Near-optimality of the pretty good measurement for general score functions

Hemant K. Mishra, Ludovico Lami, and Mark M. Wilde

arXiv:2505.20447

Introduction.— Quantum estimation theory is crucial for understanding the extraction of accurate information from a quantum system, and it is central in metrology, quantum sensing, and quantum information processing. In its simplest form, the framework involves a *finite* parameter space $\mathcal{X}$ and an ensemble of quantum states $\mathscr{E} = \big((p(x), \rho(x))\big)_{x\in\mathcal{X}}$ on some *finite-dimensional* quantum system. The aim is to estimate the parameter x by performing a quantum measurement (POVM) on the system. The figure of merit that is typically used is the *success probability*, defined for a POVM $M = \big(M(x)\big)_{x\in\mathcal{X}}$ as

$$P_s(\mathscr{E}, M) := \sum_{x\in\mathcal{X}} p(x)\,\mathrm{Tr}[\rho(x)M(x)]\,. \tag{1}$$

In general, determining the POVM M that maximises the success probability explicitly can be quite challenging. Fortunately, for many applications this is not needed, as a measurement called the *pretty good measurement* (PGM) or *square-root measurement* [1–4] is known to perform 'pretty well'. The PGM is defined as the POVM

$$M^{\mathrm{PG}} = \big(M^{\mathrm{PG}}(x)\big)_{x\in\mathcal{X}}\,, \qquad M^{\mathrm{PG}}(x) := \rho^{-1/2}p(x)\rho(x)\,\rho^{-1/2} + p(x)\Pi_{\ker(\rho)}\,, \tag{2}$$

where $\rho := \sum_x p(x)\rho(x)$ is the average state of the ensemble, $\rho^{-1/2}$ denotes the inverse square root taken on the support of ρ, and $\Pi_{\ker(\rho)}$ is the projector onto the kernel of ρ. The importance of the PGM in different areas of quantum information processing can hardly be overestimated: in many interesting cases, it actually coincides with the optimal measurement [5–9].

The fact that the PGM is 'pretty good' is formalised by the Barnum–Knill theorem [10, Corollary 3], which states that

$$\sup_{M\in\mathrm{POVM}} P_s(\mathscr{E}, M) \leq \sqrt{P_s(\mathscr{E}, M^{\mathrm{PG}})}\,. \tag{3}$$

In other words, the optimal measurement can only yield an average success probability that is at most the square root of that of the PGM. This result can be truly considered one of the technical pillars of quantum information theory, being applied extensively throughout the field. It underpins the near optimality of the PGM for decoding classical information sent over general quantum channels, a technique used in the pioneering derivation of what is now called the Holevo–Schumacher–Westmoreland theorem [11–13]. More recently, and technically, the inequality in [14, Fact 1(vii)] (see also Eq. (A1) there), which is crucial to the elegant technique of Cheng to obtain tight one-shot bounds for classical communication, is *precisely* the Barnum–Knill theorem applied to a binary ensemble with $p(0)\rho(0) = \frac{A}{\mathrm{Tr}[A+B]}$ and $p(1)\rho(1) = \frac{B}{\mathrm{Tr}[A+B]}$.

Motivation of this work.— The above picture is simple and appealing, but it rests crucially on two seemingly innocuous assumptions: (A) the finiteness of the parameter space, and (B) the finite dimensionality of the underlying Hilbert space. Unfortunately, **dropping these assumptions causes fundamental technical and conceptual problems in both the statement and the proof of the Barnum–Knill theorem**. And yet, one can think of a wealth of physically relevant scenarios where one would want to drop either (A) or (B), or both. A prototypical example that is of interest to us is offered by **bosonic Gaussian ensembles**, which arise naturally in the context of classical communication via quantum optical channels — either over optical fibres, or satellite-based. In this case, we take $\mathcal{X} = \mathbb{R}^{2n}$ as the phase space of an n-mode bosonic system, $p(x)$ is a Gaussian probability density function over $\mathcal{X}$, and $\rho(x) = D(x)\rho(0)D(-x)$ is obtained from a fixed Gaussian state $\rho(0)$ by applying a displacement operator $D(x)$. This setting does not satisfy (A) nor (B). While it is useful to keep this example in mind, our analysis is fully general and not restricted to bosonic Gaussian ensembles.

