FACULTY OF SCIENCE
PALACKÝ UNVERSITY OLOMOUC

Department of Optics

Positivity constraints in quantum protocols of optical signal characterization

DIPLOMA THESIS

Dominik Koutný

2017

FACULTY OF SCIENCE
PALACKÝ UNVERSITY OLOMOUC

Department of Optics

Positivity constraints in quantum protocols of optical signal characterization

DIPLOMA THESIS

Author:	Bc. Dominik Koutný
Study program:	N1701 Physics
Field of study:	General and Mathematical Physics
Form of study:	Full-time
Supervisor:	doc. Mgr. Jaroslav Řeháček, Ph.D.
Co-supervisor:	prof. RNDr. Zdeněk Hradil, CSc.

PŘÍRODOVĚDECKÁ FAKULTA
UNIVERZITY PALACKÉHO V OLOMOUCI

Katedra optiky

Pozitivita v kvantových protokolech pro charakterizaci optického signálu

DIPLOMOVÁ PRÁCE

Vypracoval:	Bc. Dominik Koutný
Studijní program:	N1701 Fyzika
Studijní obor:	Obecná fyzika a Matematická fyzika
Forma studia:	prezenční
Vedoucí diplomové práce:	doc. Mgr. Jaroslav Řeháček, Ph.D.
Konzultant diplomové práce:	prof. RNDr. Zdeněk Hradil, CSc.

Abstract

Concept of informational completeness of a given measurement setup was investigated from various points of view in past decades. Presented Diploma Thesis is aimed at the certification of performance of different informationally complete measurement schemes. We showed, that symmetric protocols for quantum state estimation, such as symmetric informationally complete measurement scheme and mutually unbiased bases, which are commonly regarded as the best measurement schemes, can be easily beaten with only slightly overcomplete random measurement schemes as square root measurement or random basis measurement. Protocols for tomography with informationally incomplete measurement setup of low–rank quantum states are also investigated. Such protocols together with employing the positivity constraints are compressed sensing protocols. We showed that with physically relevant measurement setup one can reconstruct low–rank quantum state with reasonable precision.

Key words

Gerchberg–Saxton algorithm, positivity constraints, compressed sensing, Fisher information, positive operator measure, quantum–state estimation, tomographic accuracy

Acknowledgements

I would like to thank my supervisors doc. Mgr. Jaroslav Řeháček, Ph. D. and prof. RNDr. Zdeněk Hradil, CSc. for their guidance, endless patience and advices. I am also grateful to the rest of the Department of Optics for stimulating enviroment. Last but not least, I would like to thank my dear family for support.

Declaration

I declare that I have written Diploma Thesis "Positivity constraints in quantum protocols of optical signal characterization" on my own under the guidance of doc. Mgr. Jaroslav Řeháček, Ph. D. and prof. RNDr. Zdeněk Hradil, CSc. by using theoretical resources, which are referred to in the list of literature. I agree with the further usage of this document according to the requirements of the Department of Optics.

In Olomouc on .....

.....

Dominik Koutný

Contents

1 Introduction

Characterization of unknown signal plays a key role in applications of signal processing, from detections of extrasolar planets that are outside the Solar system, to the improvement of medical instruments serving to find anomalies in the human body. Scientists in all branches of the modern science need to make a trustworthy and reliable decisions based on the recovery of a signal that carries information about parameters describing the interaction with the object of interest. Standard tool used for this purpose is a tomographic reconstruction, where we leave to interact a large ensemble of identically prepared probing signals with desired object. With the development of new technologies we also have to deal with characterization of very complex objects, where standard tomographic reconstruction can be inefficient compared to accumulated information about parameters that describe complex object and number of resources to obtain such an information. Complexity really takes place in describing objects in quantum world. As a number of quantum systems increases, number of free parameters increases exponentially. Therefore a complete characterization of such a complex quantum systems or processes is nearly impossible.

Understanding the measurement in quantum mechanics is necessary prerequisite for improving and efficient implementations of quantum protocols of optical signal characterization. Choosing the measurement setup greatly affects the ability of unique and accurate reconstruction of optical signal. Uniqueness of inferred quantum state leads to the concept of informationally complete measurement schemes. An experimentalist can choose from many different informationally complete measurement schemes, but the accuracy in reconstruction may differ. Evaluating the performance of informationally measurement schemes in the context of tomographic accuracies give us a valuable preliminary information. Accurate inference of quantum state from the discrete set of data, so called quantum–state estimation is desired. Recently, a function which allows us to compare a different quantum informationally complete measurements based on average tomographic performance was introduced [1], so called quantum tomographic transfer function, quantum version of optical transfer function [2], used to describe the performance of an optical system employing the details of signal propagation from every single component in given system. Quantum tomographic transfer function describes measurement setup in the same manner and allows us to judge whether a given informationally complete quantum measurement performs better in quantum–state estimation relative to other informationally complete measurements.

As dimension of quantum systems increases, building an informationally complete experimental measurement setup becames almost impossible. Reducing the measurement settings together with preserving tomographic accuracies for large quantum systems is a vital task. For signals described by very few parameters, accurate quantum tomography would not require informationally complete measurement schemes in general. But we can aim on a subspace that contains the most information about incoming signal and extract information with much fewer measurement settings.

Presented Diploma Thesis is aimed on both aspects in quantum state tomography; comparison of average performance of different informationally complete measurement schemes and accurate reconstruction of simple quantum states described by few free parameters living in the high dimensional Hilbert space. In section 3 we introduce a reliable and powerful numeric algorithm for comparison of average tomographic accuracies of informationally complete measurement schemes. In section 4 we compare quantum tomography of low–rank quantum states using standard linear inversion and more sophisticated reconstruction employing positivity constraints using informa-

tionally incomplete measurement setup.

2 Motivation and theoretical background

2.1 Quantum states and general concept of measurement in quantum mechanics

In classical physics, a state of a system is fully described by a point in the phase space. In contrast, state of the quantum system is a vector from the complex Hilbert space $\mathcal{H}$ [3]. Representation via complex vectors also give us complete information about given quantum state.
An important class of states in quantum mechanics are so–called pure states. These states are mathematically described as a normalized complex vectors $|\psi\rangle = \frac{1}{\sqrt{\langle\tilde{\psi}|\tilde{\psi}\rangle}}\left|\tilde{\psi}\right\rangle$ where Dirac bra–ket notation is used and $\langle\psi|\psi\rangle = 1$. In experiments, we do not have a complete information about preparation process of quantum state. Then we need to introduce a generalized way of describing systems in quantum mechanics, so–called density operator, a statistical ensemble of several quantum states.
Formal definition reads

$$\varrho = \sum_j p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|, \tag{2.1}$$

where p_j are probabilities of detection of states $|\psi_j\rangle$ and ϱ is a common symbol for density operator. An operator ϱ describes a density operator if and only if ϱ is positive semi–definite Hermitian operator with a unit trace. Positive semi–definiteness is defined as

$$\langle\psi| \varrho |\psi\rangle \geq 0, \tag{2.2}$$

for every $|\psi\rangle \neq 0$, important global property of quantum states. The Hermicity follows from positive semi–definiteness and means that

$$\varrho^\dagger = \varrho. \tag{2.3}$$

Finally the unit trace condition reads as

$$\mathrm{tr}\{\varrho\} = \sum_j p_j = 1. \tag{2.4}$$

Meanwhile description of general quantum state is almost trivial, on the other hand, general concept of measurement is not so straightforward and leads to the fundamental questions in foundation of quantum mechanics such as the collapse of the wave function.
In experiment, it does not matter what we measure, measurement outcomes are always discrete. We are always looking at bright spots or pixels on a shade and then we infer how the intensity function looks like. Measurement process is schematically depicted in fig. 1. For such a described measurement, quantum mechanics give us very efficient mathematical tool for description discrete measurement outcomes . Click of a jth detector or a jth pixel is represented by a positive semi–definite operator Π_j. The set of all outcomes $\{\Pi_j\}_{j=1}^n$, where n is a number of all outcomes, form a measure called in quantum theory Positive Operator Measure (POM). Quantum mechanics allows us to calculate probabilities p_j of individual outcomes via Born's rule

$$p_j \equiv \mathrm{tr}\{\varrho\Pi_j\}, \tag{2.5}$$

where ϱ is a density matrix representing input state. Elements of POM are Hermitean positive semi–definite operators forming a decomposition of an identity operator.

$$\Pi_j = \Pi_j^\dagger \Rightarrow p_j \equiv \mathrm{tr}\{\varrho\Pi_j\} \in \mathbb{R} \tag{2.6}$$

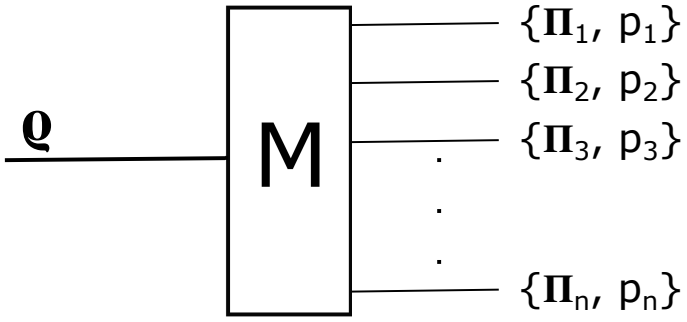

Figure 1: Measurement process known in quantum mechanics. Discrete measurement outcomes are described via set of positive operators $\{\Pi_j\}$. Quantum mechanics also provide us a rule how to count probabilities $\{p_j\}$ for a state ϱ to light up jth pixel. For more information see the text below.

$$\Pi_j \geq 0 \Rightarrow p_j \geq 0. \tag{2.7}$$

$$\sum_j \Pi_j = 1 \Rightarrow \sum_j p_j = 1. \tag{2.8}$$

Equations (2.6) to (2.8) form a mathematical definition of POM [4].
For a D–dimensional Hilbert space, the state ϱ is spanned by D^2 Hermitian, trace–orthogonal basis operators Ω_j, where one operator is a multiple of identity $1/\sqrt{D}$ and the rest D^2-1 operators are traceless

$$\begin{aligned} \mathrm{tr}\{\Omega_i\Omega_j\} &= 0 \quad \forall i \neq j, \\ \Omega_1 &= \frac{1}{\sqrt{D}}1, \\ \mathrm{tr}\{\Omega_j\} &= 0. \end{aligned} \tag{2.9}$$

If we now express the state ϱ and POM elements in our basis as follows

$$\begin{aligned} \varrho &= \frac{1}{D} + \sum_j t_j\Omega_j, \\ \Pi_k &= \sum_j C_{jk}\Omega_j, \end{aligned} \tag{2.10}$$

we can rewrite Born outcome probability rule to the set of linear equations

$$\mathbf{p}' = \boldsymbol{\mathcal{C}}\mathbf{t}, \tag{2.11}$$

where $\mathbf{t}$ is a column of D^2-1 coefficients $\mathrm{tr}\{\varrho\Omega_j\}$, $\mathbf{p}'$ is known vector of probabilities with components $p_j - \mathrm{tr}\{\Pi_j\}/D$, and the $M \times D^2-1$ matrix $\boldsymbol{\mathcal{C}}$ with entries

$$\boldsymbol{\mathcal{C}}_{jk} = \mathrm{tr}\{\Pi_j\Omega_k\} \tag{2.12}$$

is so–called measurement matrix. Matrix

$$\boldsymbol{\mathcal{C}} = \begin{pmatrix} \mathrm{tr}\{\Pi_1\Omega_1\} & \cdots & \mathrm{tr}\{\Pi_1\Omega_{D^2-1}\} \\ \vdots & \ddots & \vdots \\ \mathrm{tr}\{\Pi_M\Omega_1\} & \cdots & \mathrm{tr}\{\Pi_M\Omega_{D^2-1}\} \end{pmatrix}$$

provide full information about the apparatus. If $M \geq D^2$, we are talking about informationally complete measurement, that is, given POM uniquely characterize state ϱ; for every two density matrices $\varrho_1 \neq \varrho_2$ difference of vectors of given probabilities has to be nonzero vector, $\mathbf{p_1'} - \mathbf{p_2'} \neq \mathbf{0}$. A POM is minimally complete if it contains $M = D^2$ outcomes that are all linearly independent. Equation (2.11) can be solved using the Moore–Penrose pseudoinverse of $\boldsymbol{\mathcal{C}}$ such that $\boldsymbol{\mathcal{C}}^{-}\boldsymbol{\mathcal{C}} = 1$, solution therefore reads

$$\mathbf{t} = \boldsymbol{\mathcal{C}}^{-}\mathbf{p}'. \tag{2.13}$$

Is well-known that eq. (2.13) is the solution to the least–squares problem of minimization of the squared error $S = |\mathbf{p}' - \boldsymbol{\mathcal{C}}\mathbf{t}|^2$

2.2 Informationally complete measurement schemes

In quantum mechanics, we have many ways how to perform measurement on a quantum state. In this subsection, we aim on measurement schemes that are commonly used in experiments though all branches of quantum mechanics, where measurement takes place. One of the important property of given measurement setup, is its informational completeness; our measurement apparatus is able to distinguish between every two quantum states. Mathematically speaking,

$$\forall \varrho_1, \varrho_2, \varrho_1 \neq \varrho_2 \Rightarrow \mathbf{p_1} = \mathrm{tr}\{\Pi\varrho_1\} \neq \mathbf{p_2} = \mathrm{tr}\{\Pi\varrho_2\}, \tag{2.14}$$

where Π is a POM representing measurements outcomes.

