# Codes and Expansions (CodEx) Seminar

# Computing SIC-POVMs using Permutation Symmetries and Stark Units

Markus Grassl

International Centre for Theory of Quantum Technologies
University of Gdansk
markus.grassl@ug.edu.pl
sicpovm.markus-grassl.de

26 October 2021

in collaboration with
*Marcus Appleby, Ingemar Bengtsson, Michael Harrison, Gary McConnell*

additional support by the Max Planck Institute for the Science of Light, Erlangen, and MPG

European Funds Smart Growth
Republic of Poland
FNP Foundation for Polish Science
European Union European Regional Development Fund

# Overview

- Zauner's conjecture
- numerical search
- symmetries & Fibonacci-Lucas SIC-POVMs
- exact solutions from numerical solutions
  - using overlaps
  - using permutations
- numerical and exact solutions from Stark units
- conclusions & outlook

# A Simple to State Problem

Are there $d^2$ vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{d^2} \in \mathbb{C}^d$ in the complex vector space of dimension $d$ such that:

(i) $\langle \boldsymbol{v}_j | \boldsymbol{v}_j \rangle = 1$ for $j = 1, \ldots, d^2$

(ii) $|\langle \boldsymbol{v}_j | \boldsymbol{v}_k \rangle|^2 = \dfrac{1}{d+1}$ for $1 \le j < k \le d^2$

The vectors $\boldsymbol{v}_j$ form an equiangular tight frame/finite unit norm tight frame.

# A Simple to State Problem

Are there $d^2$ vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{d^2} \in \mathbb{C}^d$ in the complex vector space of dimension $d$ such that:

$$\begin{array}{lll} \text{(i)} & \langle \boldsymbol{v}_j | \boldsymbol{v}_j \rangle = 1 & \text{for } j = 1, \ldots, d^2 \\ \text{(ii)} & |\langle \boldsymbol{v}_j | \boldsymbol{v}_k \rangle|^2 = \dfrac{1}{d+1} & \text{for } 1 \leq j < k \leq d^2 \end{array}$$

The vectors $\boldsymbol{v}_j$ form an equiangular tight frame/finite unit norm tight frame.

All solutions form a real algebraic variety, using $2d$ real variables per vector

$$\boldsymbol{v}_j = (a_{j,1} + ib_{j,1}, a_{j,2} + ib_{j,2}, \ldots, a_{j,d} + ib_{j,d})^T \qquad (i = \sqrt{-1})$$

$2d^3$ variables, $d^2$ equations (i) of degree $2$ and $\binom{d^2}{2}$ equations (ii) of degree $4$.

# Weyl-Heisenberg Group

- generators: $$H_d := \langle X, Z \rangle$$

  where $X := \sum_{j=0}^{d-1} |j+1\rangle\langle j|$ and $Z := \sum_{j=0}^{d-1} \omega_d^j |j\rangle\langle j|$

  $$(\omega_d := \exp(2\pi i/d))$$

- relations:

$$\left(\omega_d^c X^a Z^b\right)\left(\omega_d^{c'} X^{a'} Z^{b'}\right) = \omega_d^{a'b-b'a}\left(\omega_d^{c'} X^{a'} Z^{b'}\right)\left(\omega_d^c X^a Z^b\right)$$

- basis:

$$H_d/\zeta(H_d) = \left\{X^a Z^b \colon a, b \in \{0, \ldots, d-1\}\right\} \cong \mathbb{Z}_d \times \mathbb{Z}_d$$

  trace-orthogonal basis of all $d \times d$ matrices

# Constructing SIC-POVMs

**Ansatz:**

SIC-POVM that is the orbit under the Weyl-Heisenberg group $H_d$, i. e.,

$$\begin{aligned} |\boldsymbol{v}^{(a,b)}\rangle &:= X^a Z^b |\boldsymbol{v}^{(0,0)}\rangle \\ |\langle \boldsymbol{v}^{(a,b)}|\boldsymbol{v}^{(a',b')}\rangle|^2 &= \begin{cases} 1 & \text{for } (a,b) = (a',b'), \\ 1/(d+1) & \text{for } (a,b) \neq (a',b') \end{cases} \end{aligned}$$

$$|\boldsymbol{v}^{(0,0)}\rangle = \sum_{j=0}^{d-1} (x_{2j} + i x_{2j+1}) |j\rangle,$$

($x_0, \ldots, x_{2d-1}$ are real variables, $x_1 = 0$)

$\Longrightarrow$ we have to find only one *fiducial* vector $|\boldsymbol{v}^{(0,0)}\rangle$ instead of $d^2$ vectors

$\Longrightarrow$ polynomial equations with $2d-1$ variables, but already quite complicated for $d = 6$

# Jacobi Group (or Clifford Group)

- automorphism group of the Weyl-Heisenberg group $H_d$, i. e.

$$\forall T \in J_d : T^\dagger H_d T = H_d$$

- the action of $J_d$ on $H_d$ modulo phases corresponds to the symplectic group $\mathrm{SL}(2,\mathbb{Z}_d)$, i. e.

$$T^\dagger X^a Z^b T = \omega_d^c X^{a'} Z^{b'} \qquad \text{where } \begin{pmatrix} a' \\ b' \end{pmatrix} = \tilde{T} \begin{pmatrix} a \\ b \end{pmatrix},\ \tilde{T} \in \mathrm{SL}(2,\mathbb{Z}_d)$$

$\Longrightarrow$ homomorphism $J_d \to \mathrm{SL}(2,\mathbb{Z}_d)$

- additionally: complex conjugation (anti-unitary)

$$X^a Z^b \mapsto X^a Z^{-b} \qquad \text{corresponding to } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

# Zauner's Conjecture

[G. Zauner, Dissertation, Universität Wien, 1999]

**Conjecture:**
For every dimension $d \geq 2$ there exists a SIC-POVM whose elements are the orbit of a rank-one operator $E_0$ under the Weyl-Heisenberg group $H_d$.
What is more, $E_0$ commutes with an element $S$ of the Jacobi group $J_d$.
The action of $S$ on $H_d$ modulo the center has order three.

support for this conjecture (to date):

