62 #1^6 - 14 #1^8 + #1^10 &, 2]
```

A number α is **algebraic** if $f(\alpha) = 0$ for an integer polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad a_i \in \mathbb{Z}$$

If α, β are algebraic, then so is $\alpha + \beta, \alpha - \beta, \alpha\beta$, and if $\beta \neq 0$, then α/β.

Advantages:

Can compute with perfect precision.

Beautiful mathematics "under the hood", can take advantage of symmetries.

Examples:

$i = \sqrt{-1}$ satisifies $f(i) = 0$, where $f(x) = x^2 + 1$

$\sqrt{2}$ satisfies $f\left(\sqrt{2}\right) = 0$, where $f(x) = x^2 - 2$

$\zeta_d = e^{\frac{2\pi i}{d}}$ satisfies $f(\zeta_d) = 0$, where $f(x) = x^d - 1$

Number fields

Arithmetic with algebraic numbers gives other algebraic numbers, e.g.

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$
$$(a+bi)(c+di)=(ac\ -bd)+(ad+bc)i$$

If $\alpha_1,\dots,\alpha_m$ are algebraic, they generate a **number field** $F=\mathbb{Q}(\alpha_1,\dots,\alpha_m)$
$=$ all polynomials in the α_i with $\mathbb{Q}$ coefficients.

Examples

$\mathbb{Q}(i)=\ \{a+bi:a,b\in\mathbb{Q}\}$ (Gaussian numbers)

$\mathbb{Q}\left(\sqrt{5}\right)=\{a+b\sqrt{5}:a,b\in\mathbb{Q}\}$ (real quadratic field)

$\mathbb{Q}(\zeta_d)=\left\{a_0+a_1\zeta_d+\cdots+a_{d-2}\zeta_d^{d-2}\right\}$ (cyclotomic numbers)

Normal extensions

If K is a number field and $\alpha_1, \ldots, \alpha_m$ are **all** of the roots of a polynomial

they generate a number field $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_m) \supset K$ called **Galois**, or **normal** over K.

In such cases, there is a group $\mathrm{Gal}(F/K)$ of symmetries of *F* that fix *K* elementwise, satisfyting $|\mathrm{Gal}(FK)| = [F:K] = \dim_K F$.

Examples

$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \text{complex conjugation} \rangle \simeq \mathbb{Z}/2$

$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{5}\right)/\mathbb{Q}\right) = \langle \sqrt{5} \mapsto -\sqrt{5} \rangle \simeq \mathbb{Z}/2$

$\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) = \{\zeta_d \mapsto \zeta_d^a : \gcd(a,d) = 1\} \simeq (\mathbb{Z}/d)^\times$

Explicit constructions (proofs of strong Zauner)

Explicit constructions of fiducials in dimensions $d = 2 - 21, 24, 28, 30, 35, 39, 48, 124, 323, 844, 1299$ [Scott-Grassl, Appleby-Appleby-Zauner, Appleby-Chein-Flammia-Waldron, Scott, Scott-Grassl].

Numerical (inexact) fiducials for $d = 2, 4 - 151, 168, 172, 228, 259, 844, 1299$ (not a proof)

Exact solutions constitute computer-assisted existence proofs over number fields of degrees into the 10000s. What sort of number fields?

Conjecture: Appleby-Appleby-Zauner: Every fiducial is defined over an abelian extension F/K of the real quadratic number field $K = \mathbb{Q}\left(\sqrt{(d-3)(d+1)}\right)$.

Conjecture: Appleby-Flammia-McConnell-Yard: The smallest degree extension over which fiducials are defined is the ray class field of K with conductor $(d')\infty$, where d' is d if d odd and $2d$ if d is even. Further refined by Kopp to give all the fields via "ring-ray class fields".