2.2.1 Covariant measurement

Covariant measurement is known to be an optimal measurement in pure quantum–state tomography, where POM consist of rank–one operators distributed according to Haar measure [5]. Formally, the POM outcomes over dimension D are the continuous rank–one operators

$$\Pi_\psi = D\left|\psi\right\rangle\left\langle\psi\right|, \tag{2.15}$$

such that

$$\int \Pi_\psi \left(\mathrm{d}\psi\right) = D\int \left(\mathrm{d}\psi\right)\left|\psi\right\rangle\left\langle\psi\right| = 1 \tag{2.16}$$

with respect to the unitarily-invariant Haar measure $(\mathrm{d}\psi)$.

2.2.2 Mutually unbiased bases

Mutually unbiased bases (MUB) measurement scheme is used by many experimentalists in quantum information experiments with qubits. Lets have complex D–dimensional Hilbert space $\mathcal{H}^D$. We said, that two bases $\left|d_i\right\rangle, \left|e_i\right\rangle$ are mutually orthogonal, if vectors from a given basis are orthogonal and the overlap between vectors from different basis sets is reciprocal value of dimension D. We can rewrite this conditions into equations

$$\left|\left\langle d_i|d_j\right\rangle\right|^2 = 0, i \neq j, \tag{2.17}$$

identically for $\left|e_i\right\rangle$ and

$$\left|\left\langle d_i|e_j\right\rangle\right|^2 = \frac{1}{D}, \tag{2.18}$$

eq. (2.18) must hold independently of indexes i, j. Tricky part is how to construct MUB for a given dimension D. It has been shown, that we can construct MUB on Hilbert spaces, where its

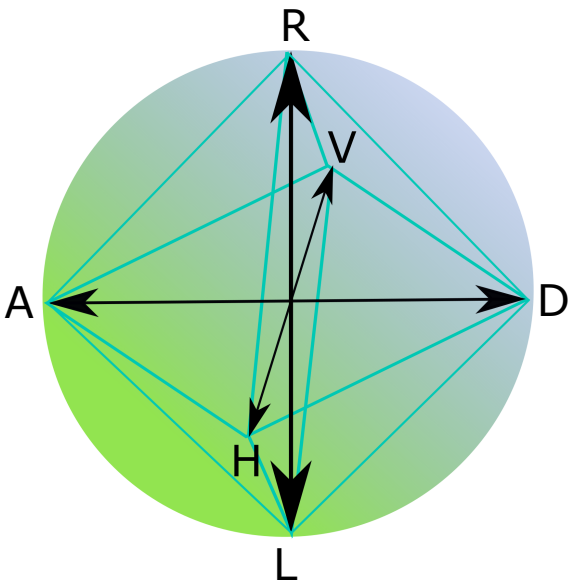

Figure 2: Schematically depicted MUB measurement outcomes in two dimensional complex Hilbert space $\mathcal{H}^2$. MUB measurement has six measurement outcomes that correspond to vertices of an octahedron and can be related to the projection onto polarization basis vectors; $|H\rangle$ horizontal polarization, $|V\rangle$ vertical polarization, $|D\rangle$ diagonal polarization, $|A\rangle$ anti–diagonal polarization, $|R\rangle$ and $|L\rangle$ for right–handed and left–handed circularly polarized light.

dimension is a power of a prime number. In a special and well–known case of dimension equal to 2, we can represent complex Hilbert space $\mathcal{H}^2$ with a unit sphere, so called Bloch sphere. Vectors living in the border of Bloch sphere are called qubits. MUB outcomes are projectors onto polarization basis vectors, schematically depicted in Fig. 2. For a dimension equal of power on any prime number, we can construct MUB as follows [6]. For example, existence of MUB is still not known for $D = 6$. We define unitary operators $\hat{X}$ and $\hat{Z}$ as follows

$$\begin{aligned} \hat{X} &= \sum_{k=0}^{D-1} |k\rangle \langle k+1| , \\ \hat{Z} &= \sum_{k=0}^{D-1} \omega^k |k\rangle \langle k| , \end{aligned} \tag{2.19}$$

where $\omega = e^{i\frac{2\pi}{D}}$ is a appropriate phase and $\{|k\rangle\}_0^{D-1}$ form a standard basis. Then eigenvectors of the following $D+1$ operators

$$\hat{X}, \hat{Z}, \hat{X}\hat{Z}, \hat{X}\hat{Z}^2, \hat{X}\hat{Z}^3, \cdots, \hat{X}\hat{Z}^{D-1} \tag{2.20}$$

are mutually unbiased.

MUB measurement found applications in quantum key distributions protocols or quantum error correction [7], since the measurement outcomes are unbiased if we perform measurement in a basis unbiased to the basis in which quantum state was prepared.

2.2.3 Symmetric informationally complete measurement

Another example of informationally complete measurement is a so called symmetric informationally complete (SIC) POM consisting of D^2 linearly independent rank–one outcomes Π_j, such that

$$\begin{aligned} \mathrm{tr}\{\Pi_j\} &= \frac{1}{D}, \\ \mathrm{tr}\{\Pi_i \Pi_j\} &= \frac{D\delta_{ij}+1}{D+1}, \end{aligned} \tag{2.21}$$

where $\delta_{ij} = 1$ for $i = j$ and 0 elsewhere. Construction of SIC POM in arbitrary dimension is still an open question, numerical solutions have been found for all integers up to $d = 151$ [8]. Despite this fact, generalized SIC POM, where POM elements are not necessarily rank–one operators, can be explicitly constructed in arbitrary dimension d [9].

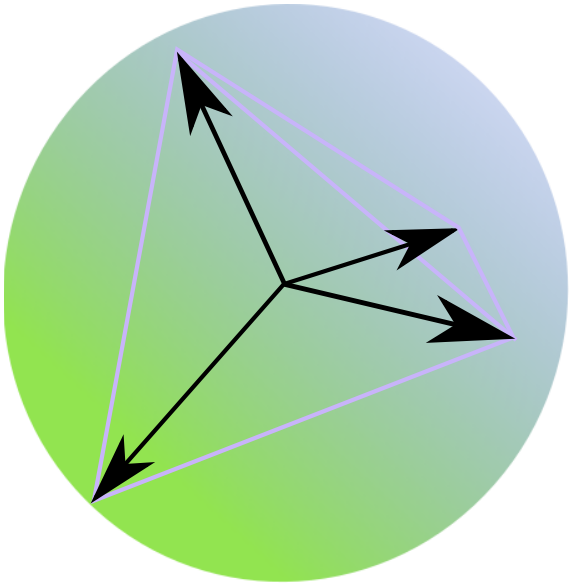

Figure 3: Schematically depicted SIC measurement outcomes in two dimensional complex Hilbert space $\mathcal{H}^2$. SIC POM has six measurement outcomes that correspond to vertices of an tetrahedron.

2.2.4 Square root measurement

Another informationally complete measurement mentioned here is so–called square root measurement (SRM). This kind of measurement is based on generating complex auxiliary kets $|a_j\rangle$, with their column entries i.i.d according to the standard Gaussian distribution. This set of pure states are uniformly distributed with respect to Haar measure [10]. Using the auxiliary kets $|a_j\rangle$, we are able to construct a random POM consisting of M random kets defined by M rank-one auxiliary $|a_j\rangle$s,

$$\Pi_j = S^{-1/2} \frac{|a_j\rangle \langle a_j|}{\langle a_j|a_j\rangle} S^{-1/2} \tag{2.22}$$

with

$$S = \sum_{j=1}^{M} \frac{|a_j\rangle \langle a_j|}{\langle a_j|a_j\rangle}\,, \tag{2.23}$$

automatically fulfilling the condition

$$\sum_{j=1}^{M} \Pi_j = 1 \tag{2.24}$$

SRM has been investigated in the study of state discrimination and the theory of quantum detection [11].

2.2.5 Randon measurement bases

The last kind of random POMs mentioned here are those comprising overcomplete random measurement bases, where each bases is defined by the unitary operator

$$U_{\mathrm{Haar}} \mathrel{\widehat{=}} \boldsymbol{U}_{\mathrm{Haar}}, \tag{2.25}$$

whose columns in matrix representation are again uniformly distributed according to Haar measure. Of course, any MUB is then zero–measure special case of minimally complete set of random bases generated this way. Random bases found applications in momentarily static experimental configurations, that is, wave–plane settings, local–oscillator amplitude and phase *etc.*
Generation of randomly distributed matrices according to Haar measure is very interesting itself [12, 13, 14]. First, one generate N complex matrices $\boldsymbol{A}$ whose entries are i.i.d. standard Gaussian random variables (RVs). Then the QR decomposition performed for each $\boldsymbol{A}$ to obtain N pairs of matrices $(\boldsymbol{Q}, \boldsymbol{R})$, where $\boldsymbol{Q}$ is a unitary matrix and $\boldsymbol{R}$ is an upper triangular matrix. The N kets that form the set of Haar-distributed pure states are therefore defined by the action of N unitary matrices

$$\boldsymbol{U}_{\mathrm{Haar}} = \boldsymbol{Q}\,\mathbf{diag}\left(\boldsymbol{R} \oslash |\boldsymbol{R}|\right) \tag{2.26}$$

on some reference ket, where $\oslash$ denotes the matrix Hadamard (entry-wise) division and $|\cdot|$ here denotes the entry-wise matrix absolute value.