- numerical solutions for all dimensions $d \leq 193$, plus a few more
- exact algebraic solutions for some dimensions (see below)

one of the prize problems in
[Paweł Horodecki, Łukasz Rudnicki, Karol Życzkowski, Five open problems in quantum information, arXiv:2002.03233]

# Numerical Search for SIC-POVMs

- "second frame potential" for $2$-designs

$$\sum_{i,j=1}^{d^2} |\langle v^{(i)} \otimes v^{(i)} | v^{(j)} \otimes v^{(j)} \rangle|^2 = \sum_{i,j=1}^{d^2} |\langle v^{(i)} | v^{(j)} \rangle|^4 = d^2 \sum_{a,b=1}^{d} |\langle \psi | X^a Z^b | \psi \rangle|^4$$

- for any state $|\psi\rangle \in \mathbb{C}^d$

$$\begin{aligned} f(|\psi\rangle) &= \sum_{j,k=1}^{d} \Big| \sum_{\ell=1}^{d} \langle \psi | j+\ell \rangle \langle \ell | \psi \rangle \langle \psi | k+\ell \rangle \langle j+k+\ell | \psi \rangle \Big|^2 \\ &= \sum_{j,k=1}^{d} \Big| \underbrace{\sum_{\ell=1}^{d} \overline{\psi}_{j+\ell}\, \psi_\ell\, \overline{\psi}_{k+\ell}\, \psi_{j+k+\ell}}_{=:G(j,k)} \Big|^2 \qquad \geq \frac{2}{d+1} \end{aligned}$$

with equality iff $|\psi\rangle$ is a fiducial vector for a Weyl-Heisenberg SIC-POVM

- gradient descent to minimize $f(|\psi\rangle)$, subject to unit norm

# Numerical Search for SIC-POVMs

- for any state $|\psi\rangle \in \mathbb{C}^d$

$$f(|\psi\rangle) = \sum_{j,k=1}^{d} \left| \sum_{\ell=1}^{d} \overline{\psi}_{j+\ell}\, \psi_\ell\, \overline{\psi}_{k+\ell}\, \psi_{j+k+\ell} \right|^2 \geq \frac{2}{d+1}$$

  with equality iff $|\psi\rangle$ is a fiducial vector for a Weyl-Heisenberg SIC-POVM

- gradient descent to minimize $f(|\psi\rangle)$, subject to unit norm

- use $F(\vec{x}) = f\left(\frac{P\vec{x}}{\|P\vec{x}\|}\right)$ for an arbitrary vector $\vec{x} \in \mathbb{C}^d$, where $P$ is the projection onto a subspace (prescribed symmetry)

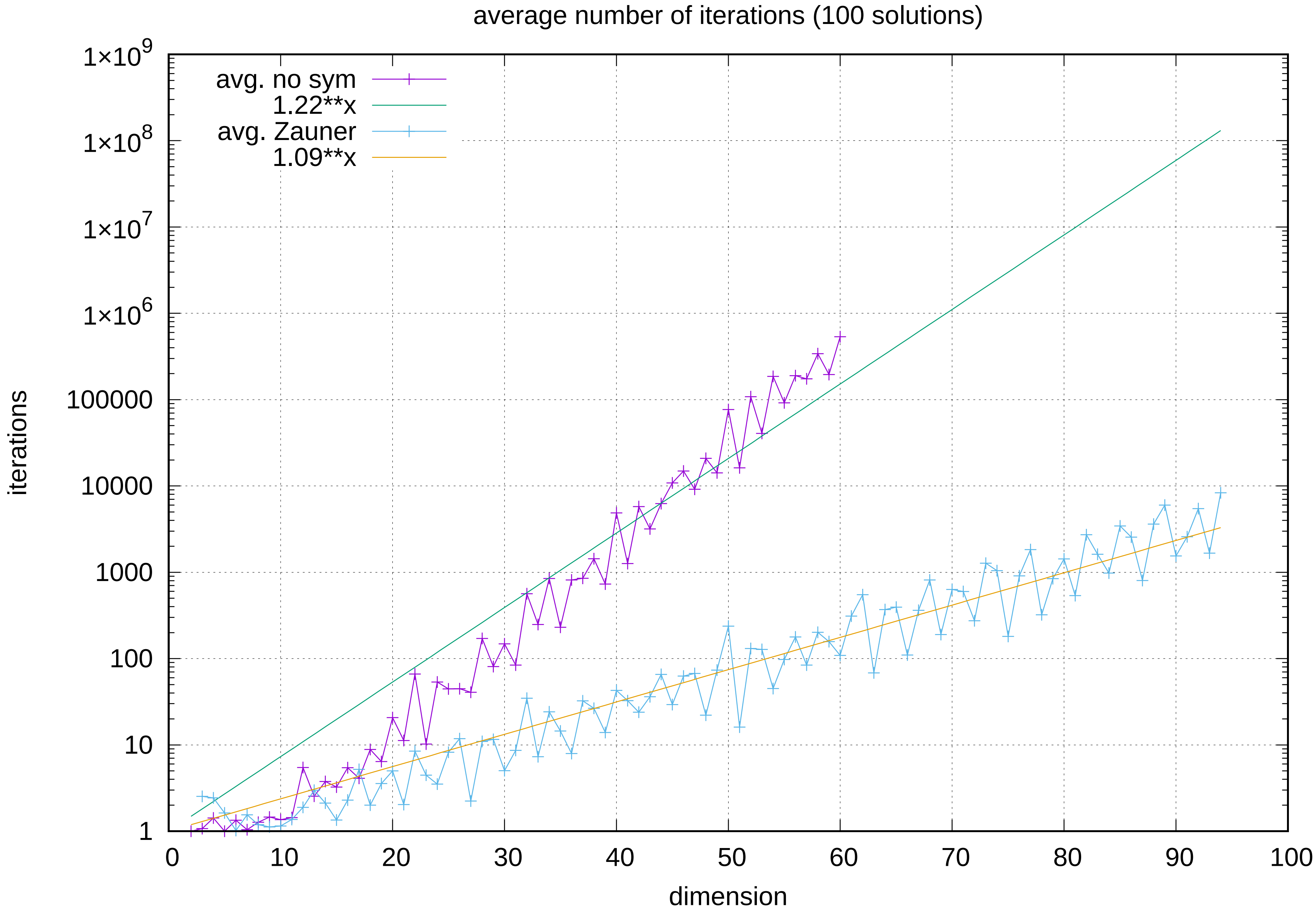
- chain rule yields a relatively simple formula for the gradient of $F(\vec{x})$ in terms of the gradient of $f$

