SIC-POVMs

The Elusive 'Standard Quantum Measurement'

Peter Wadel

University of Regina

Canadian Undergraduate Mathematics Conference, June 2023

Table of Contents

Closed quantum systems

- Physicists want to be able to study closed quantum systems

Closed quantum systems

- Physicists want to be able to study closed quantum systems
  - eg. trapped and ultracold particles, such as those in a quantum computer

Closed quantum systems

- Physicists want to be able to study closed quantum systems
  - eg. trapped and ultracold particles, such as those in a quantum computer
- A quantum state is a way of assigning numbers to the various observable properties of the system

Closed quantum systems

- Physicists want to be able to study closed quantum systems
  - eg. trapped and ultracold particles, such as those in a quantum computer
- A quantum state is a way of assigning numbers to the various observable properties of the system
- In closed systems, the state of a system is preserved as time passes (unitary evolution)

Quantum measurements of closed quantum systems

- Any interaction of a closed system with the external world breaks its isolation, **including making measurements**

Quantum measurements of closed quantum systems

- Any interaction of a closed system with the external world breaks its isolation, **including making measurements**
- This means that an observed system no longer follows unitary evolution, and thus its quantum state collapses

Quantum measurements of closed quantum systems

- Any interaction of a closed system with the external world breaks its isolation, **including making measurements**
- This means that an observed system no longer follows unitary evolution, and thus its quantum state collapses
- Since the collapse is probabilistic, a mathematical framework is required to accurately describe the system's evolution

Quantum measurements of closed quantum systems

- Any interaction of a closed system with the external world breaks its isolation, **including making measurements**
- This means that an observed system no longer follows unitary evolution, and thus its quantum state collapses
- Since the collapse is probabilistic, a mathematical framework is required to accurately describe the system's evolution
- Here is the role of quantum measurement theory

Mathematical description of quantum measurements

Consider the following objects:

- a non-empty set X, interpreted as a sample space of measurement outcomes;
- a σ-algebra Σ_X of subsets E of X, interpreted as measurement events;
- a Hilbert space $\mathcal{H}$ with inner product $\langle \cdot, \cdot \rangle$, interpreted as a set containing the possible pure states of a quantum system.

Mathematical description of quantum measurements

Consider the following objects:

- a non-empty set X, interpreted as a sample space of measurement outcomes;
- a σ-algebra Σ_X of subsets E of X, interpreted as measurement events;
- a Hilbert space $\mathcal{H}$ with inner product $\langle \cdot, \cdot \rangle$, interpreted as a set containing the possible pure states of a quantum system.

Definition

A **quantum measurement** or **operator-valued measure** is a map $\nu : \Sigma_X \to \mathcal{B}(\mathcal{H})$ that is weakly countably-additive. I.e.,

$$\left\langle \nu \left(\bigcup_{k \in \mathbb{N}} E_k \right) x, y \right\rangle = \sum_{k \in \mathbb{N}} \langle \nu(E_k) x, y \rangle ,$$

for every pairwise-disjoint family $\{E_k\}_{k \in \mathbb{N}} \subset \Sigma_X$, and every x, $y \in \mathcal{H}$. In addition, if $\nu(X) = I$, then ν is called a **quantum probability measurement**.

Remark

Suppose X is a countable set and let $\Sigma_X = \mathscr{P}(X)$ be the power set of X. Then any quantum measurement ν on X is uniquely determined by the collection of operators

$$M_x = \nu(\{x\}), \;\; x \in X,$$

called **measurement operators**.

Remark

Suppose X is a countable set and let $\Sigma_X = \mathscr{P}(X)$ be the power set of X. Then any quantum measurement ν on X is uniquely determined by the collection of operators

$$M_x = \nu(\{x\}), \quad x \in X,$$

called **measurement operators**.

If the state of the quantum system before the measurement is $\psi \in \mathcal{H}$, $\|\psi\| = 1$, then the new state ψ_x of the system after the measurement is

$$\psi_x = \frac{M_x \psi}{\|M_x \psi\|}.$$

Remark

Suppose X is a countable set and let $\Sigma_X = \mathscr{P}(X)$ be the power set of X. Then any quantum measurement ν on X is uniquely determined by the collection of operators

$$M_x = \nu(\{x\}), \;\; x \in X,$$

called **measurement operators**.