2.3 Measurement as a statistics of independent outcomes and Fisher information

Certification of performance of a different informationally complete measurements for quantum state tomography is based on a statistical theory of the large number of independent detections and Fisher information, as will be discussed in section 3. As a typical situation, when detection of N copies of the quantum state ϱ happen independently, the resulting data statistics is multinomial with probabilities $p_j, 0 \leq j \leq M$. The probability mass function up to norm is given by

$$f(\{p_j\}; N) \propto \prod_k p_k^{n_k}, \tag{2.27}$$

where $\sum_k n_k = N$. Reciprocal Fisher information is known to be a Cramér–Rao lower bound on variance of an unbiased estimator and it is a way of measuring an amount of information that an observable random variable X carries about random parameter θ upon which the probability X depends. One can compute the Fisher information $F(\cdot)$ from

$$F(\theta) = \mathbb{E}\left[\left(\frac{\partial}{\partial\theta}\log\mathcal{L}(X,\theta)\right)^2 \middle| \theta\right], \tag{2.28}$$

where $\mathbb{E}$ stands for mean value; $\mathbb{E}(X) = \sum_i X_i p(X_i)$ and $\mathcal{L}(X, \theta)$ is a likelihood function. For a fixed sequence of data, the likelihood for multinomial statistics is given by

$$\mathcal{L}(\{n_j\}; \varrho) = \prod_k p_k^{n_k}. \tag{2.29}$$

In terms of the column $\mathbf{t}$ of coefficients t_j introduced via eqs. (2.10) and (2.11) for the state $\varrho = 1/D + \sum_j t_j \Omega_j$ we can evaluate term

$$\frac{\partial}{\partial \mathbf{t}} \log \mathcal{L}(\{n_j\}; \varrho) = \sum_k n_k \frac{\partial}{\partial \mathbf{t}} \log(p_k) = \sum_k \frac{n_k}{p_k} \frac{\partial p_k}{\partial \mathbf{t}}, \tag{2.30}$$

where

$$\begin{aligned} p_k &= \mathrm{tr}\{\varrho \Pi_k\} = \frac{\mathrm{tr}\{\Pi_j\}}{D} + \sum_j t_j \mathrm{tr}\{\Omega_j \Pi_k\} \\ \frac{\partial p_k}{\partial \mathbf{t}} &= \mathrm{tr}\{\ \Pi_k\}, \end{aligned}$$

Then the scaled Fisher information matrix for ϱ can be found to be

$$\begin{aligned} \boldsymbol{F}(\varrho) &= \frac{1}{N} \overline{\left(\sum_k \frac{n_k}{p_k} \frac{\partial p_k}{\partial \mathbf{t}} \right) \left(\sum_l \frac{n_l}{p_l} \frac{\partial p_l}{\partial \mathbf{t}} \right)} \\ &= \frac{1}{N} \sum_{k,l} \frac{\overline{n_k n_l}}{p_k p_l} \frac{\partial p_k}{\partial \mathbf{t}} \frac{\partial p_l}{\partial \mathbf{t}} \\ &= \frac{N^2 - N}{N} \underbrace{\sum_{k,l} \frac{\partial p_k}{\partial \mathbf{t}} \frac{\partial p_l}{\partial \mathbf{t}}}_{=0} + \sum_l \frac{1}{p_l} \frac{\partial p_l}{\partial \mathbf{t}} \frac{\partial p_l}{\partial \mathbf{t}} \\ &= \sum_l \frac{1}{p_l} \frac{\partial p_l}{\partial \mathbf{t}} \frac{\partial p_l}{\partial \mathbf{t}} \end{aligned} \tag{2.31}$$

we conclude that

$$\begin{aligned} \boldsymbol{F}(\varrho) &= \sum_l \mathrm{tr}\{\ \Pi_l\} \frac{1}{p_l} \mathrm{tr}\{\ \Pi_l\} \\ &= \boldsymbol{\mathcal{C}}^{\mathrm{T}} \boldsymbol{\mathcal{P}}^{-1} \boldsymbol{\mathcal{C}}, \end{aligned} \tag{2.32}$$

with $\boldsymbol{\mathcal{P}} = \mathrm{diag}(p_1, p_2, \ldots, p_M)$. Equation (2.32) is an important result. In further text, namely in section 3, we will deal with determining which quantum measurement performs better for state estimation and our argumentation is based on eq. (2.32), respectively trace of the inverse of the scaled Fisher information, an appropriate quantity to consider for tomographic–accuracy estimation.

2.4 Quantum Tomographic Transfer Function

For successful quantum state tomography, before carrying out any quantum protocol, we have to perform at least preliminary resource optimization, for example, minimization of reconstruction errors. For a given quantum measurement, we can rely on state estimation scheme which provides us the most accurate estimators. One can use standard estimation schemes such as maximum–likelihood schemes [15, 16] and the Bayesian–mean scheme [17, 18]. For strategies to improving

tomographic accuracies of state estimators for ill–calibrated and noisy measurements we can refer to [19, 20, 21, 22, 23, 24].
On the other hand, the choice of suitable measurement apparatus is also an important task. Usually we insist that the quantum state have to be uniquely characterized with given quantum measurement, that is, given quantum measurement have to be informationally complete, described in section 2.2. For such a quantum measurements the errors differ for a given estimation scheme. Recently, quantum tomographic transfer function (qTTF) [1] , that allows us to classify all quantum measurements schemes according to the average performance in quantum–state estimation was investigated. This function contains all information about given measurement and its output is average accuracy of reconstructed unbiased estimator over pure states together with employing the condition that measurement is informationally complete. Average over pure states is not a strict condition, since useful quantum–information protocols requires states designed close to pure states to work adequately. To sum up, qTTF is a good approximation to the average performance of realistic measurement setup. Also there are different techniques to evaluate the tomographic performance of quantum measurement based on linear–algebraic stability of corresponding measurement matrices that fully characterize given measurement. It have been shown that this way of characterizing tomographic accuracy led to contradictory predictions to well–known results.
The exact evaluation of the qTTF is very complicated. In [1] we can find approximations in terms of series expansion of the qTTF. In section 3 we will introduce a reliable numerical scheme to evaluate the qTTF almost exactly up to certain specified significance level. Our scheme is based on Monte Carlo averaging over pure states and a statistical concentration inequality that applies to bounded random matrices in the quantum state space. It turns out that commonly regarded optimal measurements such as SIC measurements and MUB measurements can be easily beaten with randomly generated SRM which are slightly more overcomplete then supposedly optimal SIC and MUB measurements. We also illustrate the well–known convergence to optimal pure–state tomography by evaluation the qTTF for measurements with various number of outcomes.

2.5 Gerchberg–Saxton algorithm

Even though informationally complete measurement schemes are desired in general, on the other hand, for simple systems, accurate reconstruction can be achieved with much fewer measurement settings. In classical optics, the Gerchberg–Saxton (GS) algorithm [2] is a well–known and a common tool used for wavefront reconstruction. GS algorithm is a very simple algorithm, based on scanning intensities and propagating of light in free space. To be more precise, GS algorithm works with two intensity scans, one taken close to the beam source and in a far field, in spectrum. Such a measurement setup is informationally incomplete. Information obtained from two intensity scans never characterize general input field with desired accuracy. But in the case of reconstruction of wavefront of a simple coherent field, GS algorithm works well. GS algorithm is sketched in fig. 4.

GS algorithm is a standard tool for experimentalists in classical optics because of the reasonable precision of the reconstructed wavefront together with reasonable measurement setup. Even with measurement that is informationally incomplete, accurate estimation of simple signal can be achieved.
In a section 4 we would like to convince you that in the middle of great success of GS algorithm lies an automatically fulfilled positivity constraints. As a brief outline, quantum mechanical analog

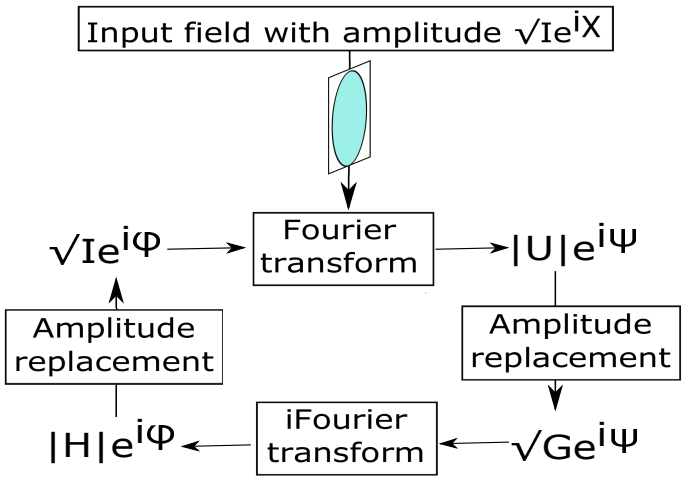

Figure 4: Schematically depicted Gerchberg–Saxton algorithm. First, an intensity scan I of incoming wave is taken. Together with our initial phase guess x we let the beam to propagate. Mathematically one take a Fourier transform of $\sqrt{I}e^{ix}$, which gives us a new wavefront in spectrum $|U|e^{i\psi}$. An important step, we replace the amplitude $|U|$ with an exactly known amplitude $\sqrt{G}$ where G is given as Fourier transform of our intensity scan I. After inverse Fourier transform and amplitude replacement we end up with a phase ϕ, our first estimation of true phase of incoming wave. One can iterate this procedure and reconstruct a desired wavefront with reasonable precision.

of a wavefront is a pure state, complex vector in state space. Density matrix corresponding to a given pure state is always positive operator, since outer product of complex vector with itself is from the definition positive matrix. We further generalize our scheme to reconstruction of density matrices of rank greater than one, i.e. partially coherent fields, where positivity constraints is not fulfilled automatically and we have to adopt it.
These thoughts which are also based on work of [25, 26, 27] led us to clarify the role of positivity constraints in compress sensing, reconstruction of very simple incoming signal using physically relevant measurement setup.

2.6 Compressed sensing

Determining an unknown signal from a set of measurements is a core problem in physics and engineering. This task is definitely not easy as the number of free parameters defining the signal increases and signal becomes complex. A breakthrough in signal processing was the Nyquist–Shannon sampling theorem, derived in 1928. It states that if the signals highest frequency is less than half of the sampling rate, then the signal can be reconstructed perfectly. Around 2006 it was proven that signals, that are sparse in some basis, can be reconstructed with much fewer samplings than it is stated in the famous Nyquist–Shannon sampling theorem [26, 27]. Sparsity of a coherent signal represented by a column vector $\mathbf{v}$ is understood such that vector $\mathbf{v}$ has only few nonzero elements in some domain. The function that can tell us how sparse given vector is is the L_0 norm, defined as a sum of zeroth powers of elements of given vector $||\mathbf{v}||_{L_0} = \sum_i v_i^0$, what is clearly equal to the number of nonzero elements. In compressed sensing protocols, we are dealing with undetermined systems. Matrix $\boldsymbol{\mathcal{C}}$ defined in eq. (2.12) representing our measurement setup

is informationally incomplete. Solution of the undetermined system of linear equations $\mathbf{p}' = \boldsymbol{\mathcal{C}}\mathbf{x}$ where $\boldsymbol{\mathcal{C}}$ is rectangle matrix and $\mathbf{p}'$ is a vector of measured frequencies, is known to be a solution to the least square problem $|\mathbf{p}' - \boldsymbol{\mathcal{C}}\mathbf{x}|^2$, where we minimize L_2 norm, that is, amount of energy in the system. Since L_2 do not tell us something about sparsity we need to enforce it. One can minimize the number of nonzero components of the solution. The function counting the number of non-zero components of a vector is desired L_0 norm. On the other hand, L_0 norm is not a convex norm, therefore finding global minimum is very hard and requires nontrivial nonlinear techniques in non–convex optimization problems. Luckily enough, it was proved [26] that L_1 norm, sum of absolute values of vector elements, has very similar properties and is usable for optimization protocols in compressed sensing.

Generalization of compressed sensing protocols via L_1 norm minimization from coherent signals described by vectors to application in reconstruction of density matrices with rank greater than one, quantum–mechanical analog of partially coherent fields, can be performed through induced L_1 norm acting on matrices. Such an induced norm works with singular values, easily accessible from singular value decomposition of any rectangular matrix $\boldsymbol{\mathcal{A}}_{m\times n} = \boldsymbol{\mathcal{U}}_{m\times m}\boldsymbol{\mathcal{S}}_{m\times n}\boldsymbol{\mathcal{V}}^{\mathrm{T}}_{n\times n}$, where $\boldsymbol{\mathcal{U}}$ and $\boldsymbol{\mathcal{V}}$ are unitary matrices and $\boldsymbol{\mathcal{S}}$ is a diagonal matrix with real non–negative entries known as singular values of $\boldsymbol{\mathcal{A}}$. Applications of compressed sensing protocols for quantum state tomography can bring advantages in the form of reducing the number of measurement outcomes without sacrificing information. Employing quantum mechanics with continuous variables, where the state of the system living in Hilbert space of infinite dimension is in general described by infinite number of free parameters. With preliminary knowledge about purity of our state, where quantum state is close to the border of pure quantum states given by saturated uncertainty relations

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}, \tag{2.33}$$

for almost complete description of such a set of states we need only few parameters, first and second moments in position and momentum, satisfying canonical commutation relation $[x, p] = i\hbar$. Class of quantum states saturating inequality in eq. (2.33) are gaussian states.

It has been shown [25] that positivity constraint $\varrho \geq 0$ plays an important role in compressed sensing protocols for estimation of low–rank quantum states. Positivity constraints leads to unique and robust reconstruction of an unknown quantum state.