Harmonic invariant characterization

Theorem: Given a group G acting on $\mathbb{CP}^{d-1}$, $G \cdot [v_0]$ is a t-design iff $f([v_i]) = 0$ if for all $f \in \mathrm{Harm}_1\left(\mathbb{CP}^{d-1}\right)^G + \cdots + \mathrm{Harm}_t\left(\mathbb{CP}^{d-1}\right)^G$
Proof: straightforward – generalizes result of Sobolev for S^2 from 60s.

Corollary: $v_0 \in \mathbb{C}^d$ is a fiducial iff $f([v_i]) = 0$ if for all $f \in \mathrm{Harm}_2\left(\mathbb{CP}^{d-1}\right)^{(\mathbb{Z}/d)^2}$.

Some observations:

- $\mathrm{Harm}_1\left(\mathbb{CP}^{d-1}\right)^{(\mathbb{Z}/d)^2} = 0$
- $\dim \mathrm{Harm}_2\left(\mathbb{CP}^{d-1}\right)^{(\mathbb{Z}/d)^2} = \left|\{f_{ij}(z, \bar{z})\}\right| - 1 = \begin{cases} \frac{(d+3)(d-1)}{4}, d \text{ odd} \\ \frac{(d+2)(d-2)}{4}, d \text{ even} \end{cases}$
- $\dim \mathrm{Harm}_2(\mathbb{CP}^{d-1}) = \frac{d^2(d+3)(d-1)}{4}$

Equations for fiducial vectors

A conjecture (folklore):

0-dimensional real projective variety (1-dimensional if $d = 3$)

$$\left\{ f_{ij}(z,\bar{z}) = \sum_k z_k \bar{z}_{k+i} \bar{z}_{k+j} z_{k+i+j} - \frac{\delta_i + \delta_j}{d+1} \|z\|_2^4, \bar{z}_i = c(z_i) \colon i,j = 0,\dots,d-1 \right\} \subset \mathbb{CP}^{d-1}$$

Conjecture (Y'18): The *complex* projective subvariety

$$\left\{ f_{ij}(z,\bar{z}) = \sum_k z_k \bar{z}_{k+i} \bar{z}_{k+j} z_{k+i+j} - \frac{\delta_i + \delta_j}{d+1} \|z\|_2^4 : i,j = 0,\dots,d-1 \right\} \subset \mathbb{CP}^{d-1} \times_{\mathbb{C}} \mathbb{CP}^{d-1}$$

is still 0-dimensional if $d \neq 3$ (and 1-dimensional if $d = 3$) (checked $d \leq 7$ in Magma).

Conjecture (Y): The $d \neq 3$ fiducials themselves form a projective variety defined over

$$K = \mathbb{Q}\left(\sqrt{(d-3)(d+1)}\right)$$

Quadratic forms on matrices

Let $V = \mathbb{C}^d$ and consider the space of quadratic forms on $\mathrm{End}(V)$:

$$Q(X) = \mathrm{Tr}(X \otimes X)A, \qquad A \in \mathrm{Sym}^2\big(\mathrm{End}(V)\big) \subset \mathrm{End}(V) \otimes \mathrm{End}(V)$$

Under action of $\mathrm{GL}(V)$, $g \cdot A = (g \otimes g)A(g \otimes g)^\dagger$, decomposes into irreps:

$$\mathrm{Sym}^2\big(\mathrm{End}(V)\big) \simeq_{\mathrm{GL}(d)} \underset{\mathrm{Pol}_2(\mathbb{CP}^{d-1})}{\mathrm{End}\big(\mathrm{Sym}^2(V)\big)} + \underset{\{2\times 2 \text{ minors}\}}{\mathrm{End}\big(\Lambda^2(V)\big)}$$

Further decomposes upon restriction to $U(V)$:

$$\mathrm{Sym}^2\big(\mathrm{End}(V)\big) \simeq_{U(V)} \underset{\mathrm{Harm}_2}{\mathrm{Sym}^{2,2}(V)} + \underset{\mathrm{Harm}_1}{\mathrm{Sym}^{1,1}(V)} + \underset{\mathrm{Harm}_0}{\mathbb{C}P_+} \quad + \quad \Lambda^{2,2}(V) + \Lambda^{1,1}(V) + \mathbb{C}P_-$$

