① Recap: Projected least-squares quantum-state tomography

OPEN ACCESS
IOP Publishing

Made open access 9 October 2020
Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. **53** (2020) 204001 (28pp)
https://doi.org/10.1088/1751-8121/ab8111

Fast state tomography with optimal error bounds

M Guţă[1,4], J Kahn[2], R Kueng[3] and J A Tropp[3]

[1] School of Mathematical Sciences, University of Nottingham, United Kingdom
[2] Institut de Mathématiques de Toulouse, Toulouse, France
[3] California Institute of Technology, Pasadena, United States of America

- General idea: use an information-complete measurement ("IC-POVM")

(also sometimes called "tomographically-complete measurement").

$\{M_i\}_{i=1}^m$ is a measurement (POVM) $\left(\text{i.e., } M_i \geq 0 \ \forall i, \ \sum_{i=1}^m M_i = \mathbb{1}\right)$

such that $\mathrm{Span}\{M_i\}_{i=1}^m = L(\mathbb{C}^d)$. (Called a "frame" in mathematics.)

- Estimator: Least-squares estimator:

$$\hat{R} := \operatorname{argmin}\left\{ \sum_{i=1}^m \left(f_i - \mathrm{Tr}[M_i H]\right)^2 : H \text{ Hermitian} \right\}$$

Relative frequencies of measurement outcomes wrt IC-POVM $\{M_i\}_{i=1}^m$.
(Unbiased estimators of $\mathrm{Pr}[M_i \rho]$.)

- Theorem: Let $\mathcal{M}(H) = \sum_{i=1}^m \mathrm{Tr}[M_i H]\, |i\rangle\langle i|$, $F = \sum_{i=1}^m f_i\, |i\rangle\langle i|$

Then, $\hat{R} = (\mathcal{M}^\dagger \mathcal{M})^{-1}(\mathcal{M}^\dagger(F))$, $\mathcal{M}^\dagger(\cdot) = \sum_{i=1}^m \langle i|(\cdot)|i\rangle M_i$.

- Project to get a density operator estimator.

$$\hat{\rho} = \text{argmin}\{ \|\hat{R} - \sigma\|_2 : \sigma \geq 0, \text{Tr}[\sigma] = 1 \}.$$

- We then want to do a sample complexity analysis. For this, we need specific examples of IC-POVMs.

② Examples of IC-POVMs

- Theorem: In finite dimensions, a finite set $\{M_i\}_{i=1}^m$ is an IC-POVM iff M_i are Hermitian, $M_i \geq 0 \ \forall i$, $\sum_{i=1}^m M_i = \mathbb{1}$ (so $\{M_i\}_{i=1}^m$ is a POVM), and there exist $0 < a \leq b < \infty$ such that

$$= \sum_{i=1}^m \text{Tr}[X^\dagger M_i]\text{Tr}[M_i X] = \text{Tr}\left[(X^\dagger \otimes X)\left(\sum_{i=1}^m M_i \otimes M_i\right)\right]$$

$$a\,\text{Tr}[X^\dagger X] \leq \sum_{i=1}^m |\text{Tr}[M_i X]|^2 \leq b\,\text{Tr}[X^\dagger X] \quad \forall \ X \in L(\mathbb{C}^d).$$

(a) Minimal IC-POVM (MIC-POVM) : contains d^2 elements.

- Necessarily linearly independent.
- Known to exist in all dimensions!
- Explicit construction: consider the following set of d^2 density operators:

$$\frac{1}{\sqrt{2}}(|2\rangle + |3\rangle)$$

$$M = \sum_{a,b} m_{a,b} |a\rangle\langle b| \qquad \rho_{a,b} = \begin{cases} |a\rangle\langle a|, & \text{if } a = b \\ |+_{(a,b)}\rangle\langle +_{(a,b)}|, & \text{if } a < b \\ |+i_{(a,b)}\rangle\langle +i_{(a,b)}|, & \text{if } a > b \end{cases} \qquad \begin{aligned} |+_{(a,b)}\rangle &= \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle) \\ |+i_{(a,b)}\rangle &= \frac{1}{\sqrt{2}}(|a\rangle + i|b\rangle). \end{aligned}$$