3 Fast universal certification of measurement schemes for quantum tomography

Fisher information matrix $\boldsymbol{F}(\rho) = \boldsymbol{\mathcal{C}}^{\mathrm{T}}\boldsymbol{\mathcal{P}}^{-1}\boldsymbol{\mathcal{C}}$ derived in section 2.3 in eq. (2.32), where measurement matrix $\boldsymbol{\mathcal{C}}$ is defined via eq. (2.12) is intimately related to the accuracy of quantum tomography. If the quantum source is described by a full–rank density matrix ϱ then all statistically consistent state estimators $\tilde{\varrho}$ became unbiased in the limit of many independent measurement detections N [28]. In this limit, the scaled mean squared-error (MSE) $N\,\mathbb{E}\big[\mathrm{tr}\big\{(\widehat{\varrho}-\varrho)^2\big\}\big]$ approaches the Cramér-Rao bound

$$f(\varrho) = \mathrm{Sp}\big\{\boldsymbol{F}(\varrho)^{-1}\big\} \tag{3.1}$$

under the matrix trace $\mathrm{Sp}\{\cdot\}$. The Fisher matrix has one very important physical invariance property, $\boldsymbol{F}(\varrho)$ it is invariant under channel duplication. Duplicating the POM outcome channels will not give us any more additional information. The qTTF is defined as the average

$$\mathrm{qTTF}(\{\Pi_j\}) = \mathbb{E}_{|\psi\rangle\langle\psi|}[f(|\psi\rangle\langle\psi|)] \tag{3.2}$$

of the Cramér-Rao bound over all pure states $|\psi\rangle\langle\psi|$ distributed with the Haar measure that is uniform and unitarily invariant [29]. As we describe in section 2.4, this function serves as a performance certifier for a given POM $\{\Pi_j\}$. The smaller value of qTTF implies smaller average reconstruction error. For minimally complete measurements, where number of outcomes M is D^2 and minimal bases measurements, where $M = D(D+1)$, analytical expressions for qTTF has been computed [1], together with expressions for POMs possessing certain kinds of symmetry. For SIC POMs, described in section 2.2.3 it is

$$\mathrm{qTTF}(\{\Pi_j\}_{\mathrm{SIC}}) = D^2 + D - 2. \tag{3.3}$$

For a MUB measurement described in section 2.2.2, we have

$$\mathrm{qTTF}(\{\Pi_j\}_{\mathrm{MUB}}) = D^2 - 1. \tag{3.4}$$

For the covariant measurement described in section 2.2.1, the qTTF is given by

$$\mathrm{qTTF}(\{\Pi_j\}_{\mathrm{COV}}) = 2(D-1), \tag{3.5}$$

which defines the limit for pure-state tomography.
In what follows, we propose a numerical scheme that evaluates the qTTF almost exactly up to a pre–chosen significance level.

3.1 Numerical scheme for evaluating the qTTF

3.1.1 Properties of qTTF estimator

With the help of eq. (3.2) we can define an estimator

$$\widehat{\mathrm{qTTF}}(\{\Pi_j\}) = \frac{1}{L}\sum_{l=1}^{L} f(\varrho_l) \tag{3.6}$$

for the qTTF as the discrete average sum over L randomly generated pure states ϱ_l distributed randomly according to Haar measure. The qTTF estimator is both unbiased and consistent, reads

$$\mathbb{E}_{|\psi\rangle\langle\psi|}\Big[\widehat{\mathrm{qTTF}}(\{\Pi_j\})\Big] = \mathrm{qTTF}(\{\Pi_j\}) \tag{3.7}$$

and

$$\widehat{\mathrm{qTTF}}(\{\Pi_j\}) \longrightarrow \mathrm{qTTF}(\{\Pi_j\}) \tag{3.8}$$

in the limit of sufficiently large L.
Generation of pure states randomly distributed according to Haar measure is described in section 2.2.4 via generating complex auxiliary kets $|a_j\rangle$ with i.i.d entries according to standard Gaussian distribution.

3.1.2 A conservative concentration inequality–the Hoeffding inequality

To proceed further, we need to treat the convergence of estimator $\widehat{\mathrm{qTTF}}(\{\Pi_j\})$ to the actual value of $\mathrm{qTTF}(\{\Pi_j\})$. Of course, we know from the consistency eq. (3.8) that as L increases, the two quantities approach each other. But if we want to put things more rigorously, let us recall that $f(\varrho)$ is a bounded random variable in state space for any informationally complete tomography scheme since the MSE $\mathbb{E}\big[\mathrm{tr}\big\{(\widehat{\varrho}-\varrho)^2\big\}\big]$ is always finite for any ϱ. For such a random variable, there exists the following concentration inequality

$$\begin{aligned} &\mathrm{Prob}\left(\left|\widehat{\mathrm{qTTF}}(\{\Pi_j\}) - \mathrm{qTTF}(\{\Pi_j\})\right| \geq \delta\right) \\ &\leq \epsilon \equiv 2\exp\left(-\frac{2\,L\,\delta^2}{(f_{\max}-f_{\min})^2}\right), \end{aligned} \tag{3.9}$$

where δ quantifies the reliability of $\widehat{\mathrm{qTTF}}(\{\Pi_j\})$ relative to $\mathrm{qTTF}(\{\Pi_j\})$ for a given L, which is characterized by the optimum values $f_{\max} = \max\limits_{|\psi\rangle\langle\psi|}\Big\{f(|\psi\rangle\langle\psi|)\Big\}$ and $f_{\min} = \min\limits_{|\psi\rangle\langle\psi|}\Big\{f(|\psi\rangle\langle\psi|)\Big\}$. This inequality was first established by Hoeffding [30].
Right–hand side of eq. (3.9) (ϵ) is a measure of the significance level in using numerical estimator $\widehat{\mathrm{qTTF}}(\{\Pi_j\})$ as a performance certifier in place of $\mathrm{qTTF}(\{\Pi_j\})$ because of the difficulties with analytical evaluation of qTTF. Equation (3.9) gives us a general recipe for determining the critical value of L (L_{crit}) beyond which the probability that $\left|\widehat{\mathrm{qTTF}}(\{\Pi_j\}) - \mathrm{qTTF}(\{\Pi_j\})\right|$ is larger than a certain specified difference δ is assured to be less than the significance level ϵ. In further work, we set $\epsilon = 0.05$. Critical value of L that ensure that the difference between qTTF estimator and true value of the qTTF will not fluctuate beyond significance level ϵ can be obtained from the formula [31]

$$L_{\mathrm{crit}} = \left\lceil \log\left(\frac{2}{\epsilon}\right)\frac{(f_{\max}-f_{\min})^2}{2\,\delta^2}\right\rceil. \tag{3.10}$$

For a POMs that posses a high symmetry such as SIC POMs and MUB, the Cramér–Rao bound $f(\varrho)$ with a fixed purity $\mathrm{tr}\big\{\rho^2\big\}$ is exactly the same. Thus we have that $f_{\max} - f_{\min}$ and therefore $L_{crit} = 0$. This result tells us that for such a highly specialized POMs, it is enough to evaluate $\left|\widehat{\mathrm{qTTF}}(\{\Pi_j\}) - \mathrm{qTTF}(\{\Pi_j\})\right|$ with just one quantum state of this purity, because $f(\rho) = f\big(\mathrm{tr}\big\{\rho^2\big\}\big)$ is unitarily invariant. As one can expect, for heavily overcomplete general POMs ($M \gg D^2$), the absolute value of the difference $f_{\max} - f_{\min}$ will be smaller then for near–minimaly–complete POMs with outcomes M close to D^2, therefore overcomplete POMs should give us a better precision in quantum–state tomography. Also the value of L_{crit} is expected to be smaller for highly overcomplete measurements than for measurements with number of outcomes only slightly over D^2. Due to the fact that small difference δ frequently leads to much greater value of L_{crit} than is necessary to have an accurate $\widehat{\mathrm{qTTF}}(\{\Pi_j\})$. This led us to a new definition

of δ, to be a relative difference–$\delta = \left|\widehat{\mathrm{qTTF}}(\{\Pi_j\}) - \mathrm{qTTF}(\{\Pi_j\})\right| / \mathrm{qTTF}(\{\Pi_j\})$. Because we do not know exact value of $\mathrm{qTTF}(\{\Pi_j\})$, we instead take advantage of the simple fact that

$$\begin{aligned} &\frac{\left|\widehat{\mathrm{qTTF}}(\{\Pi_j\}) - \mathrm{qTTF}(\{\Pi_j\})\right|}{\mathrm{qTTF}(\{\Pi_j\})} \\ &\leq \frac{\left|\widehat{\mathrm{qTTF}}(\{\Pi_j\}) - \mathrm{qTTF}(\{\Pi_j\})\right|}{f_{\min}}, \end{aligned} \tag{3.11}$$

and therefore new δ is defined as the right–hand side of the above inequality. We also have to redefine value L_{crit} to

$$L_{\mathrm{crit}} = \left\lceil \frac{1}{2\,\delta^2} \log\left(\frac{2}{\epsilon}\right) \left(\frac{f_{\max}}{f_{\min}} - 1\right)^2 \right\rceil. \tag{3.12}$$

These new more operational definition of δ is almost insensitive to D and M, especially for POMs with $f(\varrho)$s that are unitarily–invariant functions of ϱ. The pair $(\delta = 0.01, \epsilon = 0.05)$ gives us values of L_{crit} that are sufficiently conservative for accurate estimators in all simulations tested so far.
Numerical evaluation of $\widehat{\mathrm{qTTF}}(\{\Pi_j\})$ is not computationally expensive. What it requires is the inversion of a Hermitian matrix for every randomly–generated pure state, which is for reasonably–large dimensions efficient. On the other hand, finding optimal values $f_{\min}$ and $f_{\max}$ is in general a non–convex problem and we need help from more sophisticated nonlinear optimization routines. By experience, at least up to $D = 10$ and M of the order of $10^3 D^2$, global optimization is not time consuming problem. In the case of computationally expensive optimization, we can vary the ϵ or δ value sacrificing the precision of the computed optimum values. In this scenario conservativeness of eq. (3.9) and eq. (3.10) plays an even more important role in maintaining the reliability of the reported values.

3.2 Covariant measurement: optimal pure–state tomography

It can be shown that in the limit of large measurement outcomes M SRM described in section 2.2.4 approaches the covariant measurement. We notice that in this limit, the sum

$$\begin{aligned} S &= \sum_{j=1}^{M} \frac{|a_j\rangle\langle a_j|}{\langle a_j|a_j\rangle} = M \sum_{j=1}^{M} \frac{1}{M} \frac{|a_j\rangle\langle a_j|}{\langle a_j|a_j\rangle} \\ &\to M \int |\psi\rangle\langle\psi|\,(\mathrm{d}\psi) = \frac{M}{D} \end{aligned} \tag{3.13}$$

approaches a multiple of the identity, and the POM outcomes

$$\Pi_j = S^{-1/2} \frac{|a_j\rangle\langle a_j|}{\langle a_j|a_j\rangle} S^{-1/2} \to \frac{D}{M} |\psi\rangle\langle\psi| \tag{3.14}$$

also turn into the corresponding multiples of the continuous Haar-distributed elements over which all sums again become integrals with respect to the Haar measure.
Now we would like to demonstrate the convergence of pure state tomography by evaluating their qTTFs for increasing number of outcomes M with the numerical algorithm described in section 3.1. In Fig. 5 we plotted results obtained for qutrit, three–dimensional quantum system. We can see that the qTTF decreases with increasing M, which is clearly consistent with the fact that overcomplete measurements are more accurate in quantum–state reconstruction as compared with

measurements that are only nearly–minimally complete. We can also see that L_{crit} drops gradually on average with increasing M. In the the limit of covariant measurement, where M tends to infinity, $f_{\max}$ and $f_{\min}$ became almost the same and $L_{\rm crit}$ will therefore also tends to 0 as it should be for covariant POMs of all dimensions D. We set $(\delta = 0.01, \epsilon = 0.05)$ in all plots in the figure.