$$d^4 = \quad \left(\frac{d^2(d+3)(d-1)}{4} + (d-1) \quad + \quad 1\right) + \left(\frac{\boldsymbol{d^2(d-3)(d+1)}}{\boldsymbol{4}} + (d-1) + 1\right)$$

Generalized Clifford group (Weil representation)

Observation: Every fiducial is stabilized by an abelian subgroup of the projective generalized Clifford group $\mathrm{Aut}_{\mathbb{C}}(H)$ with order divisible by 3, where

$$1 \to U(1) \to H = \langle U(1), X, Z \rangle \to (\mathbb{Z}/d)^2 \to 0$$

Is a finite Heisenberg group. Then

$\mathrm{Aut}_{\mathbb{C}}(H) = \{$automorphisms of H fixing the center$\}$ sits in an extension

$$0 \to (\mathbb{Z}/d)^2 \to \mathrm{Aut}_{\mathbb{C}}(H) \to \mathrm{SL}_2(d) \to 1$$

That splits if doesn't divide d: $\mathrm{Aut}_{\mathbb{C}}(H) \simeq (\mathbb{Z}/d)^2 \rtimes \mathrm{SL}_2(\mathrm{d})$.
Otherwise a quotient $(\mathbb{Z}/d)^2 \rtimes \mathrm{SL}_2(\mathbb{Z}/2\mathrm{d}) \to \mathrm{Aut}_{\mathbb{C}}(H)$ by order-8 subgroup.

When d is not 3 mod 9, each SIC-POVM has a fiducial with stabilizer in $\mathrm{SL}_2(d')$
The bigger this stabilizer, the smaller the field (observed, but we can now explain)

Numerical “experimental” data

[Scott & Grassl 2009, Scott ’17]

$S =$ stabilizer in

$$\mathrm{SL}_2(d) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in (\mathbb{Z}/d)^{2\times 2} : ad - bc = 1 \right\}$$

How to e.g. explain the orders of the stabilizers?

(Much) more algebraic structure can be inferred from the known **exact** contructions in

$$d = 2 - 21{,}24,\ 28,\ 30,\ 31,\ 35,\ 37,\ 39,\ 43,\ 48{,}124,\ 323,844,1299$$

Why these “random” examples? Look at stabilizers.

d	#	|S|
2	1	6
3	∞	6
	1	12
	1	48
4	1	6
5	1	3
6	1	3
7	1	3
	1	6
8	1	3
	1	12
9	2	3
10	1	3
11	3	3
12	1	3
	1	6
13	2	3
14	2	3
15	3	3
	1	6
16	2	3
17	3	3
18	2	3
19	3	3
	1	6
	1	18
20	2	3
21	4	3
	1	3
22	1	3
23	6	3
24	2	3
	1	6
25	2	3
26	4	3
27	6	3
28	2	3
	1	6
29	4	3
30	3	3
	1	3
31	7	3
32	2	3
33	4	3
34	2	3
35	8	3
	1	6
	1	12
36	4	3
37	4	3
38	4	3
39	6	3
	2	3
	2	6
40	2	3
41	8	3
42	4	3
43	6	3
44	6	3
45	4	3
46	3	3
47	8	3
48	4	3
	1	3
	1	6
	1	24
49	7	3
50	2	3
51	14	3
52	3	3
	1	6
53	9	3
	1	9
54	4	3
55	6	3
56	6	3
57	6	3
	2	3
58	4	3
59	12	3
60	4	3
61	6	3
62	5	3
63	14	3
	2	6
64	4	3
65	8	3
66	6	3
	3	3
67	7	3
	2	6
68	4	3
69	8	3
70	5	3
71	18	3
72	4	3
73	4	3
74	7	3
75	12	3
	3	3
76	6	3
77	8	3
78	7	3
79	14	3
80	8	3
	1	6
81	12	3
82	3	3
83	16	3
84	6	3
	2	3
	2	6
85	4	3
86	10	3
87	12	3
88	4	3
89	10	3
90	4	3
91-121	≥ 1	≥ 3
99	≥ 3	≥ 6
111	≥ 1	≥ 9
120	≥ 1	≥ 6
	≥ 1	≥ 6
124	≥ 1	≥ 6
143	≥ 1	≥ 6
147	≥ 1	≥ 6
168	≥ 1	≥ 6
172	≥ 1	≥ 6
195	≥ 1	≥ 6
199	≥ 1	≥ 9
228	≥ 1	≥ 6
259	≥ 1	≥ 6
323	≥ 1	≥ 9

Algebraic integers

Some algebraic numbers are analogous to integers:

$$f(\alpha) = 0, \qquad f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

(leading coefficient of f is 1).

