Tight frames and Approximation

Taipa, Doubtless Bay

20–23 February 2018

Symmetries of Weyl-Heisenberg SIC-POVMs

Markus Grassl

joint work in progress with
Andrew Scott & Ulrich Seyfarth

Markus.Grassl@mpl.mpg.de

sicpovm.markus-grassl.de

21 February 2018

MAX PLANCK INSTITUTE
for the science of light

Tomography of Quantum States

General Problem:

What is the best way to identify an arbitrary unknown quantum state ρ in a d-dimensional Hilbert space?

- ρ is a Hermitian matrix
  $\Longrightarrow d^2 - 1$ real parameters
- one von Neumann measurement provides $d - 1$ independent parameters
  $\Longrightarrow$ at least $d + 1$ different (projective) measurements
- general measurements (POVMs)
  $\Longrightarrow$ at least d^2 POVM elements
- goal:
  "maximal independence" of the measurement results
  $\Longrightarrow$ optimal statistics with no *a priori* knowledge for a non-adaptive scheme

SIC-POVMs: Equiangular Lines in Complex Space

The General Problem

Find m normalized vectors $\{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\} \subset \mathbb{C}^d$ such that the modulus of the inner product between any pair of vectors is constant, i. e.

$$|\langle \boldsymbol{v}^{(j)} | \boldsymbol{v}^{(k)} \rangle|^2 = \left| \sum_{\ell=1}^{d} \overline{v_\ell^{(j)}} v_\ell^{(k)} \right|^2 = \begin{cases} 1 & \text{for } j = k, \\ c & \text{for } j \neq k \end{cases}$$

Special Case: SIC-POVMs

Find d^2 normalized vectors $\{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(d^2)}\} \subset \mathbb{C}^d$ such that the modulus of the inner product between any pair of vectors is constant, i. e.

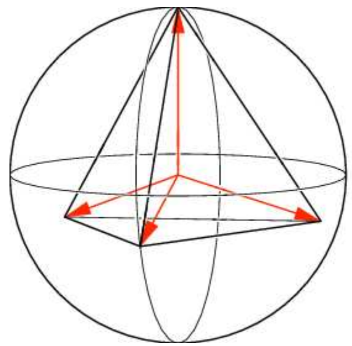
$$|\langle \boldsymbol{v}^{(j)} | \boldsymbol{v}^{(k)} \rangle|^2 = \begin{cases} 1 & \text{for } j = k, \\ 1/(d+1) & \text{for } j \neq k \end{cases}$$

Quantum Information: SIC-POVMs

- generalized quantum measurement (POVM) with d^2 rank-one elements $E_j = \Pi_j/d$ with $\Pi_j = |\boldsymbol{v}^{(j)}\rangle\langle\boldsymbol{v}^{(j)}|$
- The d^2 elements form a basis of $\mathbb{C}^{d\times d}$.
  $\Longrightarrow$ "informationally complete", i.e., reconstruction of a quantum state ρ is possible
- expectation values $p_j = \mathrm{tr}(\rho E_j)$ "maximally independent":

$$\mathrm{tr}\left(\Pi_j \Pi_k\right) = |\langle\boldsymbol{v}^{(j)}|\boldsymbol{v}^{(k)}\rangle|^2 = \frac{1}{d+1} \qquad \text{for } j \neq k,$$

  $\Longrightarrow$ "symmetric"



- applications in quantum cryptography as well

Related Problems

Complex Spherical 2-Designs

The integral of any degree-two polynomial over the complex sphere in $\mathbb{C}^d$ can be computed as finite average, i. e.

$$\frac{1}{\mu(\mathbb{C}S^{d-1})}\int_{g\in\mathbb{C}S^{d-1}} f(g)d\mu(g) = \frac{1}{m}\sum_{j=1}^{m} f(\boldsymbol{v}^{(j)})$$

if $m = d^2$ and the vectors $\boldsymbol{v}^{(i)}$ are equiangular lines.