- complexity $\mathcal{O}(d^3)$ for both the function and the gradient when storing $\mathcal{O}(d^2)$ intermediate values

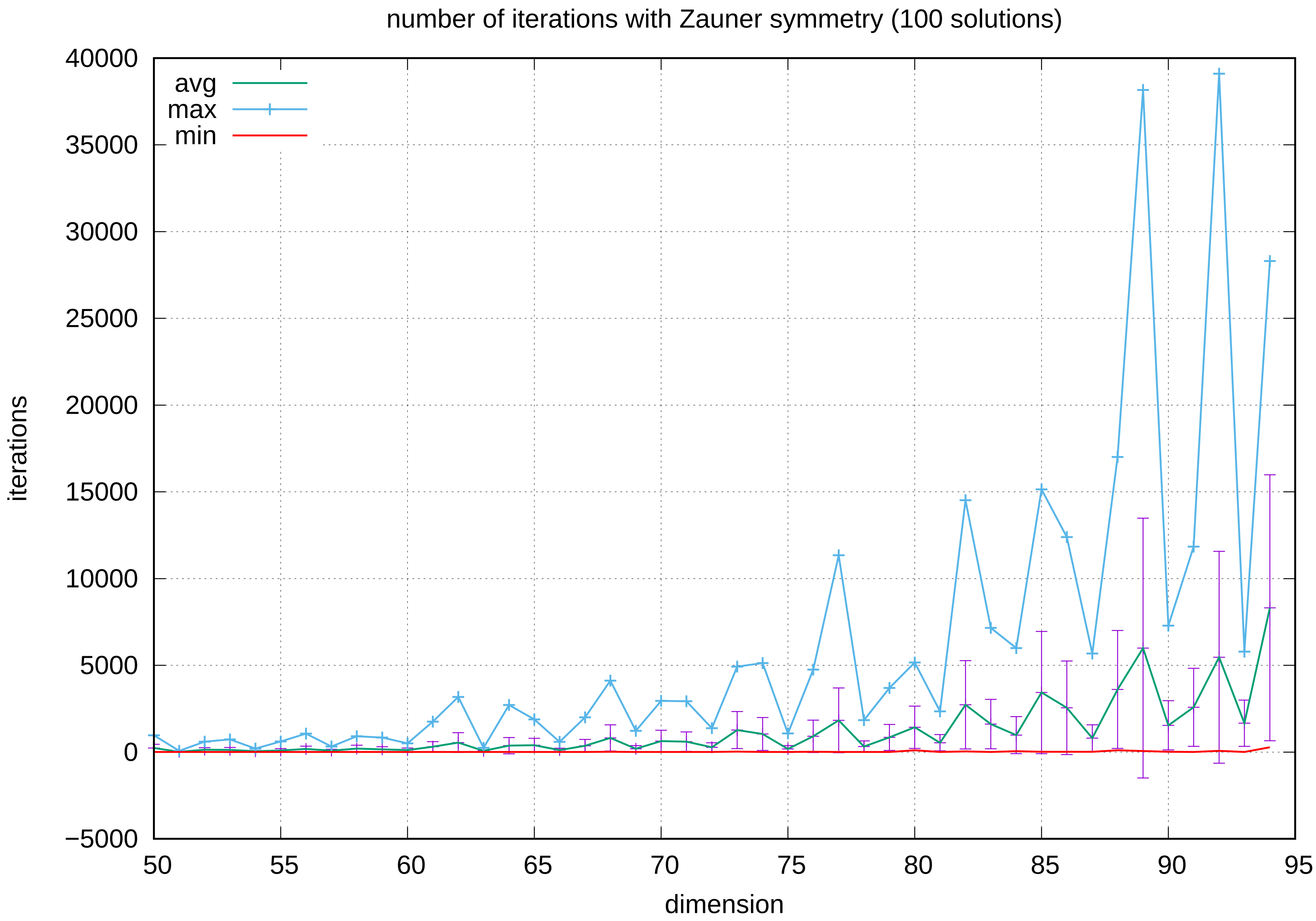
# Numerical Search for SIC-POVMs

- efficient implementation of $F(\vec{x})$ and its gradient in `C++` by Andrew Scott
- parallel computation of the function/gradient using OpenMP/CUDA
- minimization using limited-memory Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm
- search runs into local minima, we need many random initial points
- running many instances on HPC clusters by MPG and GWDG
- 
  - for $d = 189$: approx. $23.3 \times 10^6$ trials, $3.48$ CPU years
  - for $d = 190$: approx. $66.8 \times 10^6$ trials, $10.51$ CPU years
  - for $d = 193$: approx. $78.3 \times 10^6$ trials, $13.00$ CPU years
  - for $d = 5779$: $55065$ trials, $17.69$ GPU years, no success