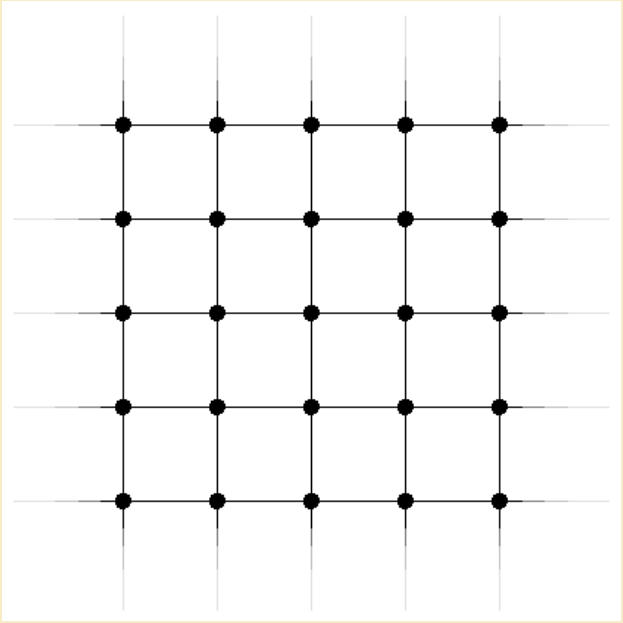
The integers of a number field generalize the relationship between $\mathbb{Z} \subset \mathbb{Q}$:

Examples

$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (Gaussian numbers)

$\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \{a + b\frac{1+\sqrt{5}}{2} : a, b \in \mathbb{Z}\}$ (real quadratic integers)

$\mathcal{O}_{\mathbb{Q}(\zeta_d)} = \mathbb{Z}[\zeta_d] = \{a_0 + a_1\zeta_d + \cdots + a_{d-2}\zeta_d^{d-2} : a_i \in \mathbb{Z}\}$
(cyclotomic integers)



Invertible algebraic integers = units

The **unit group** consists of the invertible algebraic integers:

$$\mathbb{Z}^\times = \{1, -1\}$$

$$\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$$

$$\mathbb{Z}[\zeta_d]^\times = \{\pm 1, \pm\zeta_d, \ldots \pm \zeta_d^{d-1}\}$$

$$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]^\times = \pm\left\{\left(\frac{1+\sqrt{5}}{2}\right)^a : a \in \mathbb{Z}\right\} \simeq \mathbb{Z} \times \mathbb{Z}/2$$

Note that the last one is infinite, in contrast to the others.

Order of the stabilizer

Suppose $D \equiv 0,1 \bmod 4$. Then $D = f^2 D_0$ where D_0 is a fundamental discriminant.
Then $\mathcal{O}_D = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right] \subset \mathbb{Q}(\sqrt{D})$ is the quadratic order of discriminant D.