The problems with dropping assumption (B) and considering the infinite-dimensional (separable) case are of an exquisitely technical nature: the inverse square roots in (2) are now *unbounded operators* with a domain that is strictly smaller than the Hilbert space, and they must be handled with care. The problems with dropping assumption (A) and taking $\mathcal{X}$ to be a general measurable space are, however, both technical and conceptual. To appreciate the conceptual aspect of the issue, note that **the success probability is not a meaningful figure of merit for continuous parameter spaces**. (Typically, it will be trivially equal to zero, as the set of events in which we guess the *exact* value of x, which can take continuously many values, has measure zero.) This means that not only the proof, but also the *statement* of the Barnum–Knill theorem (3) does not make sense in this context.

Summary of contributions.— In this work **we fix the above issues, generalising the Barnum–Knill theorem so that it applies to general continuous ensembles over infinite-dimensional spaces**. We begin by identifying a physically meaningful family of figures of merit that can serve as alternatives to the success probability when $\mathcal{X}$ is a general measure space. For this purpose, we introduce the notion of a *score function*: a measurable map $S\colon \mathcal{X}\times\mathcal{X}\to[0,1]$ that assigns a numerical value to the quality of a guess $\hat{x}$ when the true value of the variable is x. Taking this general approach has two advantages: first, it allows us to deal with the case of a continuous parameter space, as guesses $\hat{x}$ that are sufficiently close to x can be assigned a score $S(x,\hat{x})\approx 1$; secondly, it may also be relevant in the discrete case, when we do not want to consider all errors as equally consequential. (Consider, for example, the problem of transmitting an image: the error of assigning the wrong colour to a pixel at the output can be more or less serious depending on how distant the assigned colour is from the true colour.)

Our results apply only to *positive* score functions, i.e., functions S that can be written as

$$S(x,\hat{x}) = \int_{\mathcal{Y}} P(x,y)P(\hat{x},y)\,\pi(\mathrm{d}y)\,, \qquad \forall\, x,\hat{x}\in\mathcal{X}\,, \tag{4}$$

where $\big(\mathcal{Y},\pi(\mathrm{d}y)\big)$ is some measure space, and $P\colon \mathcal{X}\times\mathcal{Y}\to\mathbb{R}$ is a measurable function. To understand the rationale of this definition, consider the case where $\mathcal{X}$ is a finite ensemble. Then, score functions are represented by matrices $\big(S(x,\hat{x})\big)_{x,\hat{x}\in\mathcal{X}}$, and (4) simply means that such a matrix should be positive semi-definite. In particular, positive score functions are symmetric, i.e., satisfy $S(x,\hat{x})=S(\hat{x},x)$ for all $x,\hat{x}\in\mathcal{X}$.

We refer to the average score obtained by a POVM m on the ensemble $\mathcal{E}=(\mu(\mathrm{d}x),\rho)$ as the *gain*. This is defined as

$$G_{\mathcal{E},S,m} \coloneqq \int_{\mathcal{X}} \mathrm{Tr}\left[\rho(x)\int_{\mathcal{X}} S(x,\hat{x})\,m(\mathrm{d}\hat{x})\right]\mu(\mathrm{d}x)\,. \tag{5}$$

In this case, $\mathcal{X}$ is a measurable space, $\mu(\mathrm{d}x)$ is a probability measure on it, $\rho:\mathcal{X}\to\mathcal{D}(\mathcal{H})$ is a weakly measurable map that assigns a quantum state $\rho(x)$ on a separable Hilbert space $\mathcal{H}$ to each $x\in\mathcal{X}$. Furthermore, m should be thought of as a map between the σ-algebra of measurable sets on $\mathcal{X}$ to the set of positive semi-definite bounded operators on $\mathcal{X}$. In order to be a POVM, it is required to be countably additive on disjoint sets w.r.t. the strong operator topology.