Banach Spaces [König & Tomczak-Jaegermann 94]

The projection constant

$$\lambda(E) = \sup_{X\supseteq E}\inf_{P}\{\|P\| : P\colon X \to E \text{ is linear projection onto } E\}$$

of a complex d-dimensional normed space E is maximal iff a set of d^2 equiangular lines exists.

Ansatz: System of Polynomial Equations

use $2d$ real variables per vector

$$\boldsymbol{v}^{(j)} = \big(a_1^{(j)} + ib_1^{(j)}, \ldots, a_d^{(j)} + ib_d^{(j)}\big), \qquad |\langle \boldsymbol{v}^{(j)}|\boldsymbol{v}^{(k)}\rangle|^2 = \frac{1 + d\delta_{jk}}{1+d}$$

where $i^2 = -1$.

$d = 2$, $m = d^2 = 4$

$$\begin{aligned}
\boldsymbol{v}^{(1)} &= \big(a_1^{(1)} + ib_1^{(1)}, a_2^{(1)} + ib_2^{(1)}\big)\\
\boldsymbol{v}^{(2)} &= \big(a_1^{(2)} + ib_1^{(2)}, a_2^{(2)} + ib_2^{(2)}\big)\\
\boldsymbol{v}^{(3)} &= \big(a_1^{(3)} + ib_1^{(3)}, a_2^{(3)} + ib_2^{(3)}\big)\\
\boldsymbol{v}^{(4)} &= \big(a_1^{(4)} + ib_1^{(4)}, a_2^{(4)} + ib_2^{(4)}\big)
\end{aligned}$$

already rather complicated to solve for $d = 3$ and $m > 4$

MAX PLANCK INSTITUTE for the science of light

Symmetries of SIC-POVMs

SIC-POVM as set of rank-one projection operators

$$\mathcal{S} = \{P_1, \ldots, P_{d^2}\} \quad \text{where } P_i^2 = P_i,\ P_i = P_i^\dagger,\ \mathrm{tr}(P_i) = 1$$

unitary symmetry U acts on $\mathcal{S}$:

$$U P_i U^\dagger = P_{\pi(i)}$$

- permutation representation of the symmetry group $A(\mathcal{S})$

$$A(\mathcal{S}) \to S_{d^2}, U \mapsto \pi(U)$$

- for SIC-POVMs, the kernel corresponds to global phases
  $\Rightarrow$ projective representation of the permutation group

NB: $A(\mathcal{S})$ can be computed from $(T_{ij}) = \mathrm{tr}(P_1 P_i P_j)$

MAX PLANCK INSTITUTE for the science of light

Special Symmetries of SIC-POVMs

For $U \in A(\mathcal{S})$, the number $f(U)$ of fixed points i, i. e. $U P_i U^\dagger = P_i$ is given by

$$f(U) = |\operatorname{tr}(U)|^2.$$

[Zauner 99, Satz 2.34]

- **transitive symmetry group:**
  The SIC-POVM is a single orbit under $A(\mathcal{S})$, i. e. $P_i = U_i P_1 U_i^\dagger$.
- **regular symmetry (sub)group:**
  Up to phases, there is a unique element U_i with $P_i = U_i P_1 U_i^\dagger$.

candidates for regular symmetry groups are nice unitary error bases (UEBs)
[Klappenecker & Rötteler, quant-ph/0010082]

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 1:

SIC-POVM that is the orbit under H_d, i. e.,

$$|\boldsymbol{v}^{(a,b)}\rangle := X^a Z^b |\boldsymbol{v}^{(0)}\rangle$$

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

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

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

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

Jacobi Group (or Clifford Group)

- automorphism group of the 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 $SL(2, \mathbb{Z}_d)$, i. e.

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

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

- additionally: complex conjugation

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

MAX PLANCK INSTITUTE for the science of light

Constructing SIC-POVMs (cntd.)