# Average Number of Iterations



# Average Number of Iterations with Zauner Symmetry

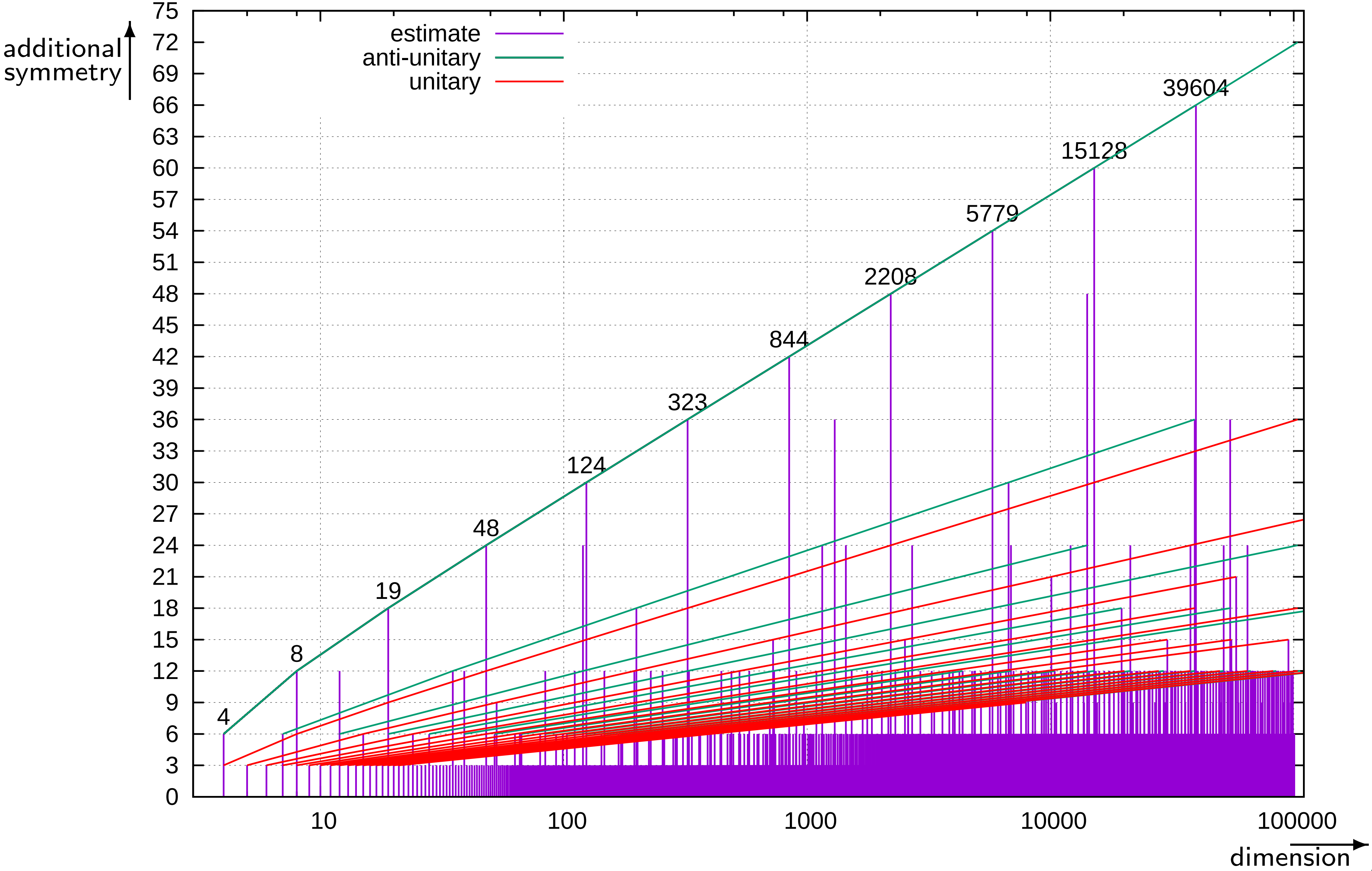


# Fibonacci-Lucas SIC-POVMs

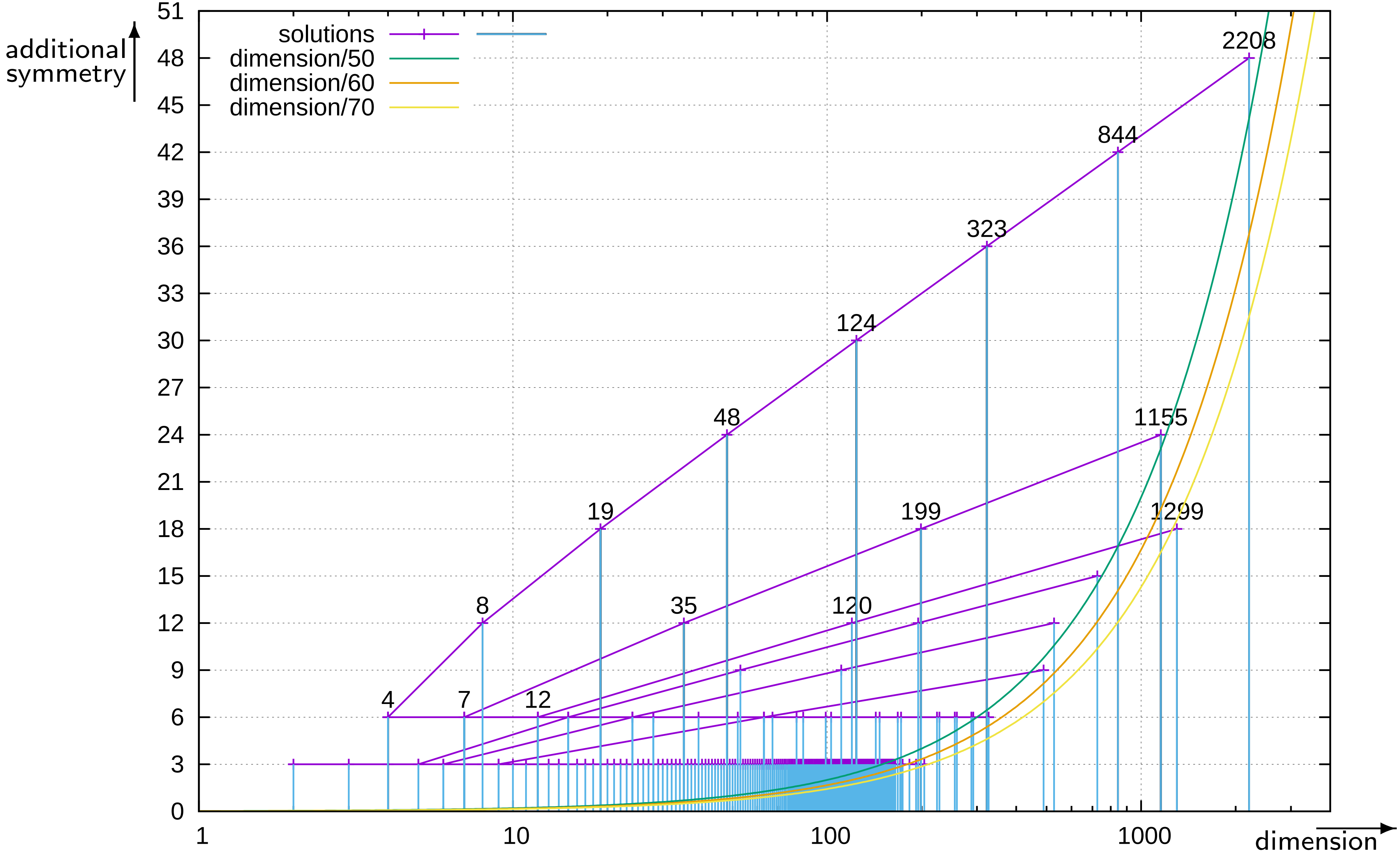
[Markus Grassl & Andrew J. Scott, JMP 58, December 2017, arXiv:1707.02944]