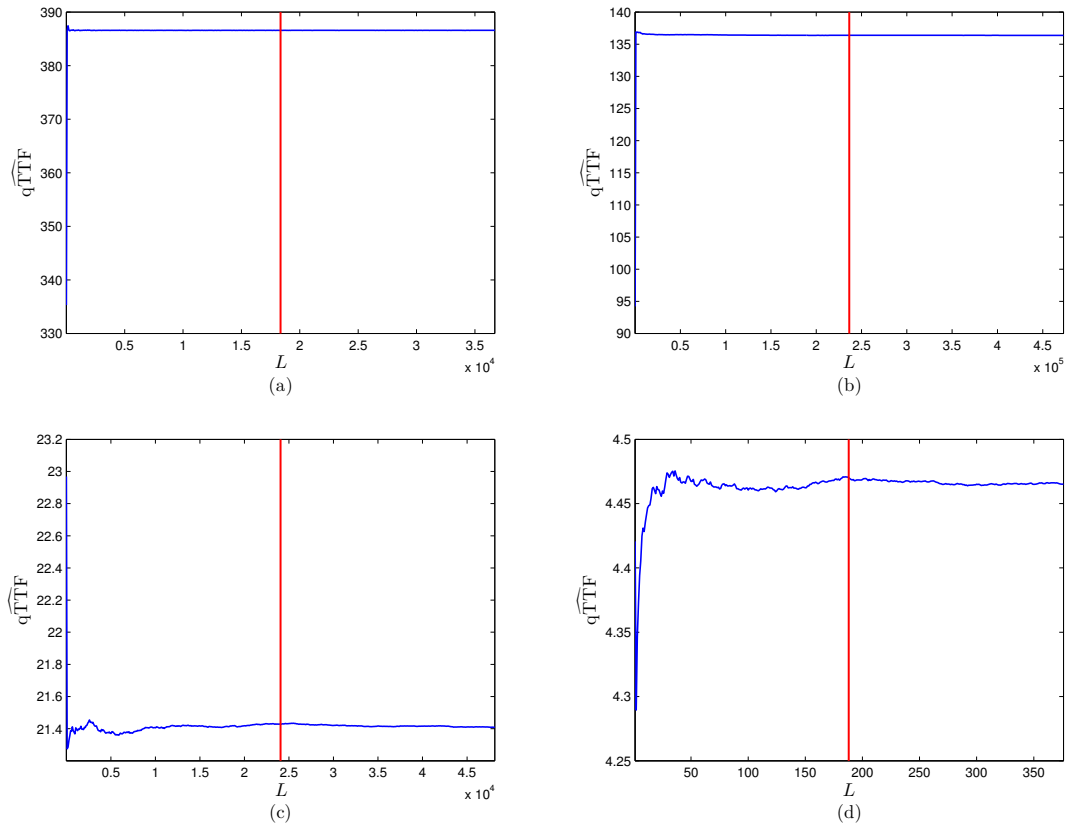

Figure 5: The convergence to optimal pure-state tomography for a qutrit ($D = 3$). We generated random POM with number of outcome M equals to[(a) $M = 9$, (b) 10, (c) 12 and (d) 10000, the graph shows the variation of $\widehat{\rm qTTF} \equiv \widehat{\rm qTTF}(\{\Pi_j\})$ with the number of randomly generated states L. The red vertical line represents $L_{\rm crit}$ computed with the parameters $(\delta = 0.01, \epsilon = 0.05)$. As we can see, $L_{\rm crit}$ is sufficiently large for a stable and reliable evaluation. In Fig. 1(a) we can immediately see the conservativeness of $L_{\rm crit}$. Its value is conservatively large that the fluctuation in $\widehat{\rm qTTF}$ can barely be seen. The convergence to a qTTF value of $2(3-1) = 4$ as follows from eq. (3.5) is clear from this figure.

3.3 Overcomplete random measurements

Now we show that popular symmetric POMs such as SIC POMs and MUB, which have enjoyed a longstanding reputation of being optimal measurements is some way, are actually suboptimal. A performance measure for quantum–state estimation strongly depends on the considered figure of merit when we are talking about tomographic accuracy of state estimation. A qTTF is related to the MSE which is a proper measure of distance of quantum states and optimal estimator to

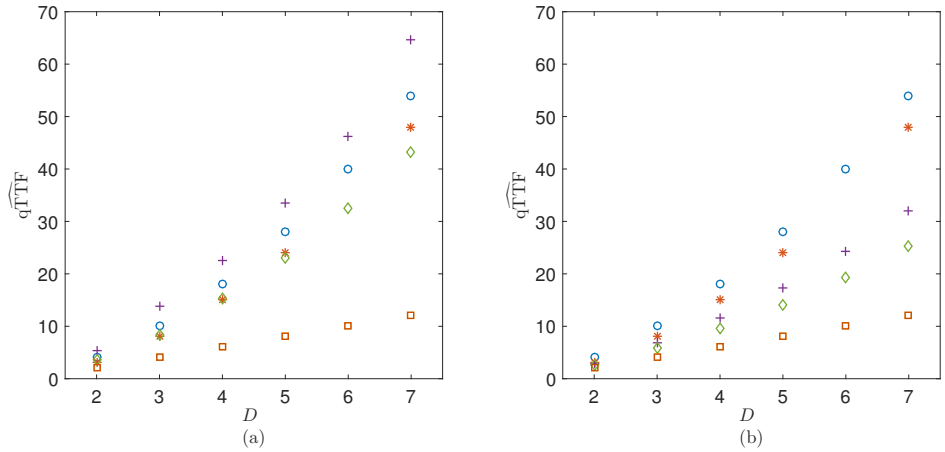

Figure 6: Comparison of the qTTF of random SRMs where we averaged over 50 POMs with SIC POMs ($\bigcirc$), MUB ($*$) and the covariant measurement ($\square$). Because the number of outcomes in random POMS are scaling of D^2, to facilitate the comparison, we define $M = KD^2$ for the random POMs, where $K \geq 1$ is a positive integer. In panel (a), the qTTFs for random SRMs of $K = 2$ ($+$) and $K = 3$ ($\Diamond$) are investigated, whereas in panel (b), the qTTFs for $K = 5$ ($+$) and $K = 10$ ($\Diamond$) are plotted. The values of L_{crit} pure states [see Eq. (3.10)] that are used to to average the qTTFs are obtained with $(\delta = 0.02, \epsilon = 0.05)$, which yield sufficiently smooth plots. Random SRMs of $K \geq 5$ give superior reconstruction over SIC POMs and MUB for any D. For $D \geq 5$, random SRMs of $K = 3$ is already better than these standard symmetric measurements, as highlighted in panel (a). The convergence of the SRMs to the covariant measurement for large K (M) is clear from figure.

be adopted for state reconstruction ϱ should be the one that minimizes the figure of merit of interest–MSE. Such an estimator that minimize MSE for overcomplete measurements was explicitly worked out for example in [28].

As a showcase of the versatility and efficiency of our numerical algorithm based on Monte–Carlo generation of random pure states to compute qTTFs, let us compare the well–known results of the qTTF for SIC POMs eq. (3.3) and MUB eq. (3.4) with overcomplete random POMs. The dependence of qTTF on the Hilbert–space dimension D is quadratic, whereas the qTTF of the covariant measurement is linear in D. This in general give us a free space where we can find POMs that give us better accuracy in quantum–state reconstruction. With the help of numerical simulations we really prove that one can be more sufficient in reconstruction of a given quantum state in average than using symmetric POMs. In practice, physical realization of sophisticated randomly–generated POM can be done with the help of spatial light modulators to carry out nontrivial light modulation [32, 33, 34].

As is mentioned in section 2.2.4 and section 2.2.5, there are two types of randomly generated POMs, namely SRM defined in eqs. (2.22) and (2.23) and overcomplete random measurement bases, where each basis is defined by the unitary operator $U_{\text{Haar}} \mathrel{\widehat{=}} \boldsymbol{U}_{\text{Haar}}$. Columns in matrix representation are uniformly distributed according to Haar measure. First, we consider the SRM in our numerical simulations. The SIC POMs with $M = D^2$ are clearly zero–measure special

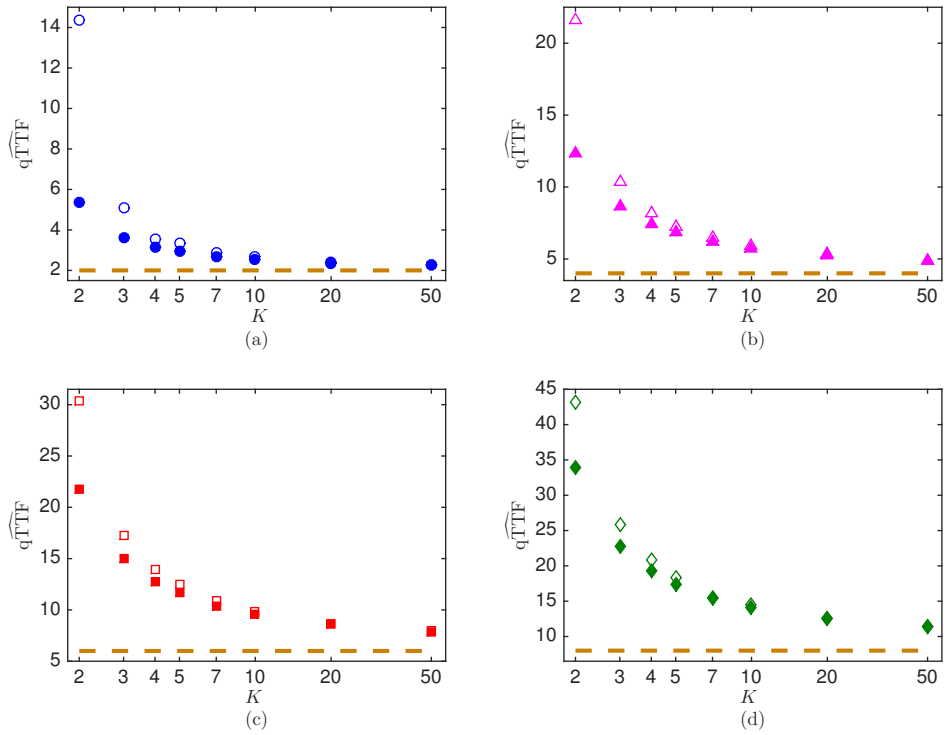

Figure 7: (Comparison of the qTTFs between random POM bases represented by empty markers and random SRMs represented by solid markers. As in Fig. 6, we take $M = KD^2$ with positive integers $K \geq 1$ and investigate the functional dependence of the qTTF on K in logarithmic scale. Graphs are plotted for various dimensions; (a) $D = 2$ ($\bigcirc, \bullet$), (b) $D = 3$ ($\triangle, \blacktriangle$), (c) $D = 4$ ($\square, \blacksquare$) and (d) $D = 5$ ($\Diamond, \blacklozenge$). As K increases, all markers approach the asymptotic optimal limit for pure-state tomography depicted by dashed line. For $K \gtrsim 7$ the difference in tomographic performance between SRMs and random bases become negligible.

cases of the SRM with $S = D$ being multiple of identity so its MUB with $M = D(D+1)$ are also zero–measure special cases of the SRM with $S = D+1$. The existence of random POMs that give lower reconstruction errors that SIC POMs and MUB is ensured by the fact that SRM approaches the covariant measurement and the fact that qTTF is a smooth function of the POM, D, M.

Our expectations that, for a given D, the average qTTF over sufficiently many randomly generated SRMs is subquadratic in D were confirmed with statistical rigor as we can see in Fig. 6 using numerical machinery developed in section 3.1. We defined $M = KD^2$ for positive integers K, numerical calculations show that SRMs of $K \geq 5$ is sufficient to overcome the reconstruction accuracies of SIC POMs and MUB for any D on average. For $D \geq 5$, random SRMs of $K = 3$ are enough to beat these symmetric measurements in tomographic performance. Random SRMs of $K = 4$ starts to outperform the MUB for $D \geq 3$.

Speaking differently, we can get in average better tomographic performance on average for more complex quantum degrees of freedom using a random SRM of three or four times as many out-

comes then SIC POMs. We can guarantee that accuracies is state–estimation will be better for any D if we increase number of outcomes $K = 5$.
The second class mentioned above of random POMs are overcomplete random bases. Once again, any MUB is then a zero–measure special case of a minimally complete set of random measurement bases generated this way. Analytical expressions of the qTTF for such POM bases are unknown, just as those for the SRMs. Due to the fact that outcomes of a random SRM are mutually nonorthonormal compared to those in a normalized basis form a set of mutually orthogonal complex vectors, we can expect that the convergence to covariant measurement is faster for random SRMs relative to random POM basis. This observation and the numerical simulations shown in Fig. 7 led us to conjecture that for a given D and M protortional to D corresponding to overcomplete measurement, the average qTTF for random SRMs defined via eq. (2.22) and eq. (2.23) is lower that the average aTTF for random POM bases defined by $U_{\text{Haar}} \widehat{=} \boldsymbol{U}_{\text{Haar}}$
This conjecture is indeed supported with the help of our numerical scheme developed in section 3.1 by numerical analysis showed in Fig. 7, where we take once again $M = KD^2$. We can see that for small number of bases, small K, on average, employing SRMs for state reconstruction over random POM bases can ensure much higher accuracies in quantum–state reconstruction. For sufficiently large K, both classes of POMs become comparable in tomographic performance, as its expected.