Then, for $a < b$:

$$|a\rangle\langle b| = \left(\rho_{a,b} - \tfrac{1}{2}\rho_{a,a} - \tfrac{1}{2}\rho_{b,b}\right) - i\left(\rho_{b,a} - \tfrac{1}{2}\rho_{a,a} - \rho_{b,b}\right)$$

$$|b\rangle\langle a| = \left(\rho_{a,b} - \tfrac{1}{2}\rho_{a,a} - \tfrac{1}{2}\rho_{b,b}\right) + i\left(\rho_{b,a} - \tfrac{1}{2}\rho_{a,a} - \rho_{b,b}\right)$$

$$\Rightarrow L(\mathbb{C}^d) = \text{span}\{ |a\rangle\langle b| : 0 \leq a \leq b \leq d-1 \} = \text{span}\{ \rho_{a,b} : 0 \leq a \leq b \leq d-1 \}.$$

Now, $Q = \sum_{a,b=0}^{d-1} \rho_{a,b} \rightarrow$ invertible, by linear independence of $\{\rho_{a,b}\}_{a,b=0}^{d-1}$.

$$\boxed{M_{a,b} := Q^{-\frac{1}{2}} \rho_{a,b} Q^{-\frac{1}{2}}}$$

$\rightarrow$ This is an example of a "pretty-good measurement" (used in hypothesis testing).

$$\sum_{a,b=0}^{d-1} M_{a,b} = \sum_{a,b=0}^{d-1} Q^{-\frac{1}{2}} \rho_{a,b} Q^{-\frac{1}{2}} = Q^{-\frac{1}{2}} \Big(\underbrace{\sum_{a,b} \rho_{a,b}}_{Q} \Big) Q^{-\frac{1}{2}} = Q^{-\frac{1}{2}} Q Q^{-\frac{1}{2}} = \mathbb{1} \checkmark$$

$$Q = Q^{\frac{1}{2}} Q^{\frac{1}{2}}$$

$\{\rho_1, \rho_2, \rho_3\}$

A 'pretty good' measurement for distinguishing quantum states

PAUL HAUSLADEN†‡ and WILLIAM K. WOOTTERS‡

† Department of Physics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6396, USA

‡ Department of Physics, Williams College, Williamstown, Massachusetts, 01267, USA

(*Received 7 January 1994 and accepted 16 February 1994*)

(a) The Pauli-basis measurements (for one qubit)

$$\left\{ \tfrac{1}{3}|0\rangle\langle 0|, \tfrac{1}{3}|1\rangle\langle 1|, \tfrac{1}{3}|+\rangle\langle +|, \tfrac{1}{3}|-\rangle\langle -|, \tfrac{1}{3}|+i\rangle\langle +i|, \tfrac{1}{3}|-i\rangle\langle -i| \right\}$$

$$M_{0,0} = \tfrac{1}{3}|0\rangle\langle 0|, \quad M_{0,1} = \tfrac{1}{3}|1\rangle\langle 1|, \quad M_{1,0} = \tfrac{1}{3}|+\rangle\langle +|, \quad M_{1,1} = \tfrac{1}{3}|-\rangle\langle -|$$

$$M_{2,0} = \tfrac{1}{3}|+i\rangle\langle +i|, \quad M_{2,1} = \tfrac{1}{3}|-i\rangle\langle -i|$$

(Recall that $|0\rangle\langle 0| + |1\rangle\langle 1| = |+\rangle\langle +| + |-\rangle\langle -| = |+i\rangle\langle +i| + |-i\rangle\langle -i| = \mathbb{1}$.)