Ansatz 2:

SIC-POVM that is the orbit under H_d,

additionally:

$|\boldsymbol{v}^{(0)}\rangle$ lies in a (degenerate) ℓ-dimensional eigenspace of some $T \in J_d$

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

where $|b_j\rangle$, $j = 1, \ldots, \ell$ is the basis of that eigenspace

$\Longrightarrow$ reduced number of variables

$\Longrightarrow$ better chances to compute algebraic solutions

additionally: choose a "good" basis such that e.g. T resp. $|\boldsymbol{v}^{(0)}\rangle$ will be sparse

Fibonacci-Lucas SIC-POVMs

[Markus Grassl & Andrew J. Scott 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)
  $d = 4, 8, 19, 48, 124, 323, 844, 2208, 5779, 15128$
- symmetry group of order $6k$ related to Fibonacci numbers
- new exact solutions for $d = 124$ and $d = 323$ (previously $d = 48$)
- new numerical solution for $d = 844$ with 150 digits (previously $d = 323$)

MAX PLANCK INSTITUTE
for the science of light

Fibonacci-Lucas SIC-POVMs

[Markus Grassl & Andrew J. Scott arXiv:1707.02944]

- Fibonacci numbers F_k with $F_0 = 0$, $F_1 = 1$, $F_{k+1} = F_k + F_{k-1}$

$$F_k = \frac{\varphi^k - (-\varphi)^{-k}}{\sqrt{5}}, \qquad \varphi = \frac{1+\sqrt{5}}{2}$$

- Lucas numbers L_k with $L_0 = 2$, $L_1 = 1$, $L_{k+1} = L_k + L_{k-1}$

$$L_k = \varphi^k + (-\varphi)^{-k}$$

- prescribed anti-unitary symmetry related to the Fibonacci matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad A^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix}$$

Fibonacci-Lucas SIC-POVMs

[Markus Grassl & Andrew J. Scott arXiv:1707.02944]

- Fibonacci numbers F_k with $F_0 = 0$, $F_1 = 1$, $F_{k+1} = F_k + F_{k-1}$
- Lucas numbers L_k with $L_0 = 2$, $L_1 = 1$, $L_{k+1} = L_k + L_{k-1}$
- prescribed anti-unitary symmetry related to the Fibonacci matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad A^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix}$$

- modulo $d_k = L_{2k} + 1$, the matrix A has order $6k$
- sequence of dimensions $d = 4, 8, 19, 48, 124, 323, 844, 2208, 5779, 15128$
- squarefree part D of $(d+1)(d-3)$ is always $D = 5$
  $\Longrightarrow$ ray class field over $\mathbb{Q}(\sqrt{5})$

Generalised Fibonacci-Lucas SIC-POVMs

- generalised Fibonacci numbers $F_{m,k}$ with
  $F_{m,0} = 0$, $F_{m,1} = 1$, $F_{m,k+1} = mF_{m,k} + F_{m,k-1}$
- generalised Lucas numbers $L_{m,k}$ with
  $L_{m,0} = 2$, $L_{m,1} = m$, $L_{m,k+1} = mL_{m,k} + L_{m,k-1}$
- prescribed anti-unitary symmetry related to the matrix

$$A_m = \begin{pmatrix} 0 & 1 \\ 1 & m \end{pmatrix} \qquad A_m^k = \begin{pmatrix} F_{m,k-1} & F_{m,k} \\ F_{m,k} & F_{m,k+1} \end{pmatrix}$$

- modulo $d_{m,k} = L_{m,2k} + 1$, the matrix A has order $6k$
- squarefree part D of $(d+1)(d-3)$ equals the squarefree part of $m^2 + 4$
  $\Longrightarrow$ ray class field over $\mathbb{Q}(\sqrt{D})$