The following is a detailed description of our main results:

1. In Theorem 3.1, we extend the notion of PGM to general quantum ensembles by canonically constructing the *generalised pretty good measurement* (GPGM). This includes quantum ensembles with continuous parameter space and infinite-dimensional quantum system.

2. We generalise the Barnum–Knill theorem so as to encompass the case of general ensembles $\mathcal{E}$ over separable Hilbert spaces $\mathcal{H}$. In a nutshell, we prove that, for a given ensemble and positive score function, **the optimal expected gain does not exceed the square root of the expected gain of the GPGM**. Formally:

Theorem 3.2. *Let $\mathcal{E}$ be a quantum ensemble over a measurable space $\mathcal{X}$, and let $S\colon\mathcal{X}\times\mathcal{X}\to[0,1]$ be a positive score function, satisfying* (4)*. Then the optimal expected gain for the ensemble and the given score function does not exceed the square root of the expected gain of the generalised pretty good measurement; i.e., the following inequality holds:*

$$\sup_m G_{\mathcal{E},S,m} \le \sqrt{G_{\mathcal{E},S,m^{\mathrm{PG}}}}\,, \tag{6}$$

where the supremum is over all POVMs m, and m^{PG} is the generalised pretty good measurement.

3. How powerful the above result is depends on how restrictive the constraint that the score function be positive really is. Here we argue that one can in fact apply Theorem 3.2 to some natural problems, by constructing positive score functions associated to them. Consider for example any ensemble $\mathscr{E} = (\mu(\mathrm{d}x), \rho)$ over $\mathcal{X} = \mathbb{R}^N$. (A special case of this would be, for instance, the aforementioned bosonic Gaussian ensemble.) A relevant figure of merit in this case is the *mean-square error* (MSE), defined by

$$\mathrm{MSE}(\mathscr{E}, m) := \int_{\mathbb{R}^N} \mathrm{Tr}\left[\rho(x) \int_{\mathbb{R}^N} \|x - \hat{x}\|^2 \, m(\mathrm{d}\hat{x})\right] \mu(\mathrm{d}x)\,. \tag{7}$$

What can we say about the relation between the *minimal* MSE over all measurements m and the value achieved by the GPGM? To deal with this problem, our idea is to define, for some positive definite $N \times N$ matrix $\Sigma > 0$, the associated Gaussian score function

$$S_\Sigma(x, \hat{x}) := \exp\left[-\frac{1}{2}(x - \hat{x})^\intercal \Sigma^{-1}(x - \hat{x})\right]. \tag{8}$$

It can be verified, perhaps surprisingly, that this score function is positive! Applying our Theorem 3.2 and using the key observation that

$$\mathrm{MSE}(\mathscr{E}, m) = \lim_{t \searrow 0} \frac{2}{t} \left(1 - G_{\mathscr{E}, S_{tI}, m}\right) \tag{9}$$

to turn gain estimates into mean square error estimates leads us to the following result:

Theorem 3.3. *For an arbitrary quantum ensemble $\mathscr{E} := \big(\mu(\mathrm{d}x), \rho\big)$ and quantum measurement m, the following inequality holds:*

$$\mathrm{MSE}\big(\mathscr{E}, m^{\mathrm{PG}}\big) \leq 2\, \mathrm{MSE}(\mathscr{E}, m)\,. \tag{10}$$

Theorem 3.3 establishes near-optimality of the GPGM in the Bayesian estimation of unknown parameters of a quantum ensemble. As a special case of this result, the GPGM for bosonic Gaussian ensembles, previously studied in [15–18], indeed does pretty well for the parameter estimation task. Since the GPGM of a bosonic Gaussian ensemble is known to be Gaussian [15] and its MSE is explicitly available [18], it is a desirable theoretical and practical tool in Bayesian estimation of unknown parameters in bosonic Gaussian ensembles.