Let $N \in L(\mathbb{C}^2)$, $N = \frac{1}{2}(\alpha_0 \mathbb{1} + \alpha_1 X + \alpha_2 Y + \alpha_3 Z)$

$$= \tfrac{1}{2}\Big(\alpha_0 (3M_{0,0} + 3M_{0,1}) + \alpha_1 (3M_{1,0} - 3M_{1,1}) + \alpha_2 (3M_{2,0} - 3M_{2,1}) + \alpha_3 (3M_{0,0} - 3M_{0,1})\Big)$$

$$= \tfrac{3}{2}(\alpha_0 + \alpha_3) M_{0,0} + \tfrac{3}{2}(\alpha_0 - \alpha_3) M_{0,1} + \tfrac{3}{2}\alpha_1 M_{1,0} - \tfrac{3}{2}\alpha_1 M_{1,1} + \tfrac{3}{2}\alpha_2 M_{2,0} - \tfrac{3}{2}\alpha_2 M_{2,1} \quad \checkmark$$

* These are mutually-unbiased bases (MUBs)

X-basis: $\{|+\rangle, |-\rangle\}$, Y-basis: $\{|+i\rangle, |-i\rangle\}$, Z-basis: $\{|0\rangle, |1\rangle\}$.

Observe that $|\langle \pm | \pm i\rangle|^2 = \frac{1}{2}$, $|\langle 0|\pm\rangle|^2 = |\langle 0|\pm i\rangle|^2 = \frac{1}{2}$, $|\langle 1|\pm\rangle|^2 = |\langle 1|\pm i\rangle|^2 = \frac{1}{2}$.

("Measuring a state from one basis wrt to another basis leads to uniformly random outcomes.")

Two ONBs $C = \{|c\rangle\}$, $D = \{|d\rangle\}$ are called mutually unbiased if

$$|\langle c|d\rangle|^2 = \frac{1}{d} \text{ for all } c \in C \text{ and } d \in D.$$

⊛ No explicit construction is known for all d!

(b) Maximal set of MUBs.

- Known fact: at most $d+1$ MUBs can exist for any d. (An example is the $d=2$ case above!)

arXiv:quant-ph/0610216

Three Ways to Look at Mutually Unbiased Bases

Ingemar Bengtsson

Fysikum, Stockholm University, 106 91 Stockholm, Sweden

Abstract. This is a review of the problem of Mutually Unbiased Bases in finite dimensional Hilbert spaces, real and complex. Also a geometric measure of "mubness" is introduced, and applied to some explicit calculations in six dimensions (partly done by Björck and by Grassl). Although this does not yet solve any problem, some appealing structures emerge.

Journal reference: International Journal of Quantum Information **8** (2010) 535–640

arXiv:1004.3348

ON MUTUALLY UNBIASED BASES

THOMAS DURT

TONA Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussels, Belgium

thomdurt@vub.ac.be

BERTHOLD-GEORG ENGLERT

Centre for Quantum Technologies, National University of Singapore
3 Science Drive 2, Singapore 117543, Singapore
and Department of Physics, National University of Singapore
2 Science Drive 3, Singapore 117542, Singapore

cqtebg@nus.edu.sg

INGEMAR BENGTSSON

Stockholms Universitet, Fysikum, Alba Nova, 106 91 Stockholm, Sweden

ingemar@physto.se

KAROL ŻYCZKOWSKI

Instytut Fizyki Uniwersytetu Jagiellońskiego, ul. Reymonta 4, 30-059 Kraków, Poland
and Centrum Fizyki Teoretycznej PAN, Al. Lotników 32/44, 02-668 Warszawa, Poland

karol@tatry.if.uj.edu.pl

• Known fact: Maximal MUBs form a "complex-projective 2-design"

(c) Complex-projective two designs

(※ Similar to unitary 2-designs that we saw earlier!)

• Consider a set $\{|v_i\rangle\langle v_i|\}_{i=1}^{m}$ of rank-one projectors.

– It is called a complex-projective one-design if

$\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{\mathbb{1}}{2}$

$$\frac{1}{m}\sum_{i=1}^{m} |v_i\rangle\langle v_i| = \frac{\mathbb{1}}{d} \Rightarrow \left\{\frac{d}{m}|v_i\rangle\langle v_i|\right\}_{i=1}^{m} \text{ is a POVM.}$$

– It is called a complex-projective two-design if

$$\frac{1}{m}\sum_{i=1}^{m} \left(|v_i\rangle\langle v_i|\right)^{\otimes 2} = \frac{1}{d(d+1)}\left(\mathbb{1}\otimes\mathbb{1} + F\right)$$