MAX PLANCK INSTITUTE for the science of light

Anti-Unitary Symmetries

	k	1	2	3	4	5	6	7	8
	ord(F)	6	12	18	24	30	36	42	48
m	D	$F_{e'}$	F_g						
1	5	4	8	19	48	124	323	844	2208
2	2	7	35	199	1155	6727	39203	228487	1331715
3	13	12	120	1299	14160	154452	1684803	18378372	200477280
4	5	19	323	5779	103683	1860499			
5	29	28	728	19603	528528	14250628			
6	10	39	1443	54759	2079363	78960999			
7	53	52	2600	132499	6754800				
8	17	67	4355	287299	18957315				
9	85	84	6888	571539	47430768				
10	26	103	10403	1060903					
11	5	124	15128	1860499					
12	37	147	21315	3111699					
13	173	172	29240	4999699					
14	2	199	39203	7761799					
15	229	228	51528						
16	65	259	66563						
17	293	292	84680						
18	82	327	106275						
19	365	364	131768						
20	101	403	161603						

MAX PLANCK INSTITUTE for the science of light

Families of SIC-POVMs with Unitary Symmetry

- prescribed unitary symmetry related to the matrix

$$B_m = \begin{pmatrix} 0 & 1 \\ -1 & m \end{pmatrix}$$

- similar recurrence relations for the entries of B_m^k and the corresponding dimension
- order of the symmetry is $3k$

Unitary Symmetries

	k	1	2	3	4	5	6	7	8	9
	ord(F)	3	6	9	12	15	18	21	24	27
m	D	F_z	F_b	F_d						
3	5	*4*	*8*	*19*	*48*	124	323	844	2208	5779
4	3	5	15	53	195	725	2703	10085	37635	140453
5	21	6	24	111	528	2526	12099	57966	277728	1330671
6	2	7	35	199	1155	6727	39203	228487	1331715	7761799
7	5	8	48	323	2208	15128	103683	710648	4870848	33385283
8	15	9	63	489	3843	30249	238143	1874889	14760963	116212809
9	77	10	80	703	6240	55450	492803	4379770	38925120	345946303
10	6	11	99	971	9603	95051	940899	9313931	92198403	912670091
11	13	12	120	1299	14160	154452				
12	35	13	143	1693	20163	240253				
13	165	14	168	2159	27888	360374				
14	3	15	195	2703	37635	524175				
15	221	16	224	3331	49728	742576				
16	7	17	255	4049	64515					
17	285	18	288	4863	82368					
18	5	19	323	5779	103683					
19	357	20	360	6803	128880					
20	11	21	399	7941	158403					

MAX PLANCK INSTITUTE
for the science of light

Symmetries and Ray Class Fields

[Appleby, Chien, Flammia & Waldron arXiv:1703.05981]

Ray class field conjecture

nested tower of fields (for the minimal field)

$$\mathbb{Q} \lhd \mathbb{E}_c = \mathbb{Q}(\sqrt{D}) \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E} = \mathbb{E}_1(i\sqrt{d'}).$$

- $\mathbb{E}$ is the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d' with ramification at both infinite places
- $\mathbb{E}_1$ is 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 over $\mathbb{Q}(\sqrt{D})$, in particular $[\mathbb{E}_0 : \mathbb{Q}(\sqrt{D})]$ equals the class number of $\mathbb{Q}(\sqrt{D})$

MAX PLANCK INSTITUTE for the science of light

Symmetries and Ray Class Fields

[Appleby, Chien, Flammia & Waldron arXiv:1703.05981]

Ray class field conjecture

nested tower of fields (for the minimal field)

$$\mathbb{Q} \lhd \mathbb{E}_c = \mathbb{Q}(\sqrt{D}) \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E} = \mathbb{E}_1(i\sqrt{d'}).$$

- for $\mathcal{M}$ a certain maximal Abelian subgroup of $\mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$ and (essentially) the symmetry group $S(\Pi)$ of the SIC-POVM:

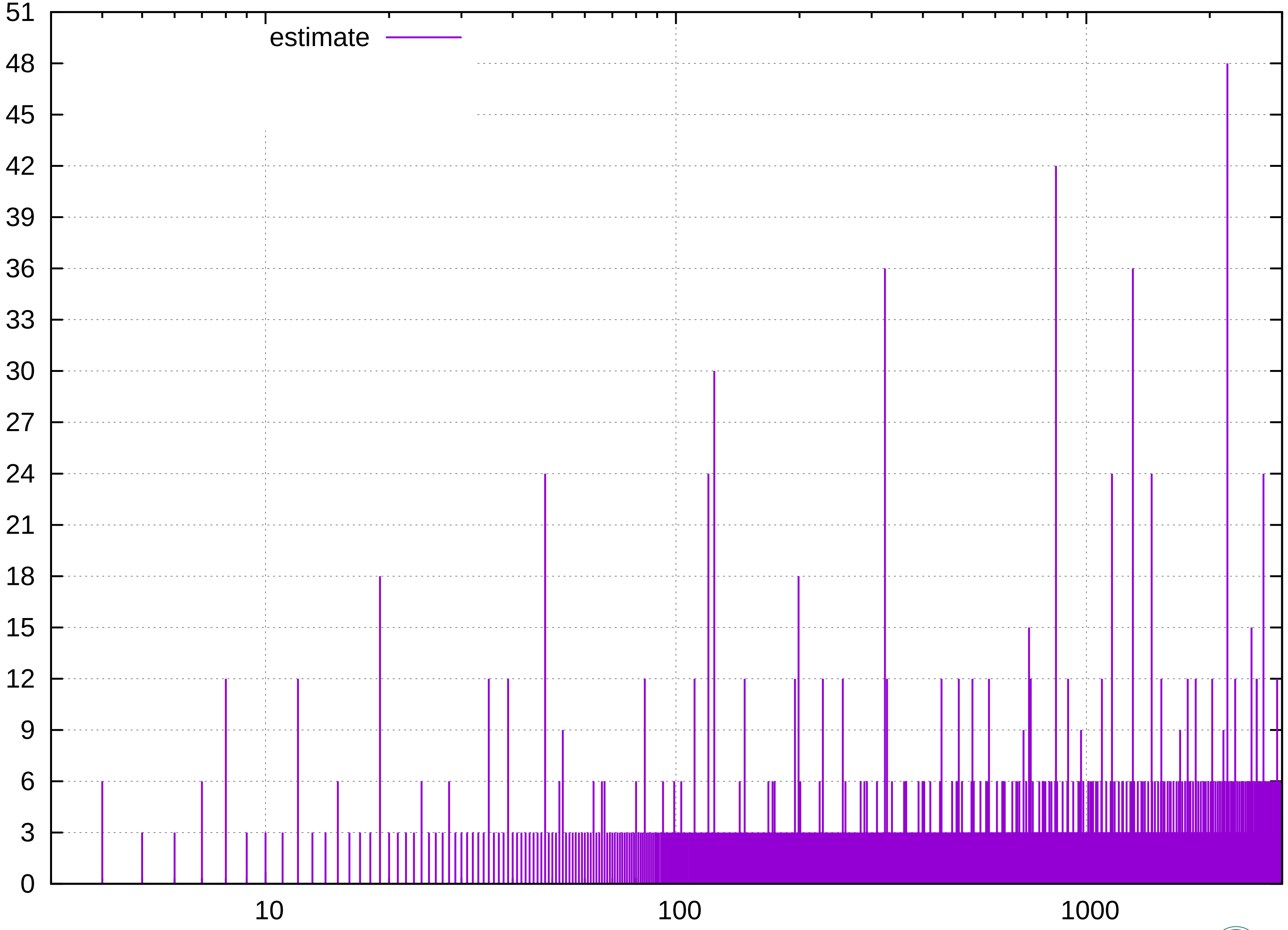
$$\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong \mathcal{M}/S(\Pi)$$

- estimate for the group order:

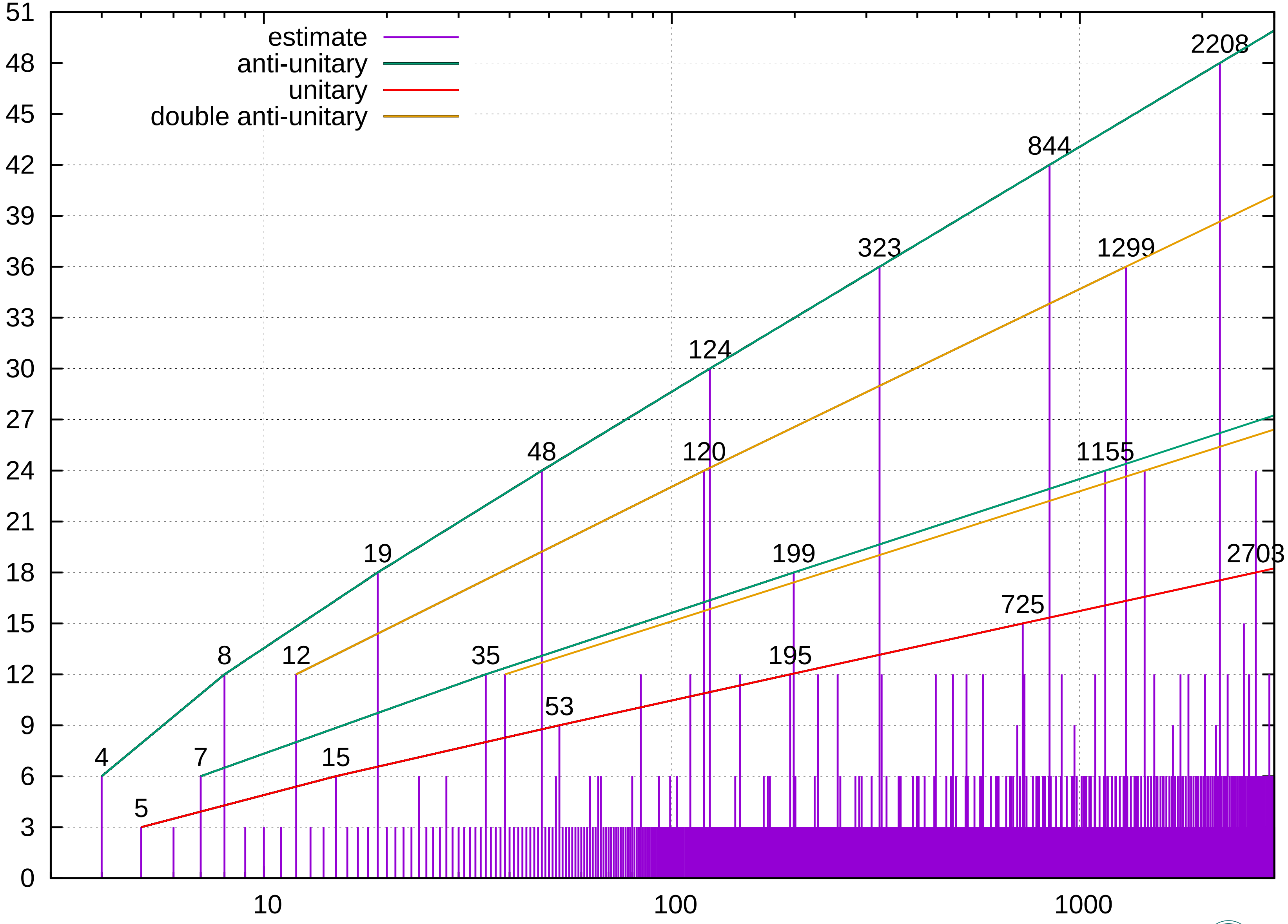
$$|S(\Pi)| = \frac{|\mathcal{M}|}{|\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)|} = \frac{|\mathcal{M}| \times |\mathrm{Gal}(\mathbb{E}_0/\mathbb{E}_c)|}{|\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_c)|}$$