- (exact) symmetry analysis of a numerical solution for $d = 124$
  $\Longrightarrow$ symmetry group of order $30$ (prescribed order $6$)
- identified as part of a series of dimensions (related to Lucas numbers)
  $d = 4, 8, 19, 48, 124, 323, 844, 2208, 5779, 15128, 39604, \ldots$
- symmetry group of order $6k$ related to Fibonacci numbers, $F = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$
- new exact solutions for $d = 124$ and $d = 323$ (previously $d = 48$)
  (found using the symmetries and via Gröbner bases)
- new numerical solutions for $d = 844$ and $d = 2208$ (previously $d = 323$)
- generalisations related to generalised Fibonacci/Lucas numbers, using
  $A_m = \left(\begin{smallmatrix} 0 & 1 \\ 1 & m \end{smallmatrix}\right)$

# Symmetries of SIC-POVMs



# SIC-POVMs by Numerical Search



# Ray Class Field Conjecture

[Appleby, Flammia, McConnell & Yard, arXiv:1604.06098 & arXiv:1701.052000]
CodEx talks by M. Appleby, S. Flammia, G. Kopp

**Ray class field conjecture**

let $\mathbb{E}$ be the field containing all rank-one projection operators of a SIC-POVM

$$\mathbb{Q} \lhd \mathbb{K} = \mathbb{Q}(\sqrt{D}) \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E}$$

for the minimal field:

- $\mathbb{E}$ is the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor[a] $d'$ with ramification at both infinite places, $D$ is the squarefree part of $(d+1)(d-3)$
- $\mathbb{E}_1$ contains the overlap phases and equals the ray class field with ramification only allowed at the infinite place taking $\sqrt{D}$ to a positive real number
- $\mathbb{E}_0$ is the Hilbert class field $H_{\mathbb{K}}$, in particular $h = [\mathbb{E}_0 : \mathbb{K}]$ equals the class number of $\mathbb{K}$

[a] $d' = d$, or $d' = 2d$ for $d$ even

# Ray Class Field Conjecture

[Appleby, Flammia, McConnell & Yard, arXiv:1604.06098 & arXiv:1701.052000]

CodEx talks by M. Appleby, S. Flammia, G. Kopp

**Ray class field conjecture**

let $\mathbb{E}$ be the field containing all rank-one projection operators of a SIC-POVM

$$\mathbb{Q} \lhd \mathbb{K} = \mathbb{Q}(\sqrt{D}) \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E}$$

- **"Fact 8"**: $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ permutes the overlaps.
  For each $\sigma \in \mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ there is a matrix $G_\sigma \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$ such that[a]

  $$\sigma\big(\langle\psi|D_{\boldsymbol{p}}|\psi\rangle\big) = \langle\psi|D_{G_\sigma \boldsymbol{p}}|\psi\rangle.$$

  $G_\sigma$ commutes with matrices $F$ related to symmetries $U_F$ of the fiducial vector $|\psi\rangle$.

[a] $D_{\boldsymbol{p}} = D_{a,b} = (e^{\frac{i\pi}{d}})^{ab} X^a Z^b$

# Exact Solutions from Numerical Solutions

[Appleby, Chien, Flammia & Waldron, J. Phys. A. 51, 2018, arXiv:1703.05981]

- matrix group $\mathcal{M} = \{G_\sigma : \sigma \in \mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)\}$, commutes with the symmetry
- projection operator $\Pi = |\psi\rangle\langle\psi|$

"Fact 8:" $$\sigma\big(\mathrm{Tr}(\Pi D_{\boldsymbol{p}})\big) = \mathrm{Tr}\big(\Pi D_{G_\sigma \boldsymbol{p}}\big)$$

- expansion coefficients $c_{\boldsymbol{p}} = \mathrm{Tr}(\Pi D_{\boldsymbol{p}})$ in the same orbit under $\mathcal{M}$ are related by Galois conjugation
- the coefficients of the polynomial $f_{\boldsymbol{p}_0}(z) = \prod_{\boldsymbol{p}\in\boldsymbol{p}_0^{\mathcal{M}}} (z - c_{\boldsymbol{p}})$

  lie in a number field of "small" degree
- find the exact minimal polynomials of those coefficients (requires high-precision numerical solution)
- find the roots of the exact polynomials $f_{\boldsymbol{p}_0}(z)$ in the ray class field
- compute $\Pi$ from the $d^2$ expansion coefficients $c_{\boldsymbol{p}}$
- exact solutions for some $d \leq 48$ ($d \leq 100$ work in progress)

# More Exact Solutions from Numerical Solutions

[Markus Grassl, Exact SIC-POVMs from permutation symmetries, in preparation]

- when $G_\sigma$ has determinant $1$, there exists a unitary $U_{G_\sigma} := T_\sigma$ with

$$\sigma\left(\mathrm{Tr}(\Pi D_{\boldsymbol{p}})\right) = \mathrm{Tr}(\Pi D_{G_\sigma \boldsymbol{p}}) = \mathrm{Tr}(\Pi T_\sigma D_{\boldsymbol{p}} T_\sigma^\dagger) = \mathrm{Tr}(T_\sigma^\dagger \Pi T_\sigma D_{\boldsymbol{p}})$$