4 Quantum Gerchberg–Saxton algorithm

In the previous section, we were investigating the performance of different informationally complete measurement schemes. Even though such schemes are desired in protocols of optical signal characterization, as number of free parameters describing quantum system increases, building informationally complete measurement setup is nearly impossible, on the other hand, density matrices with only few nonzero singular values can be reconstructed with high accuracy using informationally incomplete measurement. We already discussed in section 2.5 the significance of the classical Gerchberg–Saxton (GS) algorithm in classical optics. Using this simple procedure based on scanning intensities and free propagating of light represented by the Fourier transform one can obtain with reasonable precision reconstructed wave front. Indeed, this algorithm works well but on the other hand, wave front is a simple physical quantity. In many scenarios, our input state do not have to be such a simple state that we can not describe it only using one complex vector but we have to deal with partially coherent fields, classical analog of density operators, well–known concept in quantum mechanics described in eq. (2.1). In a classical GS algorithm, positivity constraints are not taken into consideration, which is good so far, because wave front is represented by rank one density operator, which is always a positive operator. Much work in past decade have been done [27, 26, 35, 36, 25] to understand the role of positivity constraints in quantum protocols of optical signal characterization. It turns out that positivity can help to reduce measurement outcomes so that we can perform measurement on a signal with less measurements setting required for informationally complete measurement and still gets very accurate estimate of a given signal, as we described in section 2.6.

Positivity constraints for low–rank quantum states leads to a robust precise estimation of a quantum state even though we use measurement which is not informationally complete [25]. Authors were aimed on random POM measurement such as square root measurement section 2.2.4 and random bases section 2.2.5. Together with positivity they showed that one can consider much less random measurement outcomes for reconstruction of physical state ϱ living in the Hilbert space with dimension D than number of outcomes required for minimally informationally complete measurement, that is, D^2. What we would like to bring new to this field of interests, is to probe the role of positivity constraints for a more relevant physical measurement known well in both classical and quantum optics – measurement in a basis of Laguerre–Gauss modes of light.

4.1 Laguerre–Gauss modes of light

It is well–known [37] that beam propagation along the z direction of a monochromatic scalar field of frequency ω, reads

$$E(\mathbf{r}, t) = \mathcal{E}(\mathbf{r}) exp\left[-i(\omega t - kz)\right], \tag{4.1}$$

where k is a wave vector related to the wave length λ is governed by the paraxial wave equation

$$\frac{\partial \mathcal{E}}{\partial z} = -\frac{\lambda}{4\pi}\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)\mathcal{E}. \tag{4.2}$$

Any optical beam can be therefore expressed as a superposition of a fundamental solutions of eq. (4.2). Especially, for a cylindrical symmetry, its useful to use the set of Laguerre–Gauss (LG)

modes, they read

$$\begin{aligned} LG_{mn}(r,\phi,z) =& \sqrt{\frac{2}{\pi m!n!}}\min(m,n)!(-1)^{\min(m,n)} \\ & \times (\sqrt{2}r)^{|m-n|} L^{|m-n|}_{\min(m,n)}(2r^2)\exp\left(r^2\right) \\ & \times \exp[i(m-n)\phi]\exp(i\psi(z))\,, \end{aligned} \tag{4.3}$$

where we set beam waist $w(z) = 1$ and $L_p^{|l|}$ are the generalized Laguerre polynomials. For further purposes we made a chance of variables; we define $l = m - n$ to be an azimuthal index that is responsible for topological charge giving the number of 2π–phase cycles around the mode circumference, can be both positive and negative and $p = \min(m, n)$ is a radial mode index. Phase $\psi(z)$ is so called Gouy's phase defined as

$$\psi(z) = (|l| + 2p + 1)\arctan(z). \tag{4.4}$$

In literature one can find that Gouy's phase is without physical meaning but Gouy's phase will play an crucial role in analysis of informational completeness of measurement made of projections into Laguerre–Gauss modes described above via eqs. (4.3) and (4.4).

4.2 Derivation of probability density function for Laguerre–Gauss modes

Laguerre–Gauss modes are widely used in experiments in classical singular optics and quantum optics. We can associate Laguerre–Gauss wave packet defined in eq. (4.3) with the wave function, well known concept in quantum mechanics [3], reads

$$\langle r,\phi,z|l,p\rangle = LG_{lp}(r,\phi,z). \tag{4.5}$$

In further work, we will omit the radial mode index p, because it will not bring any more information to our analysis, as we will see later. With this knowledge, our wave function will be described only by azimuthal index l and therefore wave function for our purposes will take form

$$\langle r,\phi,z|l,0\rangle = LG_{p=0,l}(r,\phi,z) \equiv LG_l(r,\phi,z). \tag{4.6}$$

Using Born rule eq. (2.5) we can obtain

$$\begin{aligned} p(r,\phi,z) =& \mathrm{tr}\{\Pi(r,\phi,z)\varrho\} \\ =& \sum_{l'} \langle l'|\,\Pi(r,\phi,z)\varrho\,|l'\rangle \\ =& \sum_{l'}\sum_{l''} \langle l'|\,\Pi(r,\phi,z)\,|l''\rangle\,\langle l''|\,\varrho\,|l'\rangle \\ =& \sum_{l'}\sum_{l''} \Pi(r,\phi,z)_{l',l''}\varrho_{l'',l'}, \end{aligned} \tag{4.7}$$

where we defined

$$\begin{aligned} \Pi(r,\phi,z)_{l',l''} &= \langle l'|\,\Pi(r,\phi,z)\,|l''\rangle \\ \varrho_{l',l''} &= \langle l'|\,\varrho\,|l''\rangle\,. \end{aligned} \tag{4.8}$$

Together with the identity

$$\Pi(r,\phi,z) = |r,\phi,z\rangle\,\langle r,\phi,z|\,, \tag{4.9}$$

we can express the POM element $\Pi(r,\phi,z)_{l'l''}$ from eq. (4.8) as

$$\begin{aligned}\Pi(r,\phi,z)_{l',l''} &= \langle l'|\,\Pi(r,\phi,z)\,|l''\rangle \\ &= \langle l'|r,\phi,z\rangle\,\langle r,\phi,z|l''\rangle \\ &= LG^{*}_{l'}(r,\phi,z)LG_{l''}(r,\phi,z),\end{aligned} \tag{4.10}$$

where * stands for the complex conjugate and

$$\langle r,\phi,z|l'\rangle \propto LG^{0}_{l'}(2r^2)r^{|l'|}e^{il'\phi}e^{i(|l'|-1)\arctan(z)}e^{-r^2}. \tag{4.11}$$

In textbooks on special function we can find that Laguerre polynomial with zero radial index is just 1. Putting eqs. (4.7), (4.10) and (4.11) together we obtain expression for probability density up to normalization

$$\begin{aligned}p(r,\phi,z) \propto &\sum_{l'l''} \varrho_{l'l''} r^{|l'|+|l''|} \\ &\times e^{i(l'-l'')\phi}e^{i(|l'|-|l''|)\arctan(z)}e^{-2r^2}.\end{aligned} \tag{4.12}$$

4.3 Analysis of probability density function

In eq. (4.12) is quantity what we measure with our experimental apparatus. From data $p(r,\phi,z)$ we have to infer input quantum state with the best accuracy with all the knowledge that we have about our measurement apparatus. The task now is how many matrix elements $\varrho_{l'l''}$ can our measurement consisting of just one intensity scan (z is a fixed value) distinguish. Since azimuthal index l can be both positive and negative, in our analysis we should distinguish these two cases.

4.3.1 Positive azimuthal index

Considering input state representing by a density matrix living in the Hilbert space with dimension D, azimuthal index l_p can therefore have values

$$l_p \in \{0,1,\cdots,D-1\}. \tag{4.13}$$

so upper limit in the sum in eq. (4.12) is $D-1$,reads

$$\begin{aligned}p(r,\phi,z) \propto &\sum_{l'l''}^{D-1} \varrho_{l'l''} r^{|l'|+|l''|} \\ &\times e^{i(l'-l'')\phi}e^{i(|l'|-|l''|)\arctan(z)}e^{-2r^2}.\end{aligned} \tag{4.14}$$

In general, we have to find out how many terms in a double–sum in eq. (4.12) we can distinguish. Using similar argumentation as in [38], we consider all matrix elements in eq. (4.12) to be nonzero, then $p(r,\phi,z)$ is made of superposition of all matrix elements. We need to figure out how many independent linear combination of density matrix we can generate varying r and ϕ and considering that distance from source on input state z is fixed. Since probability density is made of polynomial term $r^{|l'|+|l''|}$ and two phase terms $e^{i(l'-l'')\phi}$ and $e^{i(|l'|-|l''|)\arctan(z)}$, generation of independent linear superpositions will be provided with non–identical exponents in exponentials in eq. (4.14). We can omit the Gouy's phase for now since z is constant and therefore Gouy's phase will not

bring us any new piece of information to our analysis. Considering eq. (4.13) $|l'| = l'$ and setting polynomial exponential $l' + l'' = N$ and phase term $l' - l'' = M$, set of equations

$$\begin{aligned} l' + l'' &= N \\ l' - l'' &= M \end{aligned} \tag{4.15}$$

have unique solutions for all l' and $l'' \in \{0, 1, \cdots, D-1\}$. Equation (4.15) therefore generate $(D \times D)$ of independent pairs (N, M). This means, that we can distinguish D^2 elements. Talking differently, we can distinguish all matrix elements only after one intensity scan. Considering only positive azimuthal index then leads to informationally complete measurement just after taking one intensity scan.

$\|l'\| + \|l''\|$		$l' - l''$	$\|l'\| + \|l''\|$	
0	H_0H_0	0	0	•
1	H_0H_1	-1	-1	•
	H_0H_{-1}	1	-1	•
	H_1H_0	1	1	•
	$H_{-1}H_0$	-1	1	•
2	H_1H_1	0	0	•
	H_0H_2	-2	-2	•
	H_2H_0	2	2	•
	$H_{-1}H_{-1}$	0	0	∘
	H_0H_{-2}	2	-2	•
	$H_{-2}H_0$	-2	2	•
	$H_{-1}H_1$	-2	0	•
	H_1H_{-1}	2	0	•
3	H_1H_2	-1	-1	•
	H_2H_1	1	1	•
	$H_{-1}H_{-2}$	1	-1	•
	$H_{-1}H_2$	-3	-1	•
	$H_{-2}H_1$	-3	1	•
	$H_{-2}H_{-1}$	-1	1	•
	H_1H_{-2}	3	-1	•
	H_2H_{-1}	3	1	•
4	H_2H_2	0	0	∘
	H_2H_{-2}	4	0	•
	$H_{-2}H_{-2}$	0	0	•
	$H_{-2}H_2$	-4	0	•

Table 1: Special case for $D = 5$ and l defined via eq. (4.16). We set $|l'| + |l''| = N$ and showed how many pairs we can generate for a given N showed in first column. Third column is a final phase and last column is a Gouy's phase. We defined $H_n = r^{|n|}$. Fulfilled circles • are representing distinguishable matrix elements employing both phase factors described in eq. (4.17) and empty markers (∘) representing indistinguishable matrix elements.