If the state of the quantum system before the measurement is $\psi \in \mathcal{H}$, $\|\psi\| = 1$, then the new state ψ_x of the system after the measurement is

$$\psi_x = \frac{M_x \psi}{\|M_x \psi\|}.$$

If ν satisfies the relation $\sum_{x \in X} M_x^* M_x = I$, then the probability that the result x occurs is given by

$$p(x) = \|M_x \psi\|^2.$$

Two important classes of quantum probability measurements: POVMs and PVMs

Definition

A quantum probability $\nu : \Sigma_X \to \mathcal{B}(\mathcal{H})$ is said to be a **positive operator-valued measure** (POVM) on X if

$$\nu(E) \geq 0 \text{ for every } E \in \Sigma_X.$$

A POVM $\nu : \Sigma_X \to \mathcal{B}(\mathcal{H})$ is said to be a **projection-valued measure** (PVM), or a **projective quantum probability measure**, on X if

$$\nu(E \cap F) = \nu(E)\nu(F),$$

for all E, $F \in \Sigma_X$

Naimark's dilation theorem shows that any POVM can be obtained from a PVM acting on a larger space.

Remark

Suppose X is a countable set, and let $\{M_x\}_{x \in X} \subset \mathcal{B}(\mathcal{H})$ be measurement operators over X. Then:

- *if $M_x \geq 0$, for all $x \in X$, and $\sum_{x \in X} M_x = I$, then $\{M_x\}_{x \in X}$ is a POVM;*
- *if $M_x^2 = M_x = M_x^*$, for all $x \in X$, and $\sum_{x \in X} M_x = I$, then $\{M_x\}_{x \in X}$ is a PVM.*

Informationally complete positive operator-valued measures (IC-POVMs)

Let X be a finite set, $X = \{1, 2, \cdots, n\}$, and $\mathcal{H}$ be a d-dimensional Hilbert space, $\mathcal{H} = \mathbb{C}^d$.

Definition

A POVM $\{M_i\}_{i=1}^n \subset \mathcal{B}(\mathcal{H}) \cong M_d(\mathbb{C})$ is called **informationally complete** (*IC-POVM*) if $\{M_i\}_{i=1}^n$ spans the real vector space of all self-adjoint operators $A = A^* \in M_d(\mathbb{C})$.

Informationally complete positive operator-valued measures (IC-POVMs)

Let X be a finite set, $X = \{1, 2, \cdots, n\}$, and $\mathcal{H}$ be a d-dimensional Hilbert space, $\mathcal{H} = \mathbb{C}^d$.

Definition

A POVM $\{M_i\}_{i=1}^{n} \subset \mathcal{B}(\mathcal{H}) \cong M_d(\mathbb{C})$ is called **informationally complete** (*IC-POVM*) if $\{M_i\}_{i=1}^{n}$ spans the real vector space of all self-adjoint operators $A = A^* \in M_d(\mathbb{C})$.

- Any state can be written as a linear combination of the IC-POVM elements with real coefficients;

Informationally complete positive operator-valued measures (IC-POVMs)

Let X be a finite set, $X = \{1, 2, \cdots, n\}$, and $\mathcal{H}$ be a d-dimensional Hilbert space, $\mathcal{H} = \mathbb{C}^d$.

Definition

A POVM $\{M_i\}_{i=1}^n \subset \mathcal{B}(\mathcal{H}) \cong M_d(\mathbb{C})$ is called **informationally complete** (*IC-POVM*) if $\{M_i\}_{i=1}^n$ spans the real vector space of all self-adjoint operators $A = A^* \in M_d(\mathbb{C})$.

- Any state can be written as a linear combination of the IC-POVM elements with real coefficients;
- If $\{M_i\}_{i=1}^n$ is an IC-POVM, then $n \geq d^2$. If $n = d^2$, then we say that $\{M_i\}_{i=1}^n$ is a **minimal IC-POVM**, or a *MIC*;

Informationally complete positive operator-valued measures (IC-POVMs)

Let X be a finite set, $X = \{1, 2, \cdots, n\}$, and $\mathcal{H}$ be a d-dimensional Hilbert space, $\mathcal{H} = \mathbb{C}^d$.