$\Longrightarrow$ action of $T_\sigma^\dagger$ on the projection $\Pi$ and on the state $|\psi\rangle$

- when $G_\sigma = \left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{smallmatrix}\right)$ is additionally diagonal, then $T_\sigma$ is a permutation matrix

- moreover, *assume* that $\sigma(D_{\boldsymbol{p}}) = D_{\boldsymbol{p}}$; then

$$\sigma(\Pi) = T_\sigma^\dagger \Pi T_\sigma$$

and hence

$$\sigma(\Pi_{j,k}) = \Pi_{\alpha j, \alpha k}$$

where the indices are computed modulo $d$

# More Exact Solutions from Numerical Solutions

- for the first column of $\Pi$ we have

$$\sigma(\Pi_{j,0}) = \Pi_{\alpha j,0} \qquad \text{for } j = 0, \ldots, d-1$$

- we can take the first column as (unnormalised) fiducial vector $\boldsymbol{v}$, unless it is zero (which was observed for $d = 26, 28, 62, 98, 228$)
  $\Longrightarrow$ $\sigma$ permutes the components of the fiducial vector, stabilising the first coordinate

- when the first column is zero, consider a non-zero column $k$:

$$\sigma(\Pi_{j,k}) = \Pi_{\alpha j,\alpha k} \stackrel{(*)}{=} \gamma \Pi_{\alpha j,k} \qquad \text{for } j = 0, \ldots, d-1$$

  $\Longrightarrow$ $\sigma$ gives rise to a projective permutation action
  $\Longrightarrow$ consider the action on ratios $v_j/v_{j'}$

---

$^{(*)}$ $\Pi$ has rank one, so column $\alpha k$ is proportional to column $k$, i.e., $\Pi_{j,\alpha k} = \gamma \Pi_{j,k}$

# More Exact Solutions from Numerical Solutions

outline of the procedure:

- compute a numerical fiducial vector with prescribed symmetry $S$
- determine the diagonal matrices $G_\sigma \in \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ in the centraliser of $S$
- the diagonal matrices correspond to a subgroup $H \leq (Z/d'\mathbb{Z})^\times$
- consider the rescaled fiducial vector[a] $\boldsymbol{v}$ with $v_0 = 1$
- the coefficients of the polynomial $f_j(z) = \prod\limits_{\alpha \in H} (z - v_{\alpha j})$ lie in a number field of “small” degree, fixed by (a subgroup of) the Galois group
- similar as before, find the exact coefficients of $f_j(z)$ from a high-precision numerical solution, and then compute its exact roots
  $\Longrightarrow$ only $\mathcal{O}(d)$ numbers in a field of smaller degree

[a] assuming $v_0 \neq 0$ for simplicity here

# More Exact Solutions from Numerical Solutions

- the *assumption* that $\sigma(D_{\boldsymbol{p}}) = D_{\boldsymbol{p}}$ appears to be true
- new exact solutions for $57$ additional dimensions (so far)

$$d = 26, 38, 42, 49, 52, 57, 61, 62, 63, 65, 67, 73, 74, 78, 79, 84, 86, 91, 93, 95, \\ 97, 98, 103, 109, 111, 122, 127, 129, 133, 134, 139, 143, 146, 147, \\ 151, 155, 157, 163, 168, 169, 172, 181, 182, 183, 193, 199, \\ 201, 228, 259, 292, 327, 364, 399, 403, 489, 844, 1299$$

- fiducial vectors lie in a proper ("small") subfield of the ray class field from before, that intersects with the cyclotomic field $\mathbb{Q}(\zeta_{d'})$ trivially or in a smaller cyclotomic field
- "small ray class field conjecture":
  The minimal field containing a (suitably rescaled) fiducial vector is a ray class field whose conductor is a particular factor of the ideal $d\mathcal{O}_{\mathbb{K}}$ with ramification at one of the infinite places.

# Prime Dimensions $p \equiv 1 \bmod 3$

- for prime dimensions $d = p \equiv 1 \bmod 3$, the Zauner symmetry $F_z$ is conjugate to a diagonal matrix $\widetilde{F}_z$
- the centraliser of $\widetilde{F}_z$ contains all diagonal matrices in $\mathrm{SL}(2, \mathbb{Z}/d\mathbb{Z})$
- the components $v_j$, $j = 1, \ldots, d-1$, of the fiducial vector (with $v_0 = 1$) are on a single orbit with respect to the Galois group, i.e.,

$$v_{\theta^k} = \sigma^k(v_1)$$

  for generators $\theta$ and $\sigma$ of $(\mathbb{Z}/d\mathbb{Z})^\times$ and the Galois group, resp.
- for a permutation symmetry of order $3\ell$, we need only $m = \frac{d-1}{3\ell}$ numbers

**dream:**

find a *direct* way to determine the algebraic number $v_1$, as well as $\sigma$ and $\theta$

# Prime Dimensions $p = n^2 + 3$

[Appleby, Bengtsson, Grassl, Harrison, McConnell, "SIC-POVMs from Stark Units"]

**Conjecture:**

- for prime dimensions $p = n^2 + 3$ $(n > 0)$, there is an *almost flat* fiducial vector $\boldsymbol{v}$ with

$$v_j = \begin{cases} -2 - \sqrt{d+1} & j = 0 \\ \sqrt{v_0 e^{i\vartheta_j}} & j > 0 \end{cases}$$

- the components of $\boldsymbol{v}$ generate a "small" ray class field $\mathbb{K}^{\mathfrak{m}}$ with finite modulus $\sqrt{d+1} \pm 1$ and ramification at one infinite place
- the phases $e^{i\vartheta_j}$ are Galois conjugates of (real) *Stark units* for the ray class field $\mathbb{K}^{\mathfrak{m}}$