4.3.2 General azimuthal index

Next step is considering that azimuthal index can be both negative or positive, since we have no restriction on the sign of azimuthal index from theory. Therefore

$$l_{np} \in \{-\frac{D-1}{2}, \cdots, 0, \cdots, \frac{D-1}{2}\}, \tag{4.16}$$

and probability density reads

$$\begin{aligned} p(r,\phi,z) \propto & \sum_{l',l''=-\frac{D-1}{2}}^{\frac{D-1}{2}} \varrho_{l'l''} r^{|l'|+|l''|} \\ & \times e^{i(l'-l'')\phi} e^{i(|l'|-|l''|)\arctan(z)} e^{-2r^2}. \end{aligned} \tag{4.17}$$

Argumentation is very similar as we introduced in section 4.3.1. But we can no more simplify our problem since $|l'|$ is no more equal to l'. Because first look can be confusing, let us consider a special situation, for $D = 5$ and $(l', l'') \in \{-2, -1, 0, 1, 2\}$. We have 5 different values of $N = |l'| + |l''|$, namely $0, 1, 2, 3, 4$. As we can see from table 1, all number of pairs is equal to $1+4+8+8+4 = 25$ as it should be. In second column of table 1 we can find a exponent in $e^{i(l'-l'')\phi}$. From all 25 pairs we can distinguish between $1 + 2 + 3 + 4 + 3 = 13$ pairs. Considering Gouy's phase, we can distinguish $1 + 4 + 7 + 8 + 3 = 23$ elements. Two elements remain indistinguishable with our measurement apparatus. To put things in more rigorous way, lets look on how many pairs one can generate for a given $N = |l'| + |l''|$. We get Then the total number of pairs for a fixed N is given

4 pairs	$\pm\|l'\|, \pm\|l''\|$	$l', l'' \neq 0$
2 pairs	$\pm\|l'\|, 0$	l'$\neq 0$
2 pairs	$0, \pm\|l''\|$	$l'' \neq 0$
1 pairs	0, 0	

by summing through l', l'' with the condition that if we choose l' then l'' can not be arbitrary, but have to fulfill the relation $|l'| + |l''| = N$. Mathematically, we end up with a double sum

$$\sum_{l'=\max(0,N-k)}^{\min(k,N)} \sum_{l''=0}^{k} (4 - 2\delta_{l'0} - 2\delta_{l''0} + \delta_{l'0}\delta_{l''0})\, \delta_{l'',N-l'}, \tag{4.18}$$

the term $\delta_{l'',N-l'}$ to ensure that sum of l' and l'' remains fixed and $k = \max(l')$. To evaluate this sum, we have to consider two scenarios. First, when $N \leq k$, then from eq. (4.18) we get

$$\begin{aligned} & \sum_{l'=0}^{N} \sum_{l''=0}^{k} (4 - 2\delta_{l'0} - 2\delta_{l''0} + \delta_{l'0}\delta_{l''0})\, \delta_{l'',N-l'} \\ & = \sum_{l'=0}^{N} (4 - 2\delta_{l'0} - \delta_{N-l'',0} + \delta_{l'0}\delta N - l', 0) \\ & = 4(N+1) - 2 - 2 + \delta_{N0} \\ & = 4N + \delta_{N0}, \end{aligned} \tag{4.19}$$

where we used the definition of Kronecker delta. The second scenario in when $N > k$, then

$$\begin{aligned}
&\sum_{l'=N-k}^{k}\sum_{l''=0}^{k}\left(4-2\delta_{l'0}-2\delta_{l''0}+\delta_{l'0}\delta_{l''0}\right)\delta_{l'',N-l'}\\
&=\sum_{l'=N-k}^{k}\left(4-2\delta_{l'0}-2\delta_{N-l',0}\right)\\
&=4(k-N+k+1)\\
&=4(2k-N+1).
\end{aligned}\tag{4.20}$$

The term $\delta_{l'0}$ in each sum in eq. (4.20) will be evaluated only once so it is equal to 1 so as δ_{N-k}. This result is indeed in conformity with first observation for special case, when $D = 5$ and thus $k = 2$. Using formulas derived in eqs. (4.19) and (4.20) we get sequence of number of pairs for given N same as we conclude before for special case, $\{1, 4, 8, 8, 4\}$.
Considering again similar equations as eq. (4.15)

$$\begin{aligned}
|l'|+|l''| &= N\\
l'-l'' &= M,
\end{aligned}\tag{4.21}$$

we want to find how many independent numbers M, N we can get. We can consider only cases when l' and l'' has the same sign, since case with different sign will use up only two cases, when $l' = 0$ or $l'' = 0$, as it follows from

$$l'-l''=l'+(-l'')=N.\tag{4.22}$$

We end up again with the sum

$$\sum_{l'=\max(0,N-k)}^{\min(k,N)}\sum_{l''=0}^{k}\delta_{l'',N-l'}.\tag{4.23}$$

Evaluation of this sum will again split into two cases, first, lets take $N \leq k$, thus

$$\begin{aligned}
&\sum_{l'=0}^{N}\sum_{l''=0}^{k}\delta_{l'',N-l'}\\
&=\sum_{l'=0}^{N}1\\
&=N+1.
\end{aligned}\tag{4.24}$$

In a second case we have $N > k$ and

$$\begin{aligned}
&2+\sum_{l'=N-k}^{k}\sum_{l''=0}^{k}\delta_{l'',N-l'}\\
&=2+\sum_{l'=N-k}^{k}1\\
&=2+k-N+k+1\\
&=2k-N+3.
\end{aligned}\tag{4.25}$$

This results are again in a conformity with special case when $D = 5$ and $k = 2$, we get the sequence of distinguishable pairs $\{1, 2, 3, 4, 3\}$. Maximum number of linearly independent pairs is then equal to $D + 1$. Considering Gouy's phase, with the help of numerical simulations, we found that there will be always $\frac{D-1}{2}$ indistinguishable matrix elements and we will reach the maximum for $\frac{D+1}{2}$ different values of distance z.

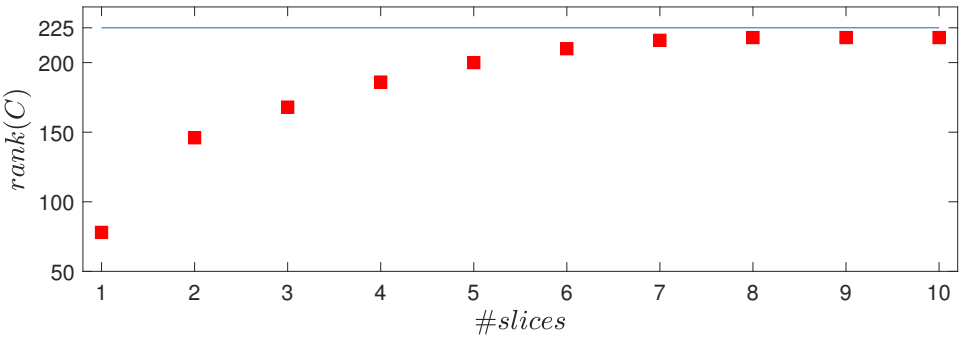

Figure 8: Dependence of the rank of measurement matrix $rank(C)$ on the number of intensity scans taken in experiment for a special case when density matrix describing input state lives on a Hiblert space with dimension 15. Numerics is in conformity with theoretical predictions, where we can see that upper bound on rank of C is indeed $D^2 - \frac{D-1}{2} = 218$ for a $D = 15$ and maximum is reached after taking $\frac{D+1}{2} = 8$ intensity scans.

In Fig. 8 we depicted the dependence of the rank of the measurement matrix C for $D = 15$ on the number of intensity scan taken. As we can see, with new intensity scan we get new piece of information but less then with previous intensity scan. Maximum affordable information is obtained for 8 intensity scans and we will end up with 7 indistinguishable matrix elements. To sup up, measurement performance in a basis of Laguerre–Gauss modes with both negative and positive azimuthal indexes will never be complete. It does not matter how many intensity scans we take, for a given dimension D there will be always $\frac{D-1}{2}$ indistinguishable matrix elements.

4.4 Numerical scheme and discussion

In this subsection, we would like to investigate how good our measurement is if we include positivity constraints to reconstruction or not. We opted to investigate the accuracy for quantum states action on a fifteen–dimensional Hilbert space. For reconstruction with a positivity constraints, we use a CVX package [39, 40] for Matlab, where positivity constraints can be easily included. Our goal is then constraint optimization, where the task is in the form

$$\begin{aligned} \min \sum_j \left[\mathrm{tr}\{\varrho \Pi_j\} - p_j\right]^2 \\ \varrho \geq 0 \\ \mathrm{tr}\{\varrho\} = 1, \end{aligned} \tag{4.26}$$

where ϱ is a quantum–mechanical state we want to reconstruct by minimizing mean–square error,

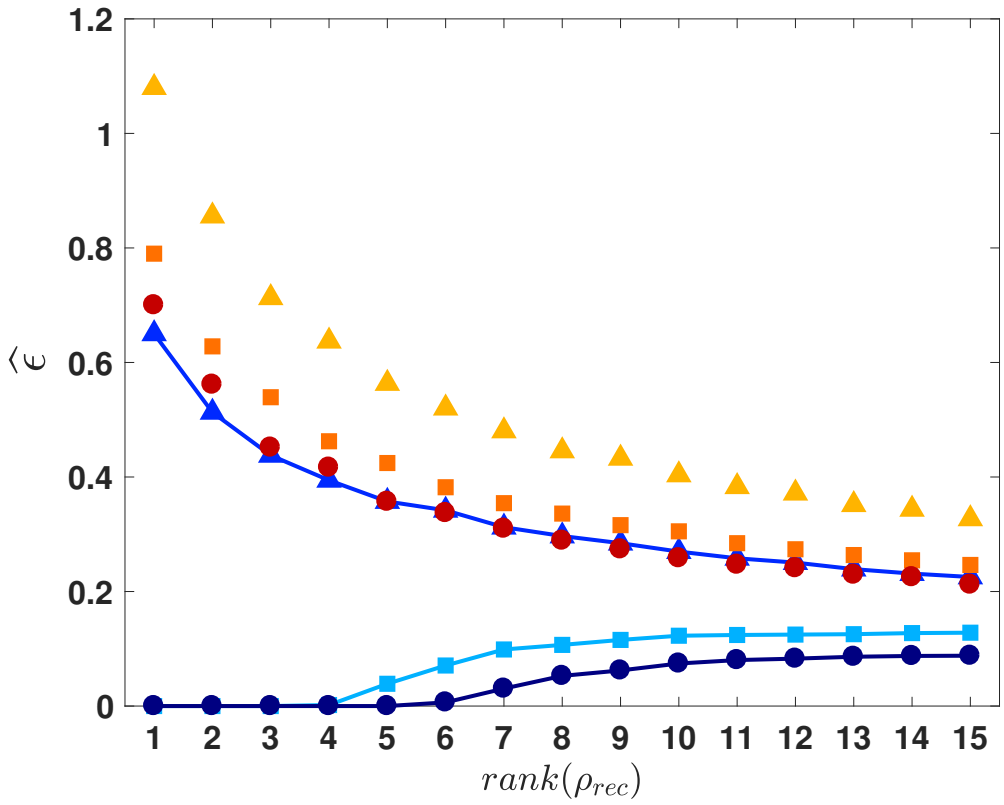

Figure 9: Numerical analysis how positivity constraints can affect quantum–state reconstruction for a dimension 15. On the horizontal axis we depicted a rank of quantum states using for averaging both constrained and unconstrained optimization. On the vertical axis we plotted the average of Hilbert–Schmidt norm ($\widehat{\epsilon} = \mathbb{E}\left[\mathrm{tr}\left\{(\varrho_{true} - \varrho_{est})^2\right\}\right]$), an appropriate measure of distance between any two quantum states. Markers not joined with a line stands for reconstruction via linear inversion of measurement matrix C and joined markers represents average accuracies after reconstruction win positivity constraints. Triangles (▲) stand for a reconstruction performed after one intensity scan, square markes (■) stand for a measurement made of two intensity scans and finally circles (●) stand for measurement made of three intensity scans. For more information see text.

Π_j is a POM element and vector $\mathbf{p}$ is a vector of output probabilities. In our numerical analysis, we perform 19×19 detections for each slices, thus POM is made of 19×19 outcomes distributed equidistantly on a vertical and horizontal lines across square in the centre of xy plane with edge length equal to 4 for each values of z. For reconstruction without positivity constraints we just solve the eq. (2.11) using Moore–Penrose pseudoinverse of the measurement matrix C. To be sure that our numerical scheme works well, we average across 200 randomly generated quantum states with respect to Haar measure with a given rank. Results are shown in Fig. 9. We plotted the mean squared–error $\mathbb{E}\left[\mathrm{tr}\left\{(\varrho_{true} - \varrho_{rec})^2\right\}\right]$ averaged over 200 quantum states with rank $r \in \{1, \cdots, 15\}$. As we can see from Fig. 9, without positivity constraints our reconstruction will never be precise.