Definition

A POVM $\{M_i\}_{i=1}^n \subset \mathcal{B}(\mathcal{H}) \cong M_d(\mathbb{C})$ is called **informationally complete** (*IC-POVM*) if $\{M_i\}_{i=1}^n$ spans the real vector space of all self-adjoint operators $A = A^* \in M_d(\mathbb{C})$.

- Any state can be written as a linear combination of the IC-POVM elements with real coefficients;
- If $\{M_i\}_{i=1}^n$ is an IC-POVM, then $n \geq d^2$. If $n = d^2$, then we say that $\{M_i\}_{i=1}^n$ is a **minimal IC-POVM**, or a *MIC*;
- MICs can be constructed in any dimension d.

Symmetric informationally complete positive operator-valued measures (SIC-POVMs)

Definition

A MIC $\{M_i\}_{i=1}^{d^2}$ is said to be **symmetric** (or a *SIC-POVM* or *SIC* for short) if

$$M_i = \frac{1}{d}\Pi_i,\ 1 \leq i \leq d^2,$$

where $\{\Pi_i\}_{i=1}^{d^2}$ are rank-1 projections that have equal pairwise Hilbert–Schmidt inner products

$$\langle \Pi_i, \Pi_j \rangle = \mathrm{tr}(\Pi_i \Pi_j) = \begin{cases} 1 & i = j \\ \frac{1}{d+1} & i \neq j \end{cases}.$$

Symmetric informationally complete positive operator-valued measures (SIC-POVMs)

Definition

A MIC $\{M_i\}_{i=1}^{d^2}$ is said to be **symmetric** (or a *SIC-POVM* or *SIC* for short) if

$$M_i = \frac{1}{d}\Pi_i,\ 1 \leq i \leq d^2,$$

where $\{\Pi_i\}_{i=1}^{d^2}$ are rank-1 projections that have equal pairwise Hilbert–Schmidt inner products

$$\langle \Pi_i, \Pi_j \rangle = \mathrm{tr}(\Pi_i \Pi_j) = \begin{cases} 1 & i = j \\ \frac{1}{d+1} & i \neq j \end{cases}.$$

A SIC-POVM may be identified with a set of equiangular vectors or equiangular lines in $\mathbb{C}^d$.

A 2-dimensional example

Suppose $d = 2$ and take an orthonormal basis $\{v_0, v_1\}$ for $\mathcal{H} = \mathbb{C}^2$. Set

$$\begin{aligned}
\psi_1 &= v_0 \\
\psi_2 &= \frac{1}{\sqrt{3}} v_0 + \sqrt{\frac{2}{3}} v_1 \\
\psi_3 &= \frac{1}{\sqrt{3}} v_0 + \sqrt{\frac{2}{3}} e^{i\frac{2\pi}{3}} v_1 \\
\psi_4 &= \frac{1}{\sqrt{3}} v_0 + \sqrt{\frac{2}{3}} e^{i\frac{4\pi}{3}} v_1
\end{aligned}$$

and

$$\Pi_i = \psi_i \psi_i^*, \quad 1 \leq i \leq 4.$$

Then $\{\frac{1}{2}\Pi_i\}_{1 \leq i \leq 4}$ is a SIC.

Zauner's Conjecture

- Unlike MICs, there is no known way to construct a SIC in an arbitrary dimension.

Conjecture (Zauner, 1999)

There exists a SIC-POVM in $M_d(\mathbb{C})$, for every $d \geq 2$.

Zauner's Conjecture

- Unlike MICs, there is no known way to construct a SIC in an arbitrary dimension.

Conjecture (Zauner, 1999)

There exists a SIC-POVM in $M_d(\mathbb{C})$, for every $d \geq 2$.

- To date, exact examples have been found in the following dimensions: 2–28, 30, 31, 35, 37–39, 42, 43, 48, 49, 52, 53, 57, 61–63, 67, 73, 74, 78, 79, 84, 91, 93, 95, 97–99, 103, 109, 111, 120, 124, 127, 129, 134, 143, 146, 147, 168, 172, 195, 199, 228, 259, 292, 323, 327, 399, 487, 489, 844, and 1299
- and approximate numerical examples in dimensions 2–193, 204, 224, 255, 288, 528, 725, 787, 1155, 1447, 2208, 2503, 2707, 3847, 4099, 4903, 5479, 5779, 8467, 8839, and 19603.