Swap operator! Recall:

$$F = \sum_{i,j=0}^{d-1} |j,i\rangle\langle i,j|$$

$$\frac{1}{M}\sum_{j=1}^{M} (u_j\otimes u_j) X (u_j\otimes u_j)^{\dagger} = \alpha\, \mathbb{1}\otimes\mathbb{1} + \beta F$$

Aside: Complex-projective k-design if

$$\frac{1}{m}\sum_{i=1}^{m} \left(|v_i\rangle\langle v_i|\right)^{\otimes k} = \int d\psi \left(|\psi\rangle\langle\psi|\right)^{\otimes k}.$$

Fubini-Study measure.
(Similar to Haar measure.)

https://sumeetkhatri.wordpress.com/wp-content/uploads/2020/05/random_pure_states.pdf

Random Pure States

Sumeet Khatri

May 31, 2020

• Let $\{U_i\}_{i=1}^{m}$ be a unitary 2-design (e.g., Clifford unitaries). Then,

Set $|v_i\rangle = U_i|0\rangle$. Then,

$$\frac{1}{m}\sum_{i=1}^{m}\left(|v_i\rangle\langle v_i|\right)^{\otimes 2} = \frac{1}{m}\sum_{i=1}^{m}\left(U_i|0\rangle \otimes U_i|0\rangle\right)\left(\langle 0|U_i^{\dagger} \otimes \langle 0|U_i^{\dagger}\right)$$

$$= |v_i\rangle\langle v_i| \otimes |v_i\rangle\langle v_i|$$

$$= \left(|v_i\rangle \otimes |v_i\rangle\right)\left(\langle v_i| \otimes \langle v_i|\right)$$

$$= \frac{1}{m}\sum_{i=1}^{m}\left(U_i \otimes U_i\right)\left(|0,0\rangle\langle 0,0|\right)\left(U_i \otimes U_i\right)^{\dagger}$$

$$= \alpha\, \mathbb{1}\otimes\mathbb{1} + \beta F$$

$$\alpha = \frac{1}{d^2-1}\left(\underbrace{\mathrm{Tr}[\mathbb{1}(\cdot)]}_{=1} - \frac{1}{d}\underbrace{\mathrm{Tr}[F(\cdot)]}_{=1}\right) = \frac{1}{d^2-1}\left(1-\frac{1}{d}\right)$$

$$= \frac{1}{d(d+1)}$$

$$|0,0\rangle\langle 0,0|$$

$$\beta = \frac{1}{d^2-1}\left(\mathrm{Tr}[F(\cdot)] - \frac{1}{d}\mathrm{Tr}[\mathbb{1}(\cdot)]\right)$$

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

$$= \frac{1}{d(d+1)}\left(\mathbb{1}\otimes\mathbb{1} + F\right)$$

⊛ For every unitary 2-design $\{U_i\}_{i=1}^{m}$, the set $\{U_i|0\rangle\}_{i=1}^{m}$ is a complex-projective 2-design.

• Let $\mathcal{C} = \{C_i\}_{i=1}^{m}$ be the n-qubit Clifford unitaries (which form a unitary 2-design).

The states $|v_i\rangle = C_i|0\rangle^{\otimes n}$ are called <u>stabilizer states</u>

(d) <u>Stabilier states</u> (See Nielsen-Chuang + Gottesman books).

(Prominent in quantum error correction)

• Consider n-qubit Pauli group with phases:

$$\hat{\mathcal{P}}_n = \{\pm\mathbb{1}, \pm i\mathbb{1}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}^{\otimes n}$$

- Consider a subgroup $S \leq \hat{\mathcal{P}}_n$, which is abelian (all elements mutually commute) and $-\mathbb{1} \notin S$.

$$V_S = \{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$$

This is a subspace of stabilizer states.