On the other hand, employing the positivity constraints, for more than two intensity scan our reconstruction will be accurate till $r = 4$. The average accuracy is of course getting lower for as we increased r, but without positivity constraints, the positivity constraints plays less and less important role in reconstruction since the rank of measurement matrix C is getting higher.

5 Conclusion

An ability to distinguish between any accessible physical quantum states is a desired property of the measurement setup. Such a measurement scheme is informationally complete. An experimentalist can choose from many realizations of different informationally complete measurement schemes. But the average accuracy in quantum state reconstruction differ using different informationally complete measurement schemes. On the other hand, dealing with systems of large dimensions, number of free parameters to be estimated grows exponentially. Employing positivity constraints to the reconstruction process, one can still estimate low–rank quantum state with reasonable precision.

With respect to quantum–state reconstruction accuracy, we developed an efficient numerical Monte–Carlo scheme (Section 3) to evaluate a well–founded universal measurement certification quantity known from classical optics, the quantum tomographic transfer function, that works for any quantum measurement. Developed numerical scheme is based on statistical reasoning, enabling us to report the measurement tomographic quality and its reliability parameters accompanying this quality number. To demonstrate the power of this scheme, we used it to numerically verify the convergence of so–called square–root measurement to the covariant measurement (Section 3.2), ideal measurement for quantum state tomography in terms of accuracy. With proposed numerical scheme, we also studied the tomographic performances of random square–root measurement and random measurement bases relative to the popular symmetric measurement schemes such as symmetric informationally complete measurement and mutually unbiased bases. We showed that random measurements that are slightly more overcomplete than the symmetric ones give state estimators with lower reconstruction errors on average (section 3.3). In this section we also compared both interesting random schemes. In practise, random measurements may be implemented with the help of spatial light modulators.

In section 4 we dealt with how positivity constraints can affect accuracy of reconstruction of a given low–rank quantum state. Motivated with classical iterative algorithm for reconstruction of wave front, Gerchberg–Saxton algorithm described in section 2.5, which is very successful despite the fact that measurement when taking intensities closely behind the source and in a far field is informationally incomplete measurement. We further extend this idea on reconstruction of partially coherent fields, classical analog of density matrices with rank greater than one. In section 2.5 we showed that with two intensity scans and measurement provided via projections into basis of Laguerre–Gauss modes of light, frequently used in the field of singular optics, we can reconstruct a quantum state living in the Hilbert space with dimension 15 with high precision, till the rank of measurement does not exceed 4. This result is based on Monte–Carlo method of generating random quantum states with given rank. Counting with positivity constraints in reconstruction schemes indeed provides a powerful tool that can make reconstruction unique and accurate (as we can see in Fig. 9) even with informationally incomplete set of positive operator valued measure, whose elements describe measurement outcomes.

An overly critical reader may contest to this numerical finding in both sections by insisting that search over a finite range of dimension D is never rigorous enough for such a concrete assertions. We would like to mention that there is no physical basis for the quantum tomographic transfer function and so for mean–squared error to possess irregular kinks or discontinuities.

Results given in a section 3 are already published in impact physical journal Physical Review A [41]. Results obtained in section 4 are being prepared for publication. An experiment is

under preparation that will bring the opportunity to verify our results with polarization encoded quantum states.

References

[1] Řeháček, J., Teo, Y. S., and Hradil, Z. "Determining which quantum measurement performs better for state estimation". In: *Physical Review A* 92.1 (July 2015) (Cited on pages 1, 10, 13).

[2] Goodman, J. W. *Introduction to Fourier Optics*. W. H. Freeman, 2004 (Cited on pages 1, 10).

[3] Sakurai, J. J. *Advanced Quantum Mechanics*. Addison-Wesley Publishing Company, 1967 (Cited on pages 3, 21).

[4] Peres, A. *Quantum Theory: Concepts and Methods (Fundamental Theories of Physics)*. Springer, 1995 (Cited on page 4).

[5] Zhu, H. "Quantum state estimation with informationally overcomplete measurements". In: *Physical Review A* 90.1 (July 2014) (Cited on page 5).

[6] Bandyopadhyay, Boykin, Roychowdhury, and Vatan. "A New Proof for the Existence of Mutually Unbiased Bases". In: *Algorithmica* 34.4 (Nov. 2002), pp. 512–528 (Cited on page 6).

[7] Calderbank, A. R., Rains, E. M., Shor, P. W., and Sloane, N. J. A. "Quantum Error Correction and Orthogonal Geometry". In: *Physical Review Letters* 78.3 (Jan. 1997), pp. 405–408 (Cited on page 6).

[8] Fuchs, C. A., Hoang, M. C., and Stacey, B. C. *The SIC Question: History and State of Play*. 2017. eprint: `arXiv:1703.07901` (Cited on page 7).

[9] Gour, G. and Kalev, A. "Construction of all general symmetric informationally complete measurements". In: *Journal of Physics A: Mathematical and Theoretical* 47.33 (Aug. 2014), p. 335302 (Cited on page 7).

[10] Mezzadri, F. "How to generate random matrices from the classical compact groups". In: *Notices of the American Mathematical Society* 54.5 (May 2007), pp. 592–604 (Cited on page 7).

[11] Eldar, Y. and Forney, G. "On quantum detection and the square-root measurement". In: *IEEE Transactions on Information Theory* 47.3 (Mar. 2001), pp. 858–872 (Cited on page 8).

[12] Mezzadri, F. "How to generate random matrices from the classical compact groups". In: *Notices of the American Mathematical Society* 54.5 (May 2007), pp. 592–604 (Cited on page 8).

[13] Zyczkowski, K. and Sommers, H.-J. "Induced measures in the space of mixed quantum states". In: *Journal of Physics A: Mathematical and General* 34.35 (Aug. 2001), pp. 7111–7125 (Cited on page 8).

[14] Bengtsson, I. and Zyczkowski, K. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2008 (Cited on page 8).

[15] Řeháček, J., Hradil, Z., Knill, E., and Lvovsky, A. I. "Diluted maximum-likelihood algorithm for quantum tomography". In: *Physical Review A* 75.4 (Apr. 2007) (Cited on page 9).

[16] Paris, M. and Řeháček, J. *Quantum State Estimation (Lecture Notes in Physics)*. Springer, 2004 (Cited on page 9).

[17] Schack, R., Brun, T. A., and Caves, C. M. "Quantum Bayes rule". In: *Physical Review A* 64.1 (June 2001) (Cited on page 9).

[18] Blume-Kohout, R. and Hayden, P. *Accurate quantum state estimation via "Keeping the experimentalist honest"*. 2006. eprint: `arXiv:quant-ph/0603116` (Cited on page 9).

[19] Flammia, S. T., Gross, D., Liu, Y.-K., and Eisert, J. "Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators". In: *New Journal of Physics* 14.9 (Sept. 2012), p. 095022 (Cited on page 10).

[20] Baumgratz, T., Gross, D., Cramer, M., and Plenio, M. B. "Scalable Reconstruction of Density Matrices". In: *Physical Review Letters* 111.2 (July 2013) (Cited on page 10).

[21] Schwemmer, C., Tóth, G., Niggebaum, A., Moroder, T., Gross, D., Gühne, O., and Weinfurter, H. "Experimental Comparison of Efficient Tomography Schemes for a Six-Qubit State". In: *Physical Review Letters* 113.4 (July 2014) (Cited on page 10).

[22] Řeháček, J., Mogilevtsev, D., and Hradil, Z. "Operational Tomography: Fitting of Data Patterns". In: *Physical Review Letters* 105.1 (June 2010) (Cited on page 10).

[23] Mogilevtsev, D., Ignatenko, A., Maloshtan, A., Stoklasa, B., Rehacek, J., and Hradil, Z. "Data pattern tomography: reconstruction with an unknown apparatus". In: *New Journal of Physics* 15.2 (Feb. 2013), p. 025038 (Cited on page 10).

[24] Motka, L., Stoklasa, B., Rehacek, J., Hradil, Z., Karasek, V., Mogilevtsev, D., Harder, G., Silberhorn, C., and Sánchez-Soto, L. L. "Efficient algorithm for optimizing data-pattern tomography". In: *Physical Review A* 89.5 (May 2014) (Cited on page 10).

[25] Kalev, A., Kosut, R. L., and Deutsch, I. H. "Quantum tomography protocols with positivity are compressed sensing protocols". In: *npj Quantum Information* 1.1 (Dec. 2015) (Cited on pages 11, 12, 20).

[26] Candes, E., Romberg, J., and Tao, T. "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information". In: *IEEE Transactions on Information Theory* 52.2 (Feb. 2006), pp. 489–509 (Cited on pages 11, 12, 20).

[27] Donoho, D. "Compressed sensing". In: *IEEE Transactions on Information Theory* 52.4 (Apr. 2006), pp. 1289–1306 (Cited on pages 11, 20).

[28] Teo, Y. S. *Introduction to Quantum-State Estimation*. WSPC, 2015 (Cited on pages 13, 17).

[29] Jones, K. R. W. "Fundamental limits upon the measurement of state vectors". In: *Physical Review A* 50.5 (Nov. 1994), pp. 3682–3699 (Cited on page 13).

[30] Hoeffding, W. "Probability Inequalities for Sums of Bounded Random Variables". In: *Journal of the American Statistical Association* 58.301 (Mar. 1963), pp. 13–30 (Cited on page 14).

[31] Bentkus, V. and Zuijlen, M. van. In: *Lithuanian Mathematical Journal* 43.2 (2003), pp. 141–160 (Cited on page 14).

[32] Bent, N., Qassim, H., Tahir, A. A., Sych, D., Leuchs, G., Sánchez-Soto, L. L., Karimi, E., and Boyd, R. W. "Experimental Realization of Quantum Tomography of Photonic Qudits via Symmetric Informationally Complete Positive Operator-Valued Measures". In: *Phys. Rev. X* 5 (4 Oct. 2015), p. 041006 (Cited on page 17).

[33] Lemos, G. B., Almeida, J. O. de, Walborn, S. P., Ribeiro, P. H. S., and Hor-Meyll, M. "Characterization of a spatial light modulator as a polarization quantum channel". In: *Phys. Rev. A* 89 (4 Apr. 2014), p. 042119 (Cited on page 17).

[34] Pimenta, W. M., Marques, B., Maciel, T. O., Vianna, R. O., Delgado, A., Saavedra, C., and Pádua, S. "Minimum tomography of two entangled qutrits using local measurements of one-qutrit symmetric informationally complete positive operator-valued measure". In: *Phys. Rev. A* 88 (1 July 2013), p. 012112 (Cited on page 17).

[35] Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S., and Eisert, J. "Quantum State Tomography via Compressed Sensing". In: *Physical Review Letters* 105.15 (Oct. 2010) (Cited on page 20).

[36] Candes, E. J. and Plan, Y. "Tight Oracle Inequalities for Low-Rank Matrix Recovery From a Minimal Number of Noisy Random Measurements". In: *IEEE Transactions on Information Theory* 57.4 (Apr. 2011), pp. 2342–2359 (Cited on page 20).

[37] Saleh, B. E. A. and Teich, M. C. *Fundamentals of Photonics*. Wiley-Interscience, 2007 (Cited on page 20).

[38] Sych, D., Řeháček, J., Hradil, Z., Leuchs, G., and Sánchez-Soto, L. L. "Informational completeness of continuous-variable measurements". In: *Physical Review A* 86.5 (Nov. 2012) (Cited on page 22).

[39] CVX Research, I. *CVX: Matlab Software for Disciplined Convex Programming, version 2.0*. `http://cvxr.com/cvx`. Aug. 2012 (Cited on page 26).

[40] Grant, M. and Boyd, S. "Graph implementations for nonsmooth convex programs". In: *Recent Advances in Learning and Control*. Ed. by V. Blondel, S. Boyd, and H. Kimura. Lecture Notes in Control and Information Sciences. `http://stanford.edu/~boyd/graph_dcp.html`. Springer-Verlag Limited, 2008, pp. 95–110 (Cited on page 26).

[41] Koutný, D., Teo, Y. S., Hradil, Z., and Řeháček, J. "Fast universal performance certification of measurement schemes for quantum tomography". In: *Physical Review A* 94.2 (Aug. 2016) (Cited on page 29).