# Application of Stark's Conjectures

- for certain ray class fields $\mathbb{K}^{\mathfrak{m}}$ over the real quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, $D > 0$, one can compute numerical approximations of *Stark units* $\epsilon_\sigma$ via special values of derivatives of $L$-functions
- the Stark units are labelled by elements $\sigma$ of the Galois group $\mathrm{Gal}(\mathbb{K}^{\mathfrak{m}}/\mathbb{K})$ such that $\epsilon_\sigma = \sigma(\epsilon_0)$
- from numerical Stark units with sufficiently high precision, we can deduce their exact minimal polynomial over $\mathbb{K}$
- we have a heuristic that allows us to deduce the required precision from numerical Stark units with low precision
- the complexity of the calculation appears to be roughly $\mathcal{O}\left(\deg(\mathbb{K}^{\mathfrak{m}}/\mathbb{K}) \times (\#\text{digits})^{3.3}\right)$

# Runtime $L$-Functions

total CPU time to compute the numerical derivative of $L$-functions using Magma and PARI/GP (last three cases)

| $d$ | $\deg(\mathbb{K}^{\mathfrak{m}}/\mathbb{K})$ | log height | precision | CPU time |
|---|---|---|---|---|
| 487 | 324 | 424 | 1000 digits | 251 hours |
| 787 | 262 | 299 | 1000 digits | 118 hours |
| 2707 | 902 | 1861 | 3800 digits | 900 days |
| 4099 | 1366 | 974 | 2000 digits | 170 days |
| 5779 | 214 | 127 | 300 digits | 18 min |
| 1447 | 964 | 2158 | 4600 digits | 111 days |
| 19603 | 2178 | 1754 | 4000 digits | 82 days |
| 2503 | 3336 | 6464 | 13000 digits | 60.5 years |

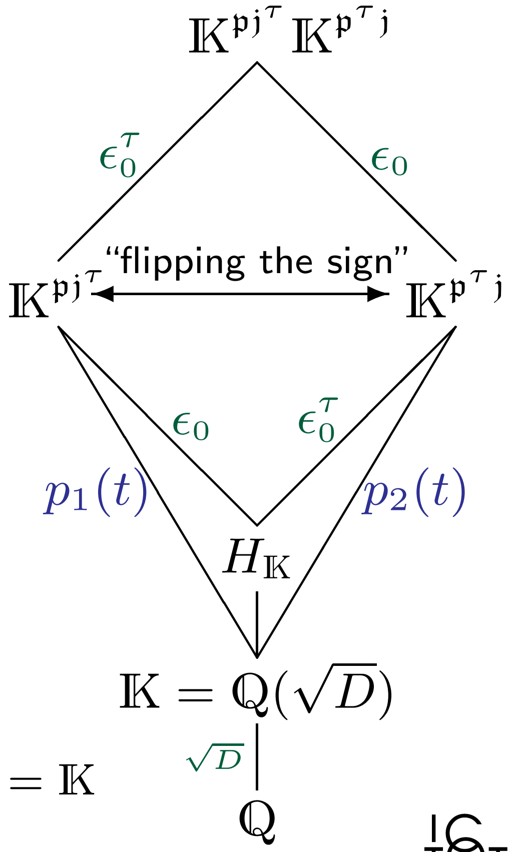
# Flipping the Sign

- real quadratic field $\mathbb{K}=\mathbb{Q}(\sqrt{D})$ with non-trivial automorphism $\tau\colon \sqrt{D}\mapsto -\sqrt{D}$

- embedding $\mathfrak{j}\colon \mathbb{K}\hookrightarrow\mathbb{R}, \mathfrak{j}(\sqrt{D})>0$, $\mathfrak{j}^\tau(\sqrt{D})=\mathfrak{j}((\sqrt{D})^\tau)<0$
  - "real" Stark units $\epsilon_\sigma$: $\mathfrak{j}(\epsilon_\sigma)>0$
  - "complex" Stark units $\epsilon_\sigma^\tau$: $\mathfrak{j}(\epsilon_\sigma^\tau)=\mathfrak{j}^\tau(\epsilon_\sigma)\in\mathbb{C}\setminus\mathbb{R}$

- minimal polynomial of $\epsilon_\sigma$: $p_1(t)\in\mathbb{K}[t]$
  $\Longrightarrow$ minimal polynomial of $\epsilon_\sigma^\tau$: $p_2(t)=p_1^\tau(t)$

- **obstacle:**
  operation of $\sigma$ on $\epsilon_0^\tau$ would require factoring $p_2(t)$




for simplicity, we assume in the following class number $h=1$, i.e., $H_\mathbb{K}=\mathbb{K}$

# The Galois Polynomial

- fixing some labelling, we know how $\sigma$ permutes the $m$ (numerical) Stark units $\epsilon_j$: $\sigma(\epsilon_j) = \sigma_{\pi_\sigma(j)}$ for some permutation $\pi_\sigma$
- there exists a unique polynomial $g_1$ of degree at most $m-1$ such that

$$g_1(\epsilon_j) = \epsilon_{\pi_\sigma(j)} \qquad \text{for } j = 1, \ldots, m \tag{1}$$

- using Newton interpolation, $g_1$ can be computed with $\mathcal{O}(m^2)$ arithmetic operations ($\mathcal{O}(m(\log m)^2)$ when using FFT-based methods)
- the coefficients of $g_1$ are in $\mathbb{K}$, as $(1)$ is invariant wrt. $\mathrm{Gal}(\mathbb{K}^{\mathfrak{p}\mathfrak{j}^\tau}/\mathbb{K})$
- $g_2(t) = g_1^\tau(t)$ corresponds to the action of $\sigma$ on $\epsilon_j^\tau$: $g_2(\epsilon_j^\tau) = \epsilon_{\pi_\sigma(j)}^\tau$
- **potential computational obstacle:**
  we don't know an *a priori* bound for the required precision
  (for $d = 19603$, the coefficients have more than 1 million digits)

# Solving the Sign Problem

Recall: We conjecture that the components of the fiducial vector are *square roots* of Galois conjugates of Stark units, i.e., $v_{\theta^k} = \sqrt{v_0 \sigma^k(\epsilon_0^\tau)}$.