- If S has r generators, then $\dim(V_S) = 2^{n-r}$.
- Total # of n-qubit stabilizer states is $2^n \prod_{k=0}^{n-1} (2^{n-k}+1)$. $\approx 2^{n^2/2+\cdots}$

PHYSICAL REVIEW A **70**, 052328 (2004)

Improved simulation of stabilizer circuits

Scott Aaronson*
Computer Science Department, University of California, Berkeley, California 94720, USA

Daniel Gottesman†
Perimeter Institute, Waterloo, Canada N2L 2Y5
(Received 25 June 2004; published 30 November 2004)

Theorem 1. Given an n-qubit state $|\psi\rangle$, the following are equivalent.

(i) $|\psi\rangle$ can be obtained from $|0\rangle^{\otimes n}$ by CNOT, Hadamard, and phase gates only.

(ii) $|\psi\rangle$ can be obtained from $|0\rangle^{\otimes n}$ by CNOT, Hadamard, phase, and measurement gates only.

(iii) $|\psi\rangle$ is stabilized by exactly 2^n Pauli operators.

(iv) $|\psi\rangle$ is uniquely determined by $S(|\psi\rangle) = \mathrm{Stab}(|\psi\rangle) \cap \mathcal{P}_n$, or the group of Pauli operators that stabilize $|\psi\rangle$.

Because of Theorem 1, we call any circuit consisting entirely of CNOT, Hadamard, phase, and measurement gates a *stabilizer circuit*, and any state obtainable by applying a stabilizer circuit to $|0\rangle^{\otimes n}$ a *stabilizer state*. As a warmup to our later results, the following proposition counts the number of stabilizer states.

Proposition 1. Let N be the number of pure stabilizer states on n qubits. Then

$$N = 2^n \prod_{k=0}^{n-1} (2^{n-k}+1) = 2^{[1/2+o(1)]n^2}.$$

✱ Recall that Clifford unitaries are generated by H, CNOT, S

$\Rightarrow C_i|0\rangle^{\otimes n} \equiv |v_i\rangle$ are stabilizer states

$\Rightarrow$ Stabilizer states form a complex-projective 2-design.

(e) SIC-POVM $\rightarrow$ "symmetric"

$$\sum_{i=1}^{m} |v_i\rangle\langle v_i| = \mathbb{1}$$

- A MIC-POVM (d^2 elements)
- $\{|v_i\rangle\}_{i=1}^{m}$ such that $|\langle v_i|v_j\rangle|^2 = \frac{1}{d+1}$ $i \neq j$ ("equiangular lines").
- Not known whether they exist for all d! (But conjectured to exist for all d — "Zauner's conjecture").

A CONSTRUCTIVE APPROACH TO ZAUNER'S CONJECTURE VIA THE STARK CONJECTURES

MARCUS APPLEBY, STEVEN T. FLAMMIA, AND GENE S. KOPP

ABSTRACT. We propose a construction of d^2 complex equiangular lines in $\mathbb{C}^d$, also known as SICs or SIC-POVMs, which were conjectured by Zauner to exist for all d. The construction gives a putatively complete list of SICs with Weyl–Heisenberg symmetry in all dimensions $d > 3$. Specifically, we give an explicit expression for an object that we call a ghost SIC, which is constructed from the real multiplication values of a special function and which is Galois conjugate to a SIC. The special function, the Shintani–Faddeev modular cocycle, is more precisely a tuple of meromorphic functions indexed by a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We prove that our construction gives a valid SIC in every case assuming two conjectures: the order 1 abelian Stark conjecture for real quadratic fields and a special value identity for the Shintani–Faddeev modular cocycle. The former allows us to prove that the ghost and the SIC are Galois conjugate over an extension of $\mathbb{Q}(\sqrt{\Delta})$ where $\Delta = (d+1)(d-3)$, while the latter allows us to prove idempotency of the presumptive fiducial projector. We provide computational tests of our SIC construction by cross-validating it with known solutions, particularly the extensive work of Scott and Grassl, and by constructing four numerical examples of nonequivalent SICs in $d = 100$, three of which are new. We further consider rank-r generalizations called r-SICs given by maximal equichordal configurations of r-dimensional complex subspaces. We give similar conditional constructions for r-SICs for all r, d such that $r(d-r)$ divides (d^2-1). Finally, we study the structure of the field extensions conjecturally generated by the r-SICs. If K is any real quadratic field, then either every abelian Galois extension of K, or else every abelian extension for which 2 is unramified, is generated by our construction; the former holds for a positive density of field discriminants.