Let $D = (d-3)(d+1)$. Then to each fiducial in dimension d, its symmetries are governed by the arithmetic of some **quadratic order**

$$\mathcal{O}_D \subset \mathcal{O} \subset \mathcal{O}_{D_0} = \mathcal{O}_K.$$

Let u_+ generate the totally positive units in $\mathcal{O}^\times$ and assume further that $\mathcal{O} = \mathcal{O}_K$ (minimal case)
Then $d = u_+^r + u_+^{-r} + 1$ and we conjecture that the order of the stabilizer subgroup equals the order of the fundamental unit u_f mod d, which is $3r$. Furthermore, if $u_f = u_+$ (i.e. if the narrow class number of K equals the class number), then each fiducial is stabilized by an antiunitary as well.

Underlying structure of SIC-POVMs

ACTA ARITHMETICA
Online First version

Generating ray class fields of real quadratic fields via complex equiangular lines

by

Marcus Appleby (Sydney), Steven Flammia (Sydney),
Gary McConnell (London) and Jon Yard (Waterloo, ON)

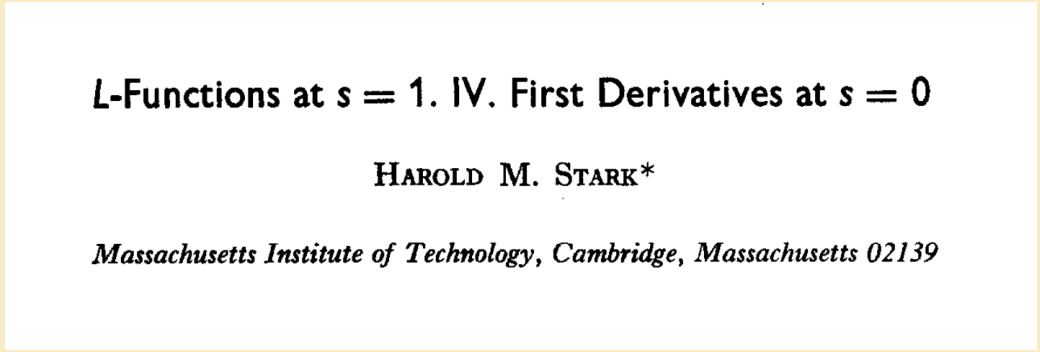
We found that certain aspects of the solutions are controlled by arithmetic in the real quadratic field $K = \mathbb{Q}(\sqrt{D})$, where $D = (d-3)(d+1)$.
For example, for every d with $D = 5$, there is an $r \in \mathbb{N}$ such that

$$d = 1 + \left(\frac{1+\sqrt{5}}{2}\right)^{2r} + \left(\frac{1+\sqrt{5}}{2}\right)^{-2r} = 4, 8, 19, 48, 124, 323, 844^{*}$$

And the order of the unitary stabilizer is $3r$.
We (AFMY + Kopp) now have precise ansatz for the relevant number fields using CFT.
Immediate goal: Use this structure to prove existence for all d (or at least infinitely many).

Stark conjectures

The overlaps are famously yet to be proven to exist…



L-Functions at $s = 1$. IV. First Derivatives at $s = 0$

HAROLD M. STARK*

Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

See Gene Kopp's recent papers

Towards an existence proof

Several ways to make our lives much easier:
Assume d = odd prime, then generalized Clifford group becomes simpler.

In this case, structure of fiducials depends on d mod 3.

Simplify number theory: restrict to primes $d \equiv 1$ mod 3 (108 such less than a million).

In certain of these cases, the number theory is even easier (class number of K is 1)

$$7, 19, 67, 199, 787, 2707, 4099, \mathbf{5779}, 19603, 132499$$

Hard open problem: prove this list is infinite (old open problem in number theory)

Conjecture (Scott): If $d = 4m^2 + 3$ expect real fiducials to exist (reduction in # variables)
The primes above have this property. Are there infinitely many such primes?

Thanks!

Harmonic tori?

Algebraic geometry?

Minimal triangulations?