4. We state and prove two mathematically interesting results related to integration of real-valued functions with respect to operator-valued measures. These results are needed for rigorously proving the main results of our paper.

   (a) The integration of a bounded real-valued measurable function with respect to a self-adjoint positive trace-class operator-valued measure is a self-adjoint trace-class operator (Theorem A.1).

   (b) The integration of a bounded real-valued measurable function with respect to a self-adjoint positive Hilbert–Schmidt operator-valued measure is a self-adjoint Hilbert–Schmidt operator (Theorem A.4).

[1] Viacheslav Belavkin. Optimal distinction of non-orthogonal quantum signals. *Radio Engineering and Electronic Physics*, 20:39–47, 1975.

[2] Viacheslav Belavkin. Optimal multiple quantum statistical hypothesis testing. *Stochastics*, 1:315–345, 1975.

[3] Alexander S. Holevo. On asymptotically optimal hypothesis testing in quantum statistics. *Theory of Probability & Its Applications*, 23(2):411–415, 1979.

[4] Paul Hausladen and William K. Wootters. A "pretty good" measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385–2390, December 1994.

[5] Y.C. Eldar and G.D. Forney. On quantum detection and the square-root measurement. *IEEE Transactions on Information Theory*, 47(3):858–872, March 2001. arXiv:quant-ph/0005132.

[6] Y.C. Eldar, A. Megretski, and G.C. Verghese. Designing optimal quantum detectors via semidefinite programming. *IEEE Transactions on Information Theory*, 49(4):1007–1012, April 2003. arXiv:quant-ph/0205178.

[7] Dave Bacon, Andrew M Childs, and Wim van Dam. Optimal measurements for the dihedral hidden subgroup problem. *Chicago Journal of Theoretical Computer Science*, 2006(2), October 2006. arXiv:quant-ph/0501044.

[8] Carlos Mochon. Family of generalized "pretty good" measurements and the minimal-error pure-state discrimination problems for which they are optimal. *Physical Review A*, 73:032328, March 2006. arXiv:quant-ph/0506061.

[9] Felix Leditzky. Optimality of the pretty good measurement for port-based teleportation. *Letters in Mathematical Physics*, 112(5):98, October 2022. arXiv:2008.11194.

[10] Howard Barnum and Emmanuel Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *Journal of Mathematical Physics*, 43(5):2097–2106, May 2002. arXiv:quant-ph/0004088.

[11] Paul Hausladen, Richard Jozsa, Benjamin Schumacher, Michael D. Westmoreland, and William K. Wootters. Classical information capacity of a quantum channel. *Physical Review A*, 54:1869–1876, 1996.

[12] Benjamin Schumacher and Michael D. Westmoreland. Sending classical information via noisy quantum channels. *Physical Review A*, 56:131–138, 1997.

[13] Alexander S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269–273, 1998.

[14] H.-C. Cheng. Simple and tighter derivation of achievability for classical communication over quantum channels. *PRX Quantum*, 4:040330, 2023.

[15] Alexander S. Holevo. Gaussian maximizers for quantum Gaussian observables and ensembles. *IEEE Transactions on Information Theory*, 66(9):5634–5641, April 2020. arXiv:1908.03038.

[16] Alexander S. Holevo. On the classical capacity of general quantum Gaussian measurement. *Entropy*, 23(3):377, March 2021. arXiv:2101.00423.

[17] Alexander S. Holevo. Accessible information of a general quantum Gaussian ensemble. *Journal of Mathematical Physics*, 62(9):092201, September 2021. arXiv:2102.01981.

[18] Hemant K. Mishra, Ludovico Lami, Prabha Mandayam, and Mark M. Wilde. Pretty good measurement for bosonic Gaussian ensembles. *International Journal of Quantum Information*, 22(5):2440010, August 2024. arXiv:2303.04949.