- Also form a complex-projective 2-design.

JOURNAL OF MATHEMATICAL PHYSICS VOLUME 45, NUMBER 6 JUNE 2004

Symmetric informationally complete quantum measurements

Joseph M. Renes
Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156

Robin Blume-Kohout
Theoretical Division, LANL, MS-B213, Los Alamos, New Mexico 87545

A. J. Scott and Carlton M. Caves
Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156

(Received 24 October 2003; accepted 25 February 2004; published online 6 May2004)

(3) Projected Least-Squares Tomography with Complex-Projective 2-Designs.

- Let $\{|v_i\rangle\}_{i=1}^{m}$ be a complex-projective 2-design

$\Rightarrow \{M_i = \frac{d}{m}|v_i\rangle\langle v_i|\}_{i=1}^{m}$ is an IC-POVM.

$$\frac{1}{m}\sum_{i=1}^{m}\left(|v_i\rangle\langle v_i|\right)^{\otimes 2} = \frac{1}{d(d+1)}\left(\mathbb{1}\otimes\mathbb{1} + F\right)$$ $\rightarrow$ Take partial trace over second tensor factor.

$$F = \sum_{i,j=0}^{d-1} |j,i\rangle\langle i,j|$$

$$\Rightarrow \frac{1}{m}\sum_{i=1}^{m} \mathrm{Tr}_2\left[|v_i\rangle\langle v_i| \otimes \underbrace{|v_i\rangle\langle v_i|}\right] = \frac{1}{d(d+1)}\mathrm{Tr}_2\left[\mathbb{1}\otimes\mathbb{1} + F\right]$$

$$\mathrm{Tr}_2[F] = \sum_{i,j=0}^{d-1} \delta_{i,j}\, |j\rangle\langle i| = \mathbb{1}$$

$$\Rightarrow \frac{1}{m}\sum_{i=1}^{m} |v_i\rangle\langle v_i| = \frac{1}{d(d+1)}\left(d\mathbb{1}+\mathbb{1}\right) = \frac{1}{d}\mathbb{1} \Rightarrow \sum_{i=1}^{m} \underbrace{\frac{d}{m}|v_i\rangle\langle v_i|}_{M_i} = \mathbb{1}. \quad \checkmark$$

Recall frame condition:

$$a\,\mathrm{Tr}[X^\dagger X] \le \sum_{i=1}^{m} |\mathrm{Tr}[M_i X]|^2 \le b\,\mathrm{Tr}[X^\dagger X] \quad \forall\ X \in L(\mathbb{C}^d).$$

$$= \sum_{i=1}^{m} \mathrm{Tr}[X^\dagger M_i]\mathrm{Tr}[M_i X] = \mathrm{Tr}\left[\left(X^\dagger \otimes X\right)\left(\sum_{i=1}^{m} M_i \otimes M_i\right)\right]$$

⊛ It can be shown that $a = b = \frac{1}{d(d+1)}$

- Least-squares estimator is $\hat{R} = (\mathcal{M}^\dagger\mathcal{M})^{-1}\left(\mathcal{M}^\dagger(F)\right)$, $F = \sum_{i=1}^{m} f_i |i\rangle\langle i|$

$$\mathcal{M}(H) = \sum_{i=1}^{m} \mathrm{Tr}[M_i H]\,|i\rangle\langle i|, \qquad \mathcal{M}^\dagger(\cdot) = \sum_{i=1}^{m} \langle i|(\cdot)|i\rangle M_i.$$