**Problem:** there are two square roots $\pm\sqrt{v_0 \sigma^k(\epsilon_0^\tau)}$

**Solution:**

- it turns out that polynomial $p_2(t^2/v_0)$ with $v_0 = -2 - \sqrt{d+1}$ factors in $\mathbb{K}[t]$ as

$$v_0^m p_2(t^2/v_0) = p_4(t) p_4(-t)$$

- pick the factor $p_4(t)$ and check which of the square roots is a root of $p_4(t)$
- we are left with a global sign ambiguity, i.e., two possibilities
- note: it does not matter which of the Galois conjugates of the Stark units is assigned to $\epsilon_0^\tau$; all choices yield eventually fiducial vectors

# Final Step: Combinatorial Search

so far, we have

- exact minimal polynomials $p_1(t), p_2(t), p_4(t) \in \mathbb{K}[t]$ and exact Galois polynomials $g_1(t), g_2(t) \in \mathbb{K}[t]$
- numerical square roots $\sqrt{v_0 \epsilon_j^\tau}$ (up to a global sign) together with the permutation action of the (cyclic) Galois group $\mathrm{Gal}(\mathbb{K}^{\mathfrak{m}}/H_{\mathbb{K}})$ on them

final step:

- we have to identify which primitive element $\theta \in (\mathbb{Z}/d\mathbb{Z})^\times$ corresponds to the action of $\sigma$
- we have to fix the global sign (we can choose the sign of the first coordinate)
- compute a (numerical) vector $\boldsymbol{v}$ for all choices (less than $d$) and test the overlap $|\langle \boldsymbol{v}|X|\boldsymbol{v}\rangle|^2/||\boldsymbol{v}||^4 \stackrel{?}{=} \frac{1}{d+1}$
- we know that $\sigma^{m/2}$ corresponds to complex conjugation

# Exact Solution

We can also compute an exact representation of the fiducial vector without explicit factorisation in the extension field:

- define the field $\mathbb{L} = H_{\mathbb{K}}(\gamma)$ with $p_4(\gamma) = 0$
- compute the exact Galois polynomial $g_4(t) \in H_{\mathbb{K}}[t]$ from the numerical values $\sqrt{v_0 \epsilon_\sigma^\tau}$
- the action of the Galois automorphism $\sigma$ on $\mathbb{L}$ is defined by $\sigma\colon \gamma \mapsto g_4(\gamma)$
- we can compute the components of the fiducial vector using

$$v_0 = \pm(2 + \sqrt{d+1}), \qquad v_1 = \gamma, \qquad \text{and } v_{\theta j} = g_4(v_j) \text{ for } j > 0$$

**computational obstacles:** missing an *a priori* bound on the precision to compute the exact Galois polynomial $p_4(t)$ and arithmetic in the field $\mathbb{L}$ is slow when the degree is large (use tower of subfields if possible)

# Verification of the Solution

- second frame potential for a fiducial vector

$$f(|\psi\rangle) = \sum_{j,k=1}^{d} \Bigg| \underbrace{\sum_{\ell=1}^{d} \overline{\psi}_{j+\ell}\, \psi_\ell\, \overline{\psi}_{k+\ell}\, \psi_{j+k+\ell}}_{=:G(j,k)} \Bigg|^2 = \frac{2}{d+1}$$

- moreover $G(j,k) = \dfrac{\delta_{j,0} + \delta_{k,0}}{d+1}$
- $G(j,k)$ has an eightfold symmetry
- we don't need $d$-th roots of unity
- $\mathcal{O}(d^3)$ arithmetic operations

*verifying the solution takes longer than computing it*

# Runtime Verification

CPU time for the exact/numerical verification of the solution

| $d$ | $\deg(\mathbb{K}^{\mathfrak{m}}/\mathbb{K})$ | precision | CPU time | $G(j,k)$ |
|---|---|---|---|---|
| 103 | $2^2 \times 17$ | exact | 440 s | 1.3 s |
| 199 | $2 \times 11$ | exact | 310 s | 0.3 s |
| 487 | $2^2 \times 3^4$ | exact | 31 days | 315 s |
| 787 | $2 \times 131$ | 10000 digits | 3 hours | 65 min |
| 1447 | $2^2 \times 241$ | 10000 digits | 17.0 hours | |
| 2707 | $2 \times 11 \times 41$ | 2000 digits | 11.2 hours | |
| 4099 | $2 \times 683$ | 2000 digits | 36.5 hours | |
| 5779 | $2 \times 107$ | 2000 digits | 100 hours | 88 min |
| 19603 | $2 \times 3^2 \times 11^2$ | 1000 digits | 1367 days | |
| 39604 | $2^2 \times 3^2 \times 5^2$ | 100 digits | 684 days | $\approx$ 28 days |

# Solutions for $d = n^2 + 3$

- the method can be generalised to composite dimensions $d = n^2 + 3$
- even dimensions $d = n^2 + 3$ are divisible by $4$, but not by $8$; almost flat fiducial vector after change of basis
- for composite dimensions, one has to compute Stark units for certain subfields as well
- there are more possibilities to match the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ and the action of the Galois group

so far, our method has been successfully applied in $34$ dimensions:

$d = 7, 12, 19, 28, 39, 52, 67, 84, 103, 124, 147, 172, 199, 259, 292, 327, 403, 487, 628, 787, 844, 964, 1027, 1228, 1299, 1447, 1684, 1852, 2404, 2707, 4099, 5779,$ $19603$, and $39604$

# Conclusions & Outlook

- deterministic procedure to compute SIC-POVMs from Stark units
- successfully applied in $34$ dimensions $d = n^2 + 3$; did not fail in any
- can we obtain a fiducial vector directly from the *real* Stark units, without "flipping the sign"?
- can we work with lower precision?
- can we avoid the combinatorial search in the final step?
- assuming Stark's conjectures to be true, can be prove that our construction always works?
- can we extend the method to other dimensions?

forthcoming publication:

Marcus Appleby, Ingemar Bengtsson, Markus Grassl, Michael Harrison, Gary McConnell, "SIC-POVMs from Stark Units"

# Thank you!
# Danke! Merci!
# Dziekuje!

**Acknowledgments**

The 'International Centre for Theory of Quantum Technologies' project (contract no. 2018/MAB/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

European Funds Smart Growth

Republic of Poland

FNP Foundation for Polish Science

European Union European Regional Development Fund

Additional computing resources were provided via MPL

MAX PLANCK INSTITUTE FOR THE SCIENCE OF LIGHT