Group covariant SIC-POVMs

Definition (Fiducial Vector)

Let $\mathcal{E} = \{v_i v_i^*\}_{i=1}^{d^2}$ be a SIC-POVM in $\mathbb{C}^d$. If some $vv^* \in \mathcal{E}$ and subgroup U of $U(d)$ may be found such that

$$\mathcal{E} = Uv,$$

then v is known as a **fiducial vector** of $\mathcal{E}$ for the subgroup U.

Group covariant SIC-POVMs

Definition (Fiducial Vector)

Let $\mathcal{E} = \{v_i v_i^*\}_{i=1}^{d^2}$ be a SIC-POVM in $\mathbb{C}^d$. If some $vv^* \in \mathcal{E}$ and subgroup U of $U(d)$ may be found such that

$$\mathcal{E} = Uv,$$

then v is known as a **fiducial vector** of $\mathcal{E}$ for the subgroup U.

Definition (Group Covariant SIC-POVM)

Let $\mathcal{E}$ be as above. If a group G may be found such that $\mathcal{E}$ has a fiducial vector for some faithful unitary representation of G, then $\mathcal{E}$ is said to be **group covariant with respect to G or G-covariant.**

Weyl-Heisenberg SIC-POVMs

- Every SIC-POVM found to date has been group covariant.
- All but one have been $(\mathbb{Z}_d)^2$-covariant.

Weyl-Heisenberg SIC-POVMs

- Every SIC-POVM found to date has been group covariant.
- All but one have been $(\mathbb{Z}_d)^2$-covariant.

Definition (Weyl-Heisenberg SIC-POVM)

Let $\{e_i\}_{i=1}^d$ be an orthonormal basis for $\mathcal{H}$ and ω a primitive dth root of unity. A SIC-POVM is called a **Weyl-Heisenberg SIC-POVM** if it is group-covariant with respect to $\mathbb{Z}_d \times \mathbb{Z}_d$ via the map

$$(p, q) \mapsto -e^{\pi ipq/d} X_p Z_q,$$

where $X_k e_j = e_{j+k}$ and $Z_k e_j = \omega^{jk} e_j$.

Weyl-Heisenberg SIC-POVMs

- Every SIC-POVM found to date has been group covariant.
- All but one have been $(\mathbb{Z}_d)^2$-covariant.

Definition (Weyl-Heisenberg SIC-POVM)

Let $\{e_i\}_{i=1}^d$ be an orthonormal basis for $\mathcal{H}$ and ω a primitive dth root of unity. A SIC-POVM is called a **Weyl-Heisenberg SIC-POVM** if it is group-covariant with respect to $\mathbb{Z}_d \times \mathbb{Z}_d$ via the map

$$(p, q) \mapsto -e^{\pi i pq/d} X_p Z_q,$$

where $X_k e_j = e_{j+k}$ and $Z_k e_j = \omega^{jk} e_j$.

Theorem (Zhu, 2010)

In every prime dimension except 3, every group covariant SIC-POVM is covariant with respect to $\mathbb{Z}_d \times \mathbb{Z}_d$.

Future work

Open problems (hopefully easier than Zauner's conjecture):

- Is every SIC-POVM group covariant? What about in prime dimensions?

Future work

Open problems (hopefully easier than Zauner's conjecture):

- Is every SIC-POVM group covariant? What about in prime dimensions?
- Does every dimension have a Weyl-Heisenberg SIC-POVM?

Future work

Open problems (hopefully easier than Zauner's conjecture):

- Is every SIC-POVM group covariant? What about in prime dimensions?
- Does every dimension have a Weyl-Heisenberg SIC-POVM?
- The elements of all known fiducial vectors lie in certain extensions of the number field $\mathbb{Q}(\sqrt{D})$, where D is the square-free part of $(d-3)(d+1)$. Does this always hold?

References

[1] M. Appleby et al. "SIC-POVMs from Stark units". In: *J. Math. Phys.* 63.11 (2022), p. 112205. DOI: 10.1063/5.0083520.

[2] J. DeBrota. "Informationally Complete Measurements and Optimal Representations of Quantum Theory". PhD Thesis. Univserity of Massachusetts, 2020.

[3] H. Zhu. "SIC POVMs and Clifford groups in prime dimensions". In: *J. Math. Phys.* 43.30 (2010), p. 305305. DOI: 10.1088/1751-8113/43/30/305305.