$M_i \to \frac{d}{m}|v_i\rangle\langle v_i|$

Now, $$(\mathcal{M}^\dagger\mathcal{M})(H) = \sum_{i=1}^{m} \mathrm{Tr}[M_i H] M_i = \mathrm{Tr}_1\left[\underbrace{\left(\sum_{i=1}^{m} M_i \otimes M_i\right)}\left(H \otimes \mathbb{1}\right)\right]$$

$$= \sum_{i=1}^{m} \frac{d}{m}|v_i\rangle\langle v_i| \otimes \frac{d}{m}|v_i\rangle\langle v_i|$$

$$= \frac{d^2}{m}\cdot\frac{1}{m}\sum_{i=1}^{m}\left(|v_i\rangle\langle v_i|\right)^{\otimes 2}$$

$$= \frac{d^2}{m}\frac{1}{d(d+1)}\left(\mathbb{1}\otimes\mathbb{1}+F\right)$$

$$\mathrm{Tr}_1\left[\underline{(\mathbb{1}\otimes\mathbb{1}+F)}\,\underline{(H\otimes\mathbb{1})}\right]$$

$$= \mathrm{Tr}_1\left[H\otimes\mathbb{1} + F(H\otimes\mathbb{1})\right]$$

$$= \mathrm{Tr}_1[H\otimes\mathbb{1}] + \mathrm{Tr}_1[F(H\otimes\mathbb{1})]$$

$$= \mathrm{Tr}[H]\mathbb{1} + \mathrm{Tr}_1[F(H\otimes\mathbb{1})]$$

$$= \frac{d}{m(d+1)}\left(\mathrm{Tr}[H]\mathbb{1} + \underbrace{\mathrm{Tr}_1[(H\otimes\mathbb{1})F]}\right)$$

$$F = \sum_{i,j=0}^{d-1} |j,i\rangle\langle i,j|$$

$$= \sum_{i,j=0}^{d-1} \mathrm{Tr}_1\left[(H\otimes\mathbb{1})|i,j\rangle\langle j,i|\right]$$

$|i\rangle\langle j| \otimes |j\rangle\langle i|$

$\mathrm{Tr}_1[AB\otimes C]$

$\mathrm{Tr}[AB]C$

$$= \sum_{i,j=0}^{d-1} \mathrm{Tr}[H|i\rangle\langle j|]\,|j\rangle\langle i| = \sum_{i,j=0}^{d-1} \langle j|H|i\rangle\,|j\rangle\langle i|$$

$|j\rangle\langle j|H|i\rangle\langle i|$

$$= \left(\sum_{j=0}^{d-1} |j\rangle\langle j|\right) H \left(\sum_{i=0}^{d-1} |i\rangle\langle i|\right)$$

$$= H$$

$$\Rightarrow (\mathcal{M}^\dagger \mathcal{M})(H) = \frac{d}{m(d+1)} \left(\mathrm{Tr}[H]\mathbb{1} + H\right)$$

⊛ Essentially a depolarizing channel!

<u>Inverse</u>: $(\mathcal{M}^\dagger\mathcal{M})^{-1}(H) = \frac{m}{d}\left((d+1)H - \mathrm{Tr}[H]\mathbb{1}\right).$

⊛ Verify: $(\mathcal{M}^\dagger\mathcal{M})^{-1}(\mathcal{M}^\dagger\mathcal{M})(H) = (\mathcal{M}^\dagger\mathcal{M})^{-1}\left(\frac{d}{m(d+1)}\left(\mathrm{Tr}[H]\mathbb{1} + H\right)\right)$

$$= \frac{d}{m(d+1)}\left(\mathrm{Tr}[H]\underbrace{(\mathcal{M}^\dagger\mathcal{M})^{-1}(\mathbb{1})}_{= \frac{m}{d}\left((d+1)\mathbb{1} - d\mathbb{1}\right) = \frac{m}{d}\mathbb{1}} + (\mathcal{M}^\dagger\mathcal{M})^{-1}(H)\right)$$

$$= \frac{d}{m(d+1)}\left(\mathrm{Tr}[H]\frac{m}{d}\mathbb{1} + \frac{m}{d}\left((d+1)H - \mathrm{Tr}[H]\mathbb{1}\right)\right)$$

$$= \frac{d}{m(d+1)}\left(\frac{m}{d}(d+1)H\right)$$

$$= H \quad \checkmark$$

Therefore, $\tilde{R} = (\mathcal{M}^\dagger\mathcal{M})^{-1}(\mathcal{M}^\dagger(F)) = \sum_{i=1}^{m} f_i (\mathcal{M}^\dagger\mathcal{M})^{-1}(M_i)$ $\quad \left(M_i = \frac{d}{m}|v_i\rangle\langle v_i|\right)$