- 1 or 4 cases for $|\mathcal{M}|$, but $|S(\Pi)|$ must be integral

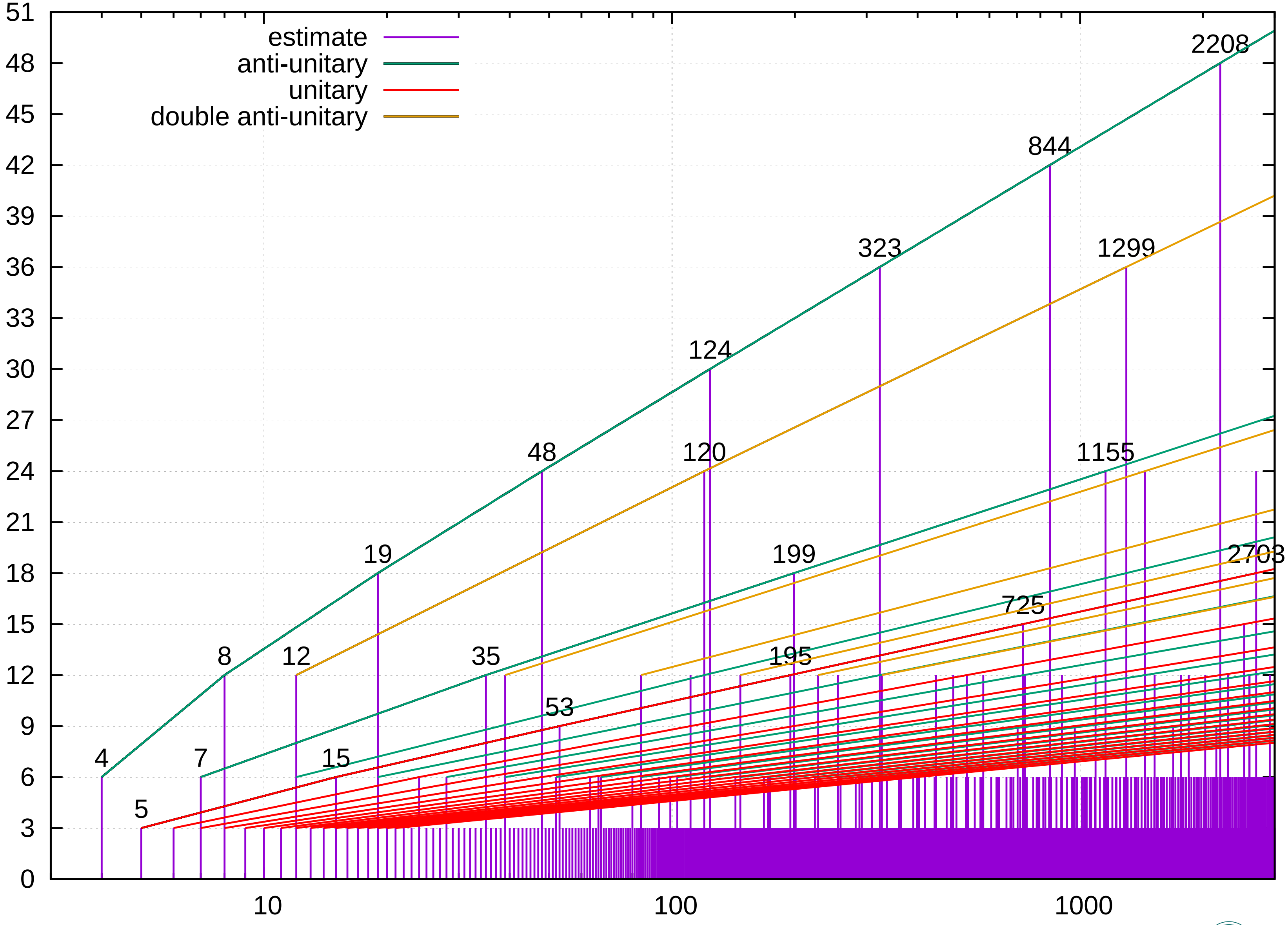
Symmetries of SIC-POVMs



Symmetries of SIC-POVMs



Symmetries of SIC-POVMs



Symmetries of SIC-POVMs