$\mathcal{M}^\dagger(F) = \sum_{i=1}^{m} f_i M_i$

$$= \sum_{i=1}^{m} f_i \frac{m}{d}\left((d+1)M_i - \mathrm{Tr}[M_i]\mathbb{1}\right)$$

$$= \sum_{i=1}^{m} f_i \frac{m}{d}\left(\left(d+1\right)\frac{d}{m}|v_i\rangle\langle v_i| - \frac{d}{m}\mathbb{1}\right)$$

$$\Rightarrow \boxed{\hat{R} = (d+1)\sum_{i=1}^{m} f_i |v_i\rangle\langle v_i| - \mathbb{1}.}$$

Observe: $\hat{R}$ is an unbiased estimator of ρ!

Proof: $$\mathbb{E}[\hat{R}] = (d+1)\sum_{i=1}^{m} \underbrace{\mathbb{E}[f_i]}_{= p_i = \mathrm{Tr}[\rho M_i] \text{ from last time!}} |v_i\rangle\langle v_i| - \mathbb{1}$$

$$= (d+1)\sum_{i=1}^{m} \mathrm{Tr}\left[\rho \frac{d}{m}|v_i\rangle\langle v_i|\right]|v_i\rangle\langle v_i| - \mathbb{1}$$

$$= (d+1)\, d\, \mathrm{Tr}_1\left[(\rho\otimes\mathbb{1})\underbrace{\left(\frac{1}{m}\sum_{i=1}^{m}\left(|v_i\rangle\langle v_i|\right)^{\otimes 2}\right)}_{\frac{1}{d(d+1)}(\mathbb{1}\otimes\mathbb{1}+F)}\right] - \mathbb{1}$$

$$= \mathrm{Tr}_1\left[(\rho\otimes\mathbb{1})(\mathbb{1}\otimes\mathbb{1}+F)\right] - \mathbb{1}$$

$$= \underbrace{\mathrm{Tr}[\rho]}_{=1}\mathbb{1} + \underbrace{\mathrm{Tr}_1\left[(\rho\otimes\mathbb{1})F\right]}_{=\rho} - \mathbb{1}$$

$$= \rho \checkmark$$

- Sample complexity analysis.

Found Comput Math (2012) 12:389–434
DOI 10.1007/s10208-011-9099-z

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

User-Friendly Tail Bounds for Sums of Random Matrices

Joel A. Tropp

Theorem 3 (Matrix Bernstein inequality). *Consider a sequence of n independent, Hermitian random matrices $A_1, \ldots, A_n \in \mathbb{H}_d$. Assume that each A_i satisfies*

$$\mathbb{E}[A_i] = 0 \quad \text{and} \quad \|A_i\|_\infty \leqslant R \text{ almost surely.}$$

Then, for any $t > 0$

$$\Pr\left[\left\|\sum_{i=1}^{n}(A_i - \mathbb{E}[A_i])\right\|_\infty \geqslant t\right] \leqslant \begin{cases} d\exp\left(-\frac{3t^2}{8\sigma^2}\right) & t \leqslant \frac{\sigma^2}{R}, \\ d\exp\left(-\frac{3t}{8R}\right) & t \geqslant \frac{\sigma^2}{R}, \end{cases}$$

where $\sigma^2 = \left\|\sum_{i=1}^{n}\mathbb{E}[A_i^2]\right\|_\infty$.

$$\hat{R} = \frac{1}{N}\sum_{j=1}^{N} R_j, \qquad \underbrace{R_j = (d+1)\sum_{i=1}^{m} \delta_{x_{j,i}}\, |v_i \rangle\langle v_i| - \mathbb{1}}_{\text{iid random matrices, } \mathbb{E}[R_j] = \rho.} \qquad \left(f_i = \frac{1}{N}\sum_{j=1}^{N} \delta_{x_{j,i}} \right)$$

Set $A_j = \frac{1}{N} R_j - \rho \Rightarrow \mathbb{E}[A_j] = 0$ b/c R_